INSTALLATION FORCE PROTECTION GUIDE

UNITED STATES AIR FORCE

RONALD R. FOGLEMAN
GENERAL, USAF
CHIEF OF STAFF

EUGENE A. LUPIA
MAJOR GENERAL, USAF
THE CIVIL ENGINEER

The U.S. Air Force has installations and facilities all over the world. Some of these installations and facilities are in locations that have long been perceived as safe, while others are in settings that are known to be unstable or even hostile. Recent events, however, have made it clear that terrorists are at work everywhere, even in our own country. In a world in which terrorist groups are numerous and diverse, geographic location is no longer an accurate indicator of a facility's vulnerability to the threat of terrorism. As such, we must make a conscious effort to recognize the risks associated with terrorist groups and take appropriate measures to protect our personnel against harmful tactics.

On November 19, 1996, in remarks to the Joint Staff and Defense Weapons Agency, the Chairman of the Joint Chiefs of Staff emphasized major reassessments of efforts to protect U.S. personnel and assets from terrorist attacks: "Some nations (and) groups that wish us ill, have reached a conclusion that our conventional capability now is so extensive …that their only chance to impose their will on (us) is through something other than conventional military operations. Terrorism is very high on the menu of options available to them, and particularly terrorism against the United States military is a very effective tool for them to use."

Senior DoD officials assured the President and Congress of a thorough review of the DoD antiterrorism force protection (AT/FP) program and the creation of DoD-wide centralized AT/FP standards. The Secretary of Defense (SECDEF) focused the DoD Combatant Commanders, Defense Directors, and Services Chiefs on improving antiterrorism and force protection measures for U.S. personnel and DoD installations inside the United States, its territories and possessions, and at overseas locations. DoD Directive 2000.12, "DoD Combating Terrorism Program" was revised and republished September 15, 1996, and SECDEF directed the implementation of other initiatives, including new DoD-wide standards to address force protection.

Force protection must be an essential part of the Air Force planning and design process. We have developed this guide to introduce the concepts of force protection and to address some of the issues involved in its implementation. Use it to protect our most valuable asset: the highly skilled individuals who are critical to the success of our mission.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

A BACKGROUND 1
B PURPOSE 1
C ORGANIZATION AND CONTENT OF THIS DOCUMENT 1
D ASSUMPTIONS 2

CHAPTER 2 FORCE PROTECTION PLAN DEVELOPMENT

A ROLES AND RESPONSIBILITIES 4
B THREAT ASSESSMENT 6
THREAT IDENTIFICATION
THREAT DEFINITION
THREAT LEVEL
C VULNERABILITY ASSESSMENT 9
D FORCE PROTECTION STRATEGIES 10
E IMPLEMENTATION 11
F FORCE PROTECTION PLANNING AND DESIGN GUIDANCE 12

CHAPTER 3 COMPREHENSIVE PLANNING

A LAND USE PLANNING 13
B SITE SELECTION 14
C AREA DEVELOPMENT PLANNING 14
D VEHICULAR ACCESS AND CIRCULATION 15
E UTILITY SYSTEMS 15

CHAPTER 4 FACILITY SITE DESIGN

A GUIDELINES FOR FACILITY SITE DESIGN 18
STAND-OFF ZONES
CONTROLLED ACCESS
SURVEILLANCE
B FACILITY SITE DESIGN TOOLS 24
ORIENTATION OF BUILDINGS ON A SITE
RELATIONSHIP OF ROADS TO AN ASSET
LAND FORMS AND NATURAL RESOURCES
CONTROL POINTS AND PHYSICAL BARRIERS
LANDSCAPE PLANTING
PARKING
SERVICE ACCESS
SITE UTILITIES

CHAPTER

5 BUILDING SYSTEMS DESIGN

A ARCHITECTURAL 31

BUILDING FORM

EXTERIOR ENVELOPE

WINDOWS

DOORS

MISCELLANEOUS

B INTERIOR DESIGN 34

SPACE PLANNING

DETAILING

CIRCULATION

SIGNAGE

C STRUCTURAL 35

D MECHANICAL 36

E ELECTRICAL 36

GLOSSARY 39

BIBLIOGRAPHY 41

LIST OF TABLES

TABLE 2.1 DoD-LEVEL DETERMINATION OF TERRORIST THREAT LEVEL 9

TABLE 3.1 THREAT & PROTECTIVE MEASURES FOR COMPREHENSIVE PLANNING 17

TABLE 4.1 THREAT & PROTECTIVE MEASURES FOR FACILITY SITE DESIGN 28

TABLE 5.1 THREAT & PROTECTIVE MEASURES FOR BUILDING SYSTEMS 37

CHAPTER 1

INTRODUCTION

A BACKGROUND

Department of Defense personnel, facilities, and materials are potential targets for attack by terrorists. During the past 20 years, over 300 personnel affiliated with United States defense forces have been killed, and another 200 have been injured as a result of terrorist attacks. On June 25, 1996, a terrorist attack at Khobar Towers in Saudi Arabia dramatically underscored the fact that the threat of terrorism against U.S. military forces is a reality. The focus of terrorism includes non-military targets, as illustrated by terrorist acts at the World Trade Center in New York City and the Murrah Federal Building in Oklahoma City. These brazen assaults occurred on domestic soil, shattering forever the traditional belief that terrorist targets are limited to overseas countries. While the tragic effects of these events cannot be reversed, every terrorist attack provides lessons on how to preclude or minimize the potential damage from future assaults. U.S. defense forces, including the Air Force, must learn from these incidents and respond appropriately to the threat.

B PURPOSE

The purpose of this document is to provide general guidance on force protection issues for the planning, design, and construction of Air Force installations and facilities to reduce the vulnerability of Air Force personnel to terrorist attacks. It is intended to raise the level of awareness among commanders, planners, designers, engineers, security personnel, and facility users to the issues of force protection that must be considered to minimize loss of personnel and property by planning for force protection and implementing physical security measures as the threat increases. *Force protection* refers to measures designed to protect personnel, facilities, and equipment that support national defense missions. This document contains *guidelines* intended to be applied when and if installation or higher headquarters commanders determine the need exists. These measures are aimed at minimizing loss of life and other critical assets. Implementation of force protection should be based on the assessment of the threat (considering that the threat may be transitory and/or changeable), resources available, and command decisions.

C ORGANIZATION AND CONTENT OF THIS DOCUMENT

This document contains information on installation planning, engineering design, and construction techniques that can preclude or minimize the effects of terrorist attacks upon existing and future facilities. It addresses the comprehensive planning process, facility site design, and building systems design. The content of this guide is divided into four chapters and draws upon and summarizes force protection issues and techniques found in existing technical sources. Due to the broad audience addressed by this guide, only general concepts are presented; detailed technical sources have been referenced where more information is available.

- **Force Protection Plan Development** Outlines a force protection program and framework for facility planning and design.
- **Comprehensive Planning** Addresses land use, transportation, utility systems, and facility siting issues as part of the comprehensive planning and area development plans preparation process.

- **Facility Site Design** Addresses site planning issues and concerns beyond the building perimeter, including exterior utility systems and functional design concepts.
- **Building Systems Design** Addresses facility design issues including architectural, interior design, structural, mechanical, and electrical systems.

D
ASSUMPTIONS

There are no universal solutions to preclude terrorist attacks, since the threat is largely unpredictable and certainly will change over time. As such, this document is not intended to identify or define specific terrorist threats, nor is it intended to mandate wholesale hardening of buildings. This guidance is principally intended to be used for facilities with large concentrations of personnel (over 300) such as administration buildings, dormitories, commissaries, and religious facilities. Planners and designers must be innovative and alert to additional opportunities and techniques for integrating physical security measures into the design and planning of these facilities. Every design is a balance of competing demands and considerations such as building codes and regulations, aesthetic concerns, and budgets. In addition to these demands and considerations, antiterrorism measures should be consciously integrated into facility planning, design, and construction efforts.

The dynamic and opportunistic nature of terrorism hampers efforts to define the character and level of threat. The Air Force objective as prescribed by *AFI 31-210, The Air Force Antiterrorism (AT) Program*, *"is to reduce the vulnerability of personnel and facilities to terrorism while balancing defensive measures with mission requirements and available resources."*

"No matter how many measures are implemented risk is always present" (Structural Engineering Guidelines for New Embassy Office Buildings, U.S. Department of State Bureau of Diplomatic Security). Force protection initiatives will be coordinated closely with Security Forces, Intelligence, and Office of Special Investigations units, given their knowledge of threat possibilities and appropriate responses. Input, guidance, and decisions from other interested agencies and personnel are important in effective force protection planning. However, ultimate responsibility for force protection rests with the Installation Commander, and any actions taken must be consistent with the Commander's decisions.

CHAPTER 2

FORCE PROTECTION PLAN DEVELOPMENT

Force protection is a security program designed to protect resources: people, facilities, and equipment. It is accomplished through the planned and integrated application of other programs such as antiterrorism and counter-terrorism, physical security, personal protective services, and intelligence programs. Focusing on facility planning and design measures, this document outlines a program of steps to accomplish force protection at the installation level. These steps are illustrated in Figures 2.1 and 2.2 and described in the text that follows.

- **Definition of Roles and Responsibilities** Development of an understanding of the roles of all responsible parties.
- **Threat Assessment** Collection and analysis of terrorist threat information, capability, and potential.
- **Vulnerability Assessment** Assessment of critical assets and their vulnerability to terrorist attacks.
- **Identification of Force Protection Strategies** Identification of force protection procedures, actions, and measures to respond to threats and achieve enhanced antiterrorism protection as part of the facility planning and design process.
- **Implementation** Implementation of force protection measures in response to identified terrorist threats.

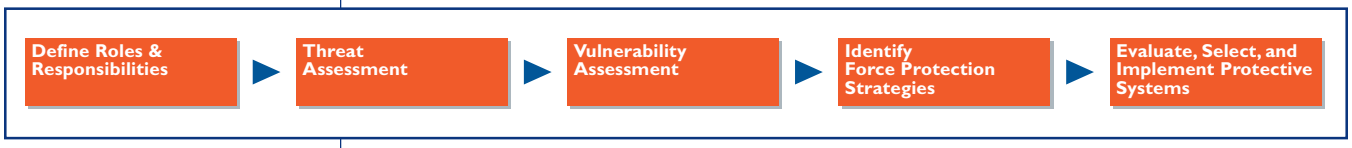


FIGURE 2.1
Force Protection Plan Development Overview

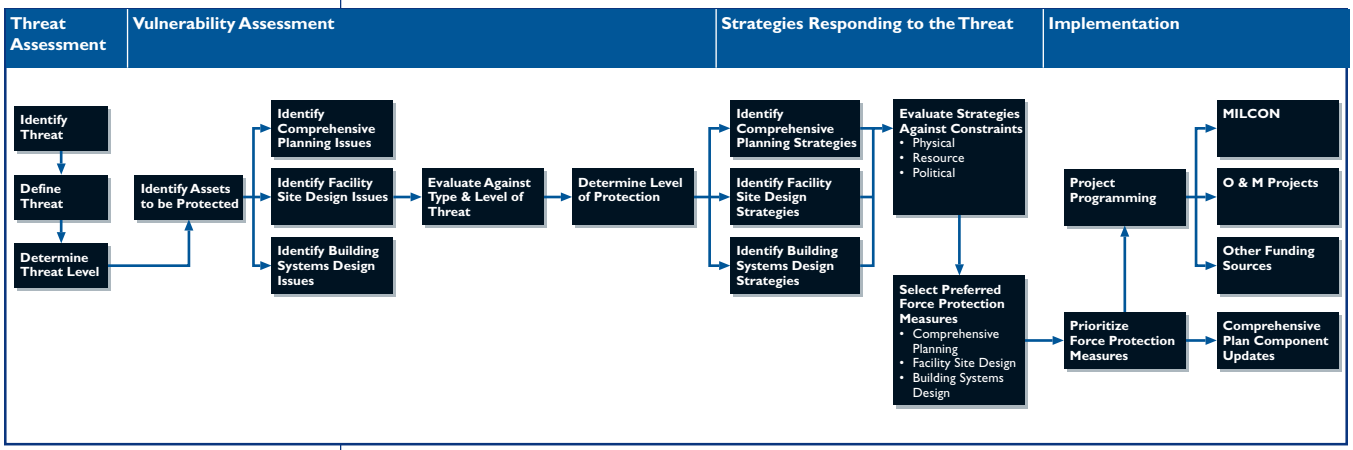


FIGURE 2.2
Force Protection Planning Steps

A
ROLES AND RESPONSIBILITIES

Responsibility for force protection flows from the President to the Office of the Secretary of Defense (OSD) to the Civilian Services Secretaries of the Army, Navy, and Air Force, to the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of DoD, and the Defense Agencies.

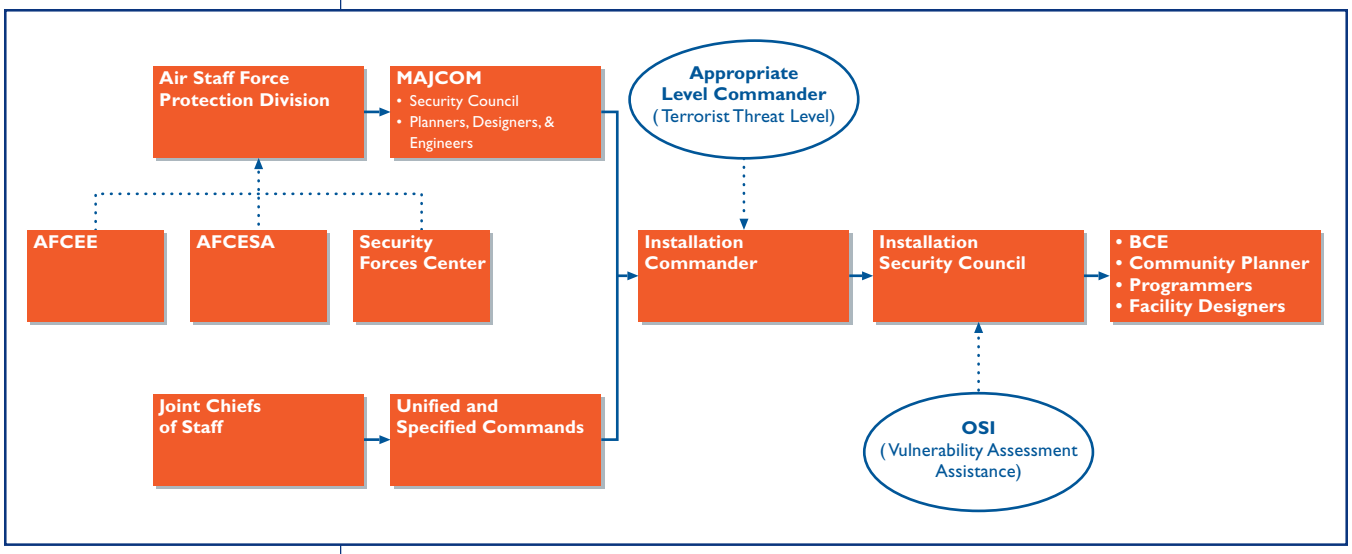


FIGURE 2.3
Roles and Responsibilities

The responsibility for force protection is inherent at all levels of the Air Force. It begins with the Air Staff, and follows a chain of command through Major Commands (MAJCOMs), Installation Commanders, and to the various installation-level organizations associated with security and facility planning and design. Installation Commanders have the ultimate responsibility to plan and implement force protection strategies at the local level. Force Protection Working Groups at the Air Staff, Unified and Specified Commands, MAJCOM, and installation levels promote awareness and provide guidance to the development of a force protection program.

Individual and organizational force protection roles and responsibilities must be practiced and publicized in order to have an effective force protection program. Once personnel and organizations recognize their new roles and responsibilities for integrating force protection, the daily practices they employ for mission accomplishment will eventually incorporate force protection (or will develop a force protection orientation).

The following summarizes the roles and responsibilities of organizations having an active role in force protection.

- **Air Staff** The Directorate of The Civil Engineer, DCS/Installations & Logistics (HQ USAF/ILE) provides direction and advocates funding support for force protection. The Force Protection Division, under the Director of Security Forces (HQ USAF/SF), provides force protection resource advocacy, policy, and guidance to the field. The division is composed of Security Forces, Intelligence and Office of Special Investigations resources. These resources, combined with the other Air Staff organizations of Operations, Civil Engineer, Surgeon General, Logistics, Personnel, and Services, make up the Force Protection Working Group.
- **Security Forces Center** Collocated with the Air Force Security Forces Academy at Lackland AFB, this Direct Reporting Unit (DRU) of Air Staff was designated as a "center of excellence" for force protection. The AF Security Forces Staff, 820th Security Forces Group, and The Force Protection Battle Lab comprise The Security

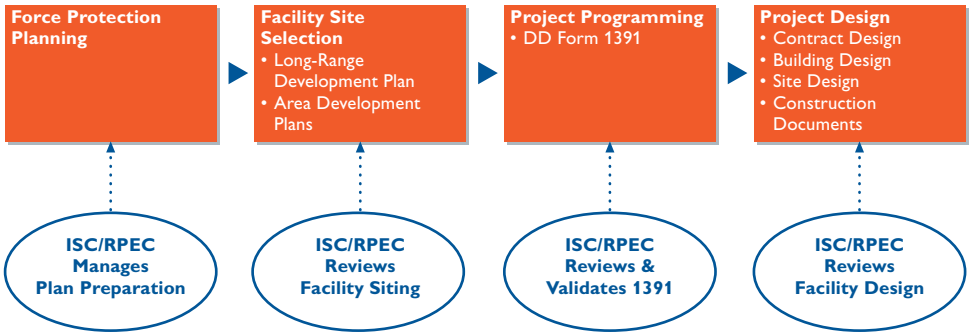
Forces Center. The Security Forces Center is composed of representatives from the Office of Special Investigations, Intelligence, Communications, Security Forces, and Civil Engineer, which includes Explosive Ordnance Disposal.

The 820th Security Forces Group provides a highly trained cohesive unit that can be employed as the initial security force element at deployed locations to establish force protection infrastructure and ensure maximum protection to deployed forces. It also makes force protection recommendations to Installation Commanders utilizing AF OSI threat assessments. Collocated with the Security Forces Group, an Office of Special Investigations Antiterrorism Specialty Teams (AST) provides specialized investigative and force protection services including vulnerability surveys of installation, facilities, buildings, and travel routes; counter-surveillance of potential terrorist targets; and responses to specific terrorist incidents.

- **Air Force Civil Engineer Support Agency (AFCESA)** AFCESA, a Field Operating Agency (FOA) of the Civil Engineer, provides engineering expertise and related information on force protection. The Wright Lab Detachment, collocated with AFCESA, conducts research on explosive testing and analysis of building design and materials to minimize damage as a result of an explosion. Examples of Wright Labs force protection initiatives include planning tools, blast and fragment barriers, structural retrofits, and glass protection. Wright Labs also provides direct assistance to the Air Force operational community in the areas of terrorist weapon effects, installation and facility assessments, and design and analysis of physical protection measures.
- **Air Force Center for Environmental Excellence (AFCEE)** As an FOA and Air Staff service agency, AFCEE executes projects and issues planning and design guidance. AFCEE is the "keeper" of the Force Protection Guide and will be responsible for updating it with new force protection information.
- **Unified and Specified Commands** Provide policy and guidance to Component Commanders regarding threat and force protection measures.
- **Office of Special Investigations (OSI)** In addition to promoting force protection awareness, OSI conducts vulnerability assessments and surveys. OSI also collects intelligence data on terrorist threats through an established intelligence source network, counter surveillance of potential terrorist groups, and response to specific terrorist incidents.
- **Major Commands (MAJCOMs)** Planners, designers, and engineers at the MAJCOM level provide guidance and oversee the implementation of force protection standards at the installation level.
- **Installation Commander** Ultimate responsibility for implementing of force protection measures at the installation level rests with the Installation Commander. The Installation Commander chairs the Installation Security Council (ISC) and/or the Resource Protection Executive Committee (RPEC) and initiates the installation's response to identified threats through the ISC/RPEC.
- **Installation Security Council (ISC)/Resource Protection Executive Committee (RPEC)** An ISC (at installations that support priority resources) manages force protection activities including a vulnerability assessment of critical assets to identified threats and preparation of the Installation Security Plan (ISP). This installation-level organization may be combined with the RPEC. The committee is chaired by the Installation Commander and is composed of, but not limited to, representatives from Office of Special Investigations, Security Forces, Civil Engineers, Fire, Safety, Communications, and Transportation. In

addition to validating and reviewing programming and project design, the ISC should monitor installation facility planning, design, and construction activities to ensure that they comply with established force protection strategies. The ISC/RPEC publishes Installation Security Plans (ISP) which can be combined with the Installation Resource Protection Plan (IRPP) and with other related operation plans (Oplan) into one ISP. *(See AFI 31-209, The Air Force Resource Protection Program).*

FIGURE 2.4
ISC/RPEC's Role in the Facility Planning and Design Process

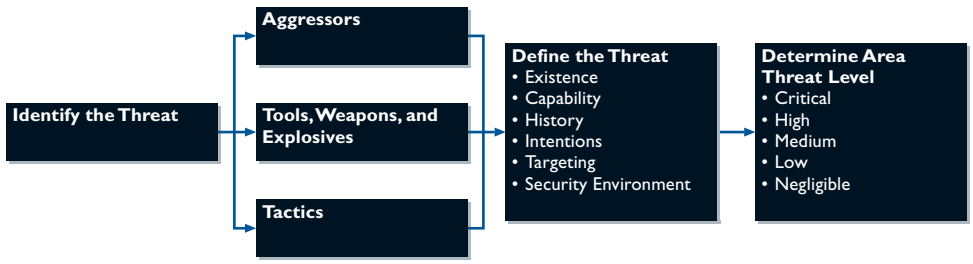


- **Base Civil Engineer (BCE) and Installation Community Planner** The Base Civil Engineer, supported by the installation's community planner and the ISC/IRPEC, ensures that facility force protection measures are included in the Installation Security Plan/Installation Resource Protection Plan. The BCE is also responsible for the integration of force protection measures into the installation's General Plan, Area Development Plans, and Facility Designs.
- **Programmers** Programmers are responsible for integrating force protection measures during project scoping. They ensure that force protection measures are included in the special requirements section of DD Form 1391 in accordance with *AFI 32-1021, Planning and Programming of Facility Construction Projects.*
- **Facility Designers** Facility designers include installation architects, planners, landscape architects, engineers, project managers, and contracted consulting architect-engineers (A-Es). They are responsible for integrating force protection measures during the facility and site design process.

B
THREAT ASSESSMENT

Identification and characterization of terrorist threats are the first steps in developing an antiterrorism force protection program. Once commanders understand the threat, they can assess their facilities' ability to survive an attack. The threat assessment is an essential element in the force protection planning process as it defines the parameters on which effective protective systems are based. The following is an overview of the elements within a threat assessment that relate to installation facility planning and design.

FIGURE 2.5
Threat Assessment Steps



1 THREAT IDENTIFICATION

Identifying the threat focuses on three components:

- Aggressors
- Tools, weapons, and explosives
- Tactics

a Aggressors

Aggressors generally perform hostile acts against people, facilities, and equipment. Their objectives include (1) inflicting injury or death on people; (2) destroying or damaging facilities, property, equipment, or resources; (3) stealing equipment, material, or information; and (4) creating publicity for their cause. Aggressors may use the first three objectives to accomplish the fourth.

b Tools, Weapons, and Explosives

To achieve their objectives, aggressors use various tools, weapons, and explosives, as follows:

- Tools such as forced entry tools, vehicles, and surveillance tools
- Weapons, such as incendiary devices, small arms, antitank weapons and mortars, and nuclear, biological and chemical agents (also called weapons of mass destruction)
- Explosives, such as homemade bombs, hand grenades, and vehicle bombs

c Tactics

Tactics refer to the offensive strategies employed by aggressors, reflecting their capabilities and objectives. Some of the more common tactics include:

- **Moving-vehicle bomb** The moving-vehicle bomb is a suicide attack where an explosive-laden vehicle is driven into a facility, and detonated.
- **Stationary vehicle bomb** This type of bomb may be detonated by time delay or remote control.
- **Exterior attack** This attack is at close range of a facility or exposed asset. Using clubs, rocks, improvised incendiary devices, hand grenades, or hand-placed bombs, the aggressor attempts to inflict destruction and death.
- **Stand-off weapons attack** These attacks are executed using military or improvised direct- and indirect-fire weapons, such as antitank weapons and mortars.
- **Ballistic attack** Using small arms at varying distances, the aggressor attempts to inflict death.
- **Covert entry** The aggressor attempts to enter the facility covertly using false credentials. The aggressor may attempt to carry weapons or explosives into the facility.
- **Mail bombs** Small bombs or incendiary devices are incorporated into envelopes or packages that are delivered to the targeted individual.
- **Supplies bombs** Bombs or incendiary devices, generally larger than those found in mail bombs, are incorporated into various containers and delivered to facilities or installations.
- **Airborne contamination** The aggressor uses chemical or biological agents to contaminate the air supply of a facility or installation.
- **Waterborne contamination** The aggressor uses chemical, biological, or radiological agents to contaminate the water supply of a facility or installation.

2 THREAT DEFINITION

Terrorists operate in a clandestine mode, so the information needed to define and analyze terrorist threat is often more difficult to acquire than information dealing with less esoteric military threats. To build a composite picture of threat conditions, police and intelligence personnel gather information from numerous sources such as newspapers, criminal records, government records, local organizations and people, and other intelligence organizations. As outlined in *DoD O-2000.12-H*, the Department of Defense has identified six factors to be used in the collection and analysis of information from all sources bearing on terrorist threat. These factors, which are used in making terrorist threat analyses on a country-by-country basis, are as follows:

- **Existence** A terrorist group is present, assessed to be present, or able to gain access to a given country or locale. The analysis of information regarding the existence of a terrorist group addresses the question: Who is hostile to existing organizations and social structure?
- **Capability** The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks. An analysis of terrorist group capabilities addresses the questions: What weapons have been used by terrorist groups in carrying out past attacks? What infrastructure is necessary to train, equip, target, and execute attacks?
- **History** Demonstrated terrorist activity over time. The analysis of terrorist group history addresses the questions: What have the terrorists done in the past? What is the terrorist group's method of operations? How did they acquire the capacity they demonstrated? Where did they obtain support? What additional attacks did they mount?
- **Intentions** Recently demonstrated anti-U.S. terrorist activity, or stated or assessed intent to conduct such activity. An analysis of terrorist group intentions addresses the questions: Why do groups engage in terrorist acts? What do they hope to achieve?
- **Targeting** Current credible information on activity, indicative of preparations for specific terrorist operations. Targeting addresses the questions: Who is likely to be attacked, why are they likely to be attacked, and what is the basis for accepting reports that such attacks are planned?
- **Security environment** The internal political and security considerations that impact terrorist element capability to carry out their intentions. The parameters examined within the security environment of a country include training of national law enforcement, paramilitary, and military institutions to deal with terrorist incidents and to maintain social order; quality of equipment available for law enforcement and internal security forces; and distribution of internal security forces throughout a country.

The Air Force, as does each of the Services, maintains its own terrorist threat analysis capability. While DoD methodology is used, the differences in perspective among Defense Intelligence Agency (DIA), Services, or CINC threat analysis may lead to divergent conclusions about specific terrorist threats. While the threat to all DoD assets in a country may be at one level, the Air Force, having no assets in the country, may decide it faces no threat of terrorism in the country or locale in question.

3 THREAT LEVEL

Force protection planning responds to the *threat level*. The degree to which an asset is protected against a threat or spectrum of threats is based primarily on its importance to the Air Force but secondarily to its publicity value to the terrorist and its susceptibility

to terrorist activity. Specific levels of protection are appropriate to each threat level. Levels of protection refer to an acceptable degree of damage, given an attack, or the probability that an aggressor will be defeated by the protective system. The Air Force as well as other Services uses the DoD notation system to describe the country - specific results of terrorist threats based on terrorist threat methodology used above.

The threat level for an area is determined after information on the threat factors is gathered and analyzed. The greater the presence of threat factors, the higher the threat level. Five of the six factors are used together to define the threat level; the sixth, security considerations, is used separately as a modifying factor. The following table depicts the relationships of the threat factors and threat levels. *(See DoD O-2000.12-H, Chapter 5).*

TABLE 2.1
DoD-Level Determination of Terrorist Threat Level

THREAT LEVEL	THREAT ANALYSIS FACTORS				
	Existence	Capability	History	Intentions	Targeting
Critical	■	■	□	□	□
High	■	■	■	■	
Medium	■	■	■	□	
Low	■	■	□		
Negligible	□	□			

■ Factor must be present □ Factor may or may not be present

Source: DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence, Figure 5-1

Installation Commanders should rely on local intelligence and counterintelligence (OSI) personnel to provide warnings and indicators about specific and general threats to the installation resources and personnel. The Federal Bureau of Investigation (FBI) determines threat levels in the Continental United States (CONUS) and the Defense Intelligence Agency (DIA) determines threat levels Outside the Continental United States (OCONUS) for DoD installations. Commanders at all levels establish threat conditions (threatcons) based on the FBI or DIA threat level and locally developed information. This information, coupled with the vulnerability assessment discussed in the following section, will influence decisions as to which force protection measures are applied to installation assets.

C
VULNERABILITY ASSESSMENT

A *vulnerability assessment* addresses the susceptibility to attack and the broad range of physical threats to the security of personnel and facilities and provides a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks. The Installation Commander is responsible for requesting or initiating the vulnerability assessment, which seeks to identify how susceptible an installation is to a terrorist attack and the level of security provided to the installation's assets.

The Defense Special Weapons Agency (DSWA), Force Protection Division, is designated as the central DoD office for accomplishing vulnerability assessments. DSWA is comprised of physical security specialists, engineers, and disaster preparedness specialists. DSWA provides an allocation of vulnerability assessments to Service Commanders and Theater CINCs who then determine the priority of installations to be assessed.

Locally prepared vulnerability assessments should follow the guidelines contained within *AFI 31-210, Air Force Antiterrorism (AT) Program*, as well as *DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*. An installation-wide vulnerability assessment includes an identification of the assets to be protected (i.e., critical facilities) and a determination of their ability to

withstand identified threats. A method for identifying and categorizing assets can be found in *AFJMAN 32-1071, Volume 1, Security Engineering Project Development, Chapter 3*. A vulnerability assessment also identifies and analyses land use planning, circulation, and infrastructure considerations that may improve the installation's ability to contend with a terrorist threat. The results of these analyses are then evaluated against the type of threat and identified threat level to determine the appropriate level of protection.

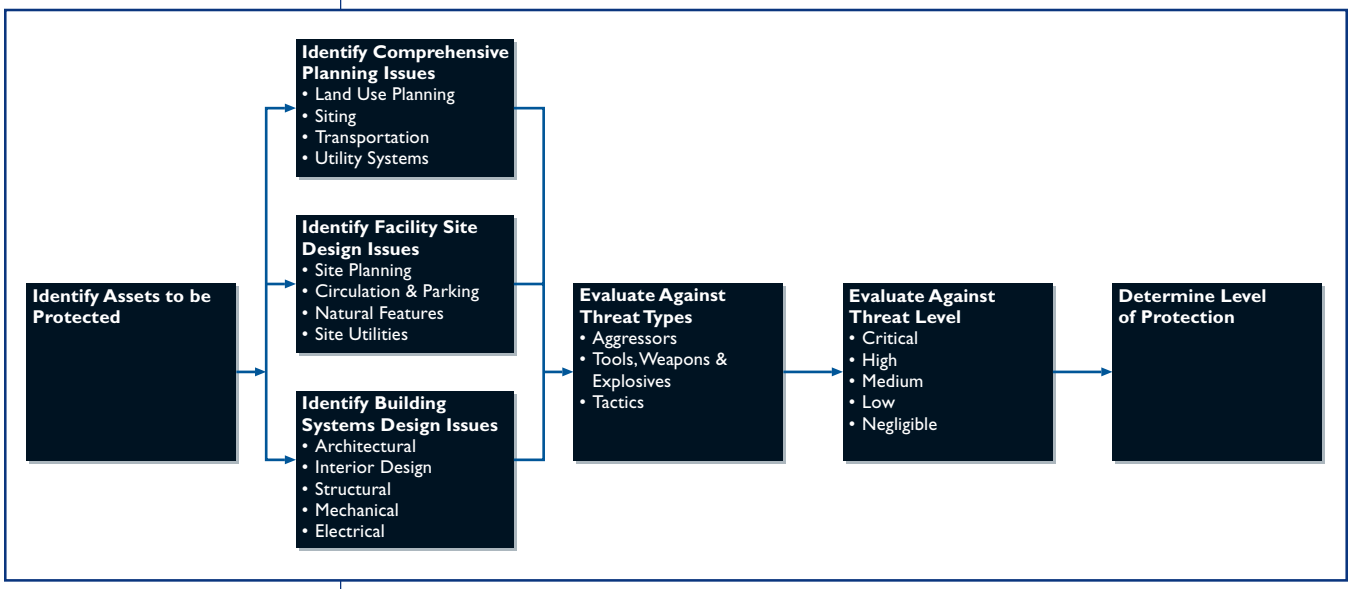


FIGURE 2.6
Steps to Conduct a Vulnerability Assessment

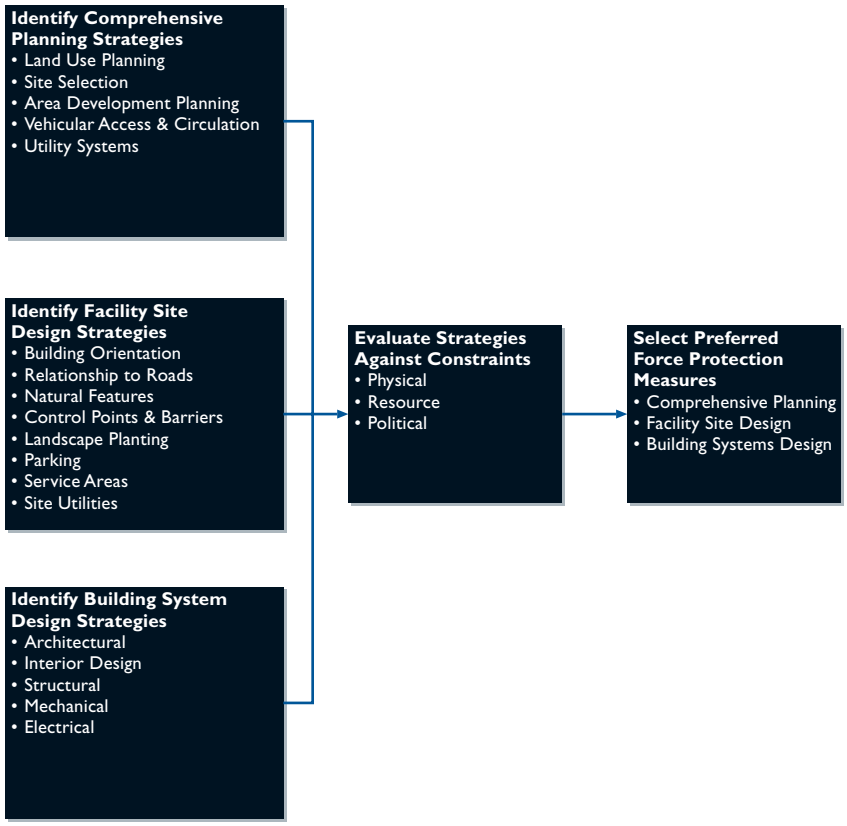
As each installation may have varying levels of threat, the level of protection will vary. Expedient force protection measures will generally not provide the highest level of protection to assets. Higher levels of protection are usually incorporated in the original design and construction of a facility or are provided by relatively extensive retrofitting.

D
FORCE PROTECTION STRATEGIES

Using the physical security systems approach recommended by *DoD O-2000.12-H, Change 2, Appendix EE, Force Protection Design Considerations* and *AFJMAN 32-1071, Volumes 1-3*, Installation Commanders have the responsibility to develop and implement physical security strategies and systems incorporating facilities, equipment, trained personnel, and procedures, designed to provide maximum antiterrorism protection to personnel and assets.

After acceptable levels of protection are determined, appropriate protective strategies are identified. The transitory nature of the threat or its duration must also be considered. These strategies may be in the form of planning actions or construction projects (either new or renovation). They could include reorganization of land uses, reorientation of roadways, security improvements to installation entries, and improvements to the facility, including the existing structure and surrounding site area. For some strategies, this process may include the identification of multiple scenarios, or alternatives, for achieving the desired goal. All alternatives should undergo a suitability analysis, which takes into account factors that may limit the feasibility of an action or project. Limiting factors consist of physical, resource, and political constraints such as land area restrictions, limited availability of construction materials, and host nation or civilian sensitivities. Following this evaluation of constraints, preferred force protection measures are selected.

FIGURE 2.7
Development of Force Protection Strategies

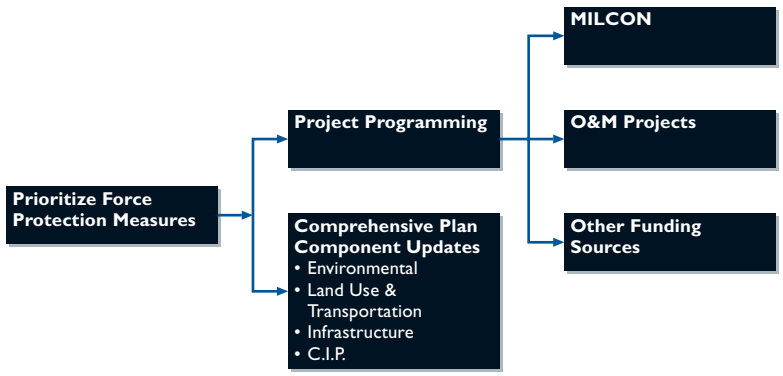


E
IMPLEMENTATION

Appropriate protective measures developed during force protection plan development are implemented through a series of actions including prioritization of recommended force protection measures, programming and funding of proposed projects, and constructing facilities in accordance with a prioritized program. Integration of force protection requirements into new projects can be achieved by using a separate line item for force protection, including a description of threat levels, in the project's documentation.

In addition to proposed projects and construction, some protective measures may include adjustments and/or updates to comprehensive plan elements.

FIGURE 2.8
Implementation Actions



Force protection planning can be implemented within the framework of existing procedures for planning and design at the installation level. Planners and designers can integrate force protection measures into three planning and design areas that support base development: *comprehensive planning*, *facility site design*, and *building systems design*. As summarized in the following text, the subsequent chapters of this document provide guidance for integrating protective measures into comprehensive planning, facility site design, and building systems design.

Chapter 3 - Comprehensive Planning Comprehensive planning provides a framework to guide development of the installation. Consideration of force protection at the planning stage may preclude the need for force protection measures at the facility site design and building systems design stages. Force protection measures should be addressed in planning documents related to land use, transportation, environmental, infrastructure, and capital improvements where appropriate. *DoD Instruction 2000.16, Enclosure (1), DoD Combating-Terrorism Program Standards* requires Installation Commanders to review their comprehensive plans annually (or more frequently when the terrorist threat level changes) to ensure that the design and implementation of physical security measures are responsive to local terrorist threat conditions.

Within the comprehensive planning framework, Area Development Plans (ADPs) address facility planning issues at a sub-area level. ADPs present conceptual facility layouts and solutions, including vehicular circulation and parking. Since they generally precede facility design, ADPs are an ideal stage for the early incorporation of force protection measures.

Chapter 4 - Facility Site Design Facility location and orientation, including separation from adjacent facilities, and natural site features can contribute to enhancing force protection. The facility site design chapter addresses methods for integrating landscape planning, entry control points, vehicle barriers, fences, and security lighting to diminish potential threat to critical assets. Landscape planning can make use of vegetation, topography, and bodies of water as protective measures.

Chapter 5 - Building Systems Design Building systems design measures are considered only after all appropriate protective measures have been considered at the comprehensive planning and facility site design levels. Walls, roofs, floors, and fenestration can be designed to reduce the vulnerability of a facility, thereby making it a less inviting target.

CHAPTER 3

COMPREHENSIVE PLANNING

Many force protection objectives can be achieved through the comprehensive planning process. The least costly and often the most effective protection measures are those incorporated during the comprehensive planning phase. Implementing appropriate force protection measures at the planning stage can preclude the need for piecemeal and costly security enhancements later on.

It is important to remember that the nature of the threat is ever changing. Some degree of security should be provided at the planning stage, with consideration given to increased or enhanced protection at times of increased threat. Force protection objectives must be balanced with other planning objectives, such as the efficient use of land and resources, and must take into account existing physical, programmatic, and fiscal constraints.

This chapter addresses force protection measures related to the following comprehensive planning areas:

- Land Use Planning
- Site Selection
- Area Development Planning
- Vehicular Access and Circulation
- Utility Systems.

For a graphic illustration of the relationship between protective measures and potential threats, refer to the matrix provided at the end of this chapter. The matrix summarizes the comprehensive planning measures presented in this chapter and indicates their effectiveness against the potential aggressor tactics discussed on Chapter Two.

A LAND USE PLANNING

- When preparing land use plans, locate high-risk land uses in the interior of the installation. High-risk land uses contain high concentrations of personnel, such as administrative, community, and housing areas.
- Consolidate high-risk land uses, to take advantage of opportunities for security efficiency such as minimized control points.
- In most cases, integration of force protection measures at the comprehensive planning level will increase the land area needed for individual facilities. Accordingly, when preparing future land use plans, take into account the land areas associated with proposed force protection measures in the calculation of land area requirements.
- Assess off-base adjacent land use and zoning plans for potential development that would impact security within the installation.

B
SITE SELECTION

- When selecting a site for a facility, consider its location relative to the base perimeter. Maximize the distance between the perimeter fence and developed areas, providing as much open space as possible inside the fence along the base perimeter.
- Elevated sites generally enhance surveillance of the surrounding area. However, adjacent high terrain or structures outside the base boundary allow observation of on-base areas by outsiders.
- Dense vegetation in proximity to a facility can screen covert activity and should be avoided.
- Avoiding low-lying topographic areas when siting facilities can mitigate the effects of the possible use of biological and/or chemical weapons.

C
AREA DEVELOPMENT PLANNING

Facility site design encompasses site planning for a specific facility and its site, including the arrangement of the facility footprint, relationship of a building to a specific site, internal circulation, access, parking, landscaping, lighting, and signage. By comparison, Area Development Plans (ADPs) focus on broader site planning, facility siting, and circulation variables. The following guidelines refer to these broader concerns associated with site planning at an area scale (i.e., multiple facilities) versus site scale (i.e., singular facility).

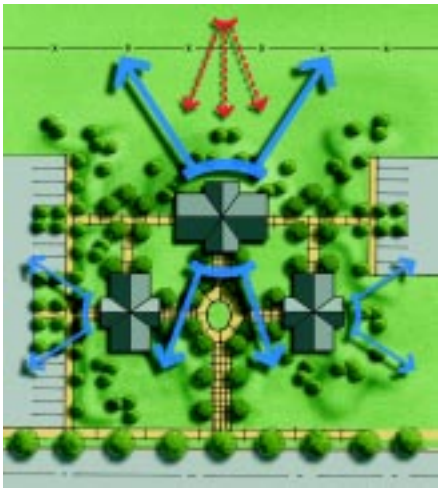
- Provide a separation distance between facilities adequate to minimize collateral damage. *(AFJMAN 32-1071, Vol. 1, 5-6.a and Appendix C)*
- Site facilities within view of other occupied facilities.
- When possible, cluster facilities that are functionally compatible and have similar threat levels. This reduces the perimeter area to be protected, limits access points to serve multiple facilities, and provides compact security areas. However, the practical benefits of clustering facilities must be balanced with the survivability benefits of resource dispersal in the event of an attack.

FIGURE 3.1
Consolidated and clustered versus separated facilities

Consolidated facilities **Separated facilities**

- The arrangement of building into complexes, with strongly delineated boundaries and buildings oriented to enhance surveillance opportunities, results in the creation of "defensible space" that can be protected more efficiently than scattered buildings *(AFI 32-209, The Air Force Resource Protection Program, par. 1.1)*. Vehicle parking should be eliminated from between clusters of high-risk buildings.

FIGURE 3.2
Enhanced surveillance opportunities from clustering of facilities while minimizing views in



D
VEHICULAR ACCESS AND CIRCULATION

- Provide pull-over lanes at installation entry gates to check suspect vehicles *(AFJMAN 32-1071, Vol. 2, 3-7).*
- Design entry roads to installations and to individual buildings so that they do not provide direct or straight-line vehicular access to high-risk resources.
- Locate vehicle parking areas remote from high-risk resources to minimize blast effects from potential vehicle bombs.
- Whenever possible, commercial, service and delivery vehicles should have a designated entry to the installation preferably distant from high-risk resources.
- When planning new roads, route major corridors away from concentrations of high-risk resources. When selecting sites for high-risk resources, locate them remote from primary roads.
- Minimize the number of signs identifying high-risk facilities.
- Clustering and securing facilities provides opportunities to minimize control points and limit vehicular access to high-risk resources. *(AFJMAN 32-1071, Vol. 1, 5-6b.(3))*

E
UTILITY SYSTEMS

- Vulnerability assessments should identify all utility service to the installation, as well as all utility lines, storm sewers, gas transmission lines, electricity transmission lines, and other utilities that may cross the installation perimeter. Detailed knowledge of such service is important for public health and safety considerations as well as installation security concerns.
- All utility penetration of the installation's perimeter, including penetrations in fences, walls, or other perimeter structures should be screened, sealed, or secured to prevent their use as access points for unlawful entry into the installation. If access is required for maintenance of utilities, secure all penetrations with screening, grating, lattice work, or other similar devices such as that openings do not allow intruder access. Provide intrusion detection sensors and consider overt or covert visual surveillance systems if warranted by the sensitivity of assets requiring protection. *(DoD O-2000.12-H, p. 9-19)*
- Develop protective measures such as screens, fences, or grates to prevent covert access through concrete trenches, storm drains, duct systems, etc. Provide and check locks on manhole covers.

- Protect water treatment plants and storage facilities from waterborne contaminants by securing access points, such as manholes. Maintain routine water testing to help detect waterborne contaminants. *(DoD O-2000.12-H, Appendix EE, p. 47 and AFJMAN 32-1071, Vol. 1, Ch. 12, Sec. III)*
- Minimize signs identifying critical utility complexes, e.g., power plants and water treatment plants. Provide fencing to prevent unauthorized access and use landscape planting to conceal above-ground systems. When possible, install utilities underground.
- Locate petroleum, oil and lubricants (POL) storage tanks and operations facilities down slope from all other facilities. Site fuel tanks at an elevation lower than operational buildings or utility plants.
- Utility systems should be provided with redundant or loop service, particularly in the case of electrical systems. Where more than one source or service is not currently available, provisions should be made for future connections. In the interim, consider "quick connects" at the facility for portable back-up systems.
- Decentralization of an installation's communications resources and the use of multiple communication networks will strengthen the communications system's ability to withstand the effects of a terrorist attack. Careful consideration should be made in locating, concealing, and protecting key network resources such as network control centers.

TABLE 3.1
Threat & Protective Measures for Comprehensive Planning

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Ballistics Attack	Covert Entry	Mail & Supplies Bombs	Airborne Contamination	Waterborne Contamination
LAND USE PLANNING									
Locate high-risk land uses in the interior of the installation	■	■	■	■	■				
Consolidate high-risk land uses	■	■	■	■	■				
Include stand-off areas in land area requirements	■	■		■	■				
Consider effects of off-base development	■	■	■		■				
SITE SELECTION									
Maximize distance from perimeter fence & developed areas	■	■	■	■	■			■	
Site critical facilities on higher ground	■	■	■	■	■			■	■
Avoid areas with adjacent high terrain or structures			■	■	■			■	■
Avoid areas with adjacent dense vegetation			■	■	■				
Avoiding low-lying topographic areas			■	■	■			■	■
AREA DEVELOPMENT PLANNING									
Provide separation between facilities	■	■	■	■	■		■		
Site facilities within view of other occupied facilities						■			
Cluster facilities with similar threat levels	■	■		■	■				
Create complexes to enhance surveillance opportunities	■	■	■	■	■				
Eliminate vehicle parking from interior of building complexes	■	■							
VEHICULAR ACCESS AND CIRCULATION									
Provide enhanced protection at installation entries	■	■	■	■	■	■			
Include pull-over lanes at checkpoints to inspect vehicles	■	■	■	■	■	■			
Avoid straight-line vehicular access to high-risk resources	■	■							
Avoid straight-line entry approach roads	■	■							
Locate vehicle parking areas far from high-risk resources	■	■							
Provide separate service & delivery access	■	■							
Route major corridors away from high-risk resources	■	■		■	■				
Locate high-risk resources remote from primary roads	■	■		■	■				
Minimize directional identification signs	■	■	■	■	■	■			
Limit vehicular access to high-risk resources	■	■	■	■	■	■			
UTILITY SYSTEMS									
Provide protection at culverts, sewers, & pipelines					■	■			■
Provide protection at concrete trenches, storm drains & duct systems					■	■			■
Provide and check locks on manhole covers					■	■			■
Minimize signs identifying identifying utility systems					■	■			■
Provide fencing at critical utility complexes						■			■
Use landscape planting to conceal above-ground systems						■			■
Install utilities underground	■	■	■	■	■	■	■		■
Locate POL storage down slope and away from facilities	■	■	■	■	■	■	■		
Provide redundant utility systems and loop service	■	■	■	■	■	■	■		
Provide utility "quick connects" for portable back-up systems	■	■	■	■	■	■	■		
Decentralize communications resources	■	■	■	■	■	■	■		
Use multiple communication networks	■	■	■	■	■	■	■		
Conceal & protect network control centers	■	■	■	■	■	■	■		

■ **The symbols indicate which of the protective measures shown in the left-hand column can be effective in countering the types of threats indicated across the top of the chart.**

CHAPTER 4

FACILITY SITE DESIGN

This chapter addresses force protection issues at the facility site design stage, including orientation of buildings and integration of vehicle access, control points, physical barriers, landscape planting, parking, and protection of utilities to mitigate threats. Taking advantage of existing site elements is also a consideration in the facility site design process. Determining how to provide for the facility's security needs requires an understanding of which site elements are beneficial and which are detrimental.

As discussed in this chapter, conflicts sometimes arise between security site design and conventional site design. For example, open circulation and common spaces, which are desirable for conventional design, are often undesirable for security design. To resolve these and other issues, coordination between design disciplines (e.g., planning, designing, and engineering) is critical to the force protection process. Facility site design works in conjunction with building design. Designers must balance force protection priorities with the requirements of the Americans with Disabilities Act Accessibility Guidelines (ADAAG), Uniform Federal Accessibility Standards (UFAS), National Fire Protection Codes (NFPA), and all applicable local building codes. Finally, the Installation Security Council should review all force protection measures incorporated into facility site designs to ensure they are beneficial and cost effective.

This chapter addresses force protection measures related to the following facility site design issues:

- Guidelines for Facility Site Design
- Facility Site Design Tools
  - Orientation of Buildings on a Site
  - Relationship of Roads to an Asset
  - Land Forms and Natural Resources
  - Control Points and Physical Barriers
  - Landscape Planting
  - Parking
  - Service Access
  - Site Utility Vulnerabilities.

For a graphic illustration of the relationship between protective measures and potential threats, refer to the matrix provided at the end of this chapter. The matrix summarizes the facility site design measures presented in this chapter and indicates their effectiveness against the potential aggressor tactics discussed in Chapter Two.

A GUIDELINES FOR FACILITY SITE DESIGN

While many different measures can be used to provide force protection in facility site design, *distance* is the most effective and desirable tool because other measures vary in effectiveness, are more costly, and often have unintended consequences. For example, a blast wall can become the source of fragmentation if an explosion occurs in close proximity to the wall.

The first mode of site protection is to create "keep out zones" that can insure a minimum guaranteed distance between an explosion, i.e., from a vehicle, and target structure. Facilities should be located on a site as far as possible from points on the site

perimeter that are accessible to vehicles. "Keep out zones" can be achieved with the use of site elements that function as perimeter barriers to vehicles that cannot be compromised by ramming with a vehicle. It is also desirable to locate facilities away from other buildings that are not potential targets to minimize damage to them.

1 STAND-OFF ZONES

The distance between an asset and a threat is referred to as the *stand-off distance*. There is no ideal stand-off distance; it is determined by the type and level of threat, the type of construction, and desired level of protection.

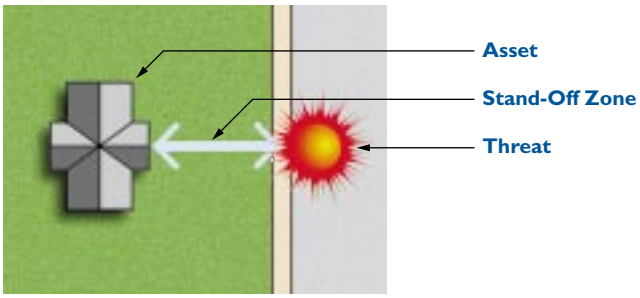


FIGURE 4.1
Concept of stand-off distance

Energy from a blast decreases over distance. The impact of a blast will decrease as the stand-off distance increases, as indicated in the blast analysis of the Khobar Towers Complex (see Figure 4.3). In general, the cost to provide force protection will decrease as the distance between an asset and a threat increases (see Figure 4.2).

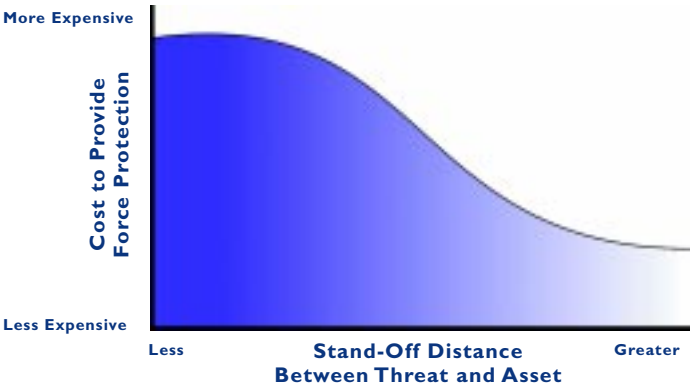
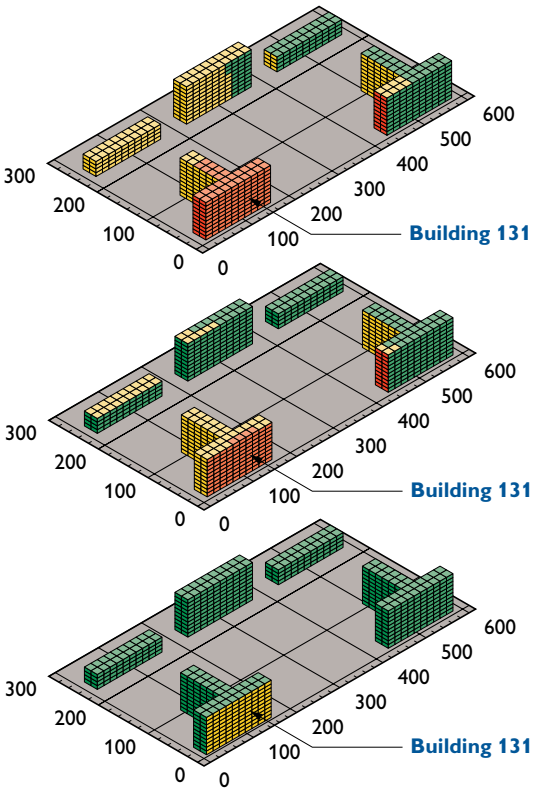


FIGURE 4.2
Relationship of cost to stand-off distance

FIGURE 4.3
Stand-off distance and its relationship to blast impact as modeled on the Khobar Tower Site



Detonation at 80 feet from Building 131
This is the actual stand-off that was provided at the Khobar Towers Complex

Detonation at 170 feet from Building 131
This is the minimum stand-off distance recommended by FM5-114 Engineer Operations Short of War

Detonation at 400 feet from Building 131
This stand-off distance would have prevented serious damage and reduced the extent of casualties

Color	Damage Category	Damage Description	Hazard to Occupants
RED	4	Very severe damage, possible collapse	Very high hazard, widespread death and serious injury likely
YELLOW	3	Heavy unrepairable structural damage	High hazard, death and serious injury possible
GREEN	2	Moderate repairable structural damage	Medium hazard, limited casualties and injury possible
BLUE	1*	Minor to no significant damage	Low hazard, casualties and injury not likely

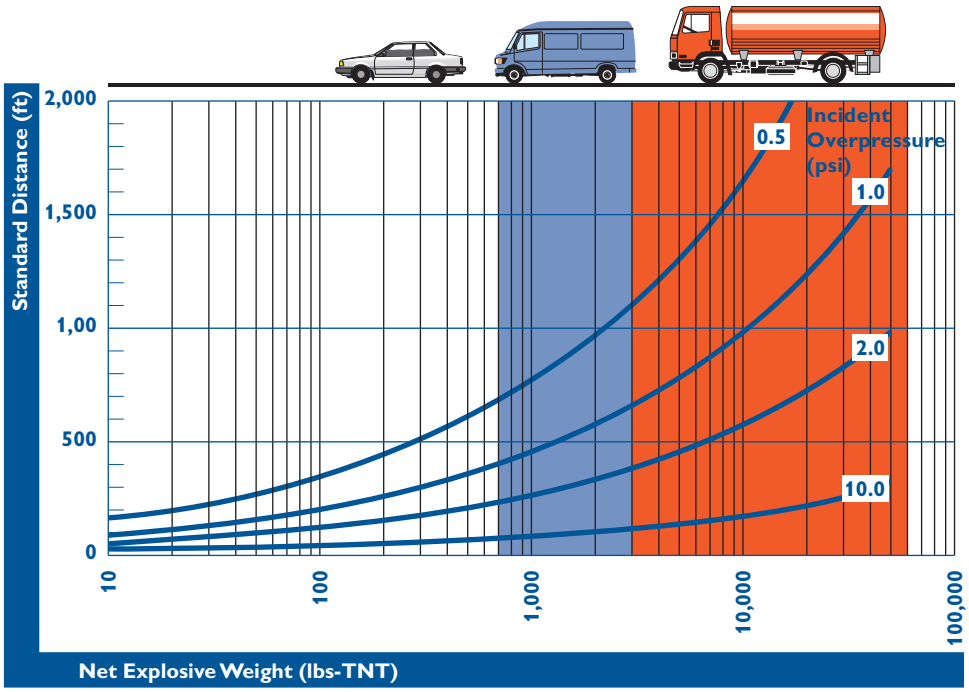
Graphic provided by Applied Research Associates, Inc.

*** Damage category 1 is not visible in the model shown in Figure 4.2**

The appropriate stand-off distance for a given building component to resist the explosives effects of various explosives weights to various levels of protection can be determined using data provided in *AFJMAN 32-1071 Volume 1, Appendix C, Blast Resistant Component Selection* and *DoD O-2000.12-H, Appendix DD, Calculated and Analyzed Blast Effects*. This information can be used in selecting or assessing stand-off distances for both conventional (not designed to resist explosives effects) and blast resistant construction. This includes rules of thumb for distances to be maintained between facilities of conventional construction and an explosive device considering the weight of the explosive (expressed in TNT), the level of protection, and characteristics of the building component.

The expected overpressure (expressed in pounds per square inch or psi) on a facility can be determined by considering the relationship between explosive weight and stand-off distance (see Figure 4.4). Enter the x-axis with the estimated explosive weight a terrorist might use and the y-axis with a known stand-off distance from a facility. Correlating the resultant effects of overpressure with other data, such as K-factors, the degree of damage that the various components of a facility might receive can be estimated. The vehicle icons at the top of Figure 4.4 indicate the relative size of the vehicles that might be used to transport various quantities of explosives.

FIGURE 4.4
Incident overpressure (psi) as a function stand-off distance and net explosive weight (lbs.-TNT)



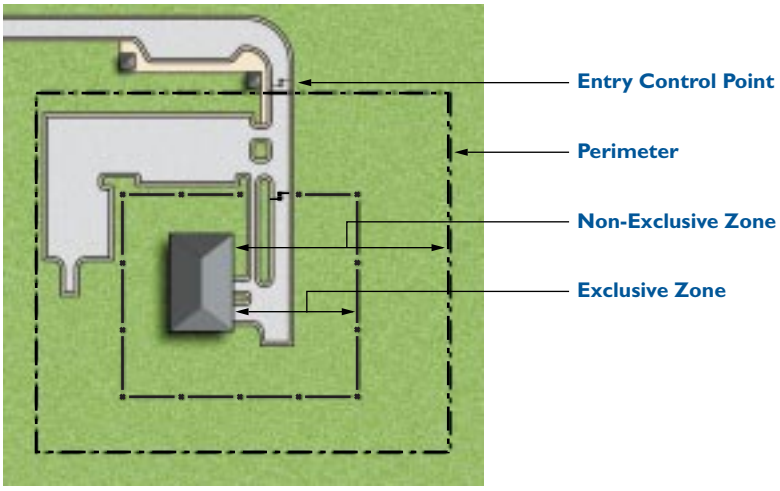
2 CONTROLLED ACCESS

Within the stand-off distance, levels of protection can be achieved by establishing controlled zones. These zones define minimum distances between assets and potential threats through the installation of barriers (such as bollards, planters, and fountains). The barriers should be designed to withstand assaults by terrorist vehicles; however, their placement must be planned to allow for access by fire and rescue vehicles in the event of an emergency.

There are two types of stand-off zones. Selection between them is based on operational considerations related to vehicle access and parking. Stand-off zones completely surround a facility. Perimeters are set at distances that consider threat levels, desired level of protection, building construction, and land availability. Entry into this controlled area is through an *entry control point*.

An *exclusive stand-off zone* is an area that has a controlled entry with highly restrictive access. It can be used with all threat levels. No vehicles except delivery and service vehicles are allowed into the exclusive stand-off zone. The entry control point provides an opportunity to search delivery and service vehicles.

FIGURE 4.5
Exclusive and non-exclusive stand-off zones



A *non-exclusive stand-off zone* is an area that has a controlled entry with less restrictive access. Non-exclusive stand-off zones can be used with exclusive stand-off zones for high and very high threat levels to minimize the use of land area. When a non-exclusive stand-off zone is used, it encloses an exclusive stand-off zone. Passenger vehicles can be allowed in the area between the exclusive and non-exclusive zone but only under surveillance.

To combat against a moving and stationary vehicle bomb tactic, the perimeter of the exclusive stand-off zone should be set at the stand-off distance necessary to mitigate the effects of a bomb that could be carried in a passenger vehicle (up to a medium threat level). Trucks (associated with higher threat levels) are capable of carrying greater quantities of explosives than automobiles and should not be allowed into the non-exclusive stand-off zone without being searched. *AFJMAN 32-1071, Volume 1, Chapter 5* provides additional guidance on the establishment of exclusive and non-exclusive zones.

The exclusive stand-off zone around an asset can include other assets. For example, where there are multiple facilities subject to vehicle bomb threats in the same general area, these facilities may be clustered into common stand-off zones to use land and guard manpower more efficiently (see Figure 4.6). If a primary asset is not currently surrounded by an exclusive stand-off zone, consider closing some streets to create an exclusive zone (see Figure 4.7). Street closures aid in excluding vehicles while continuing to allow access by pedestrians with proper credentials. The possibility of closing streets must be balanced against minimum circulation requirements and fire protection needs.

FIGURE 4.6
Facility clustering

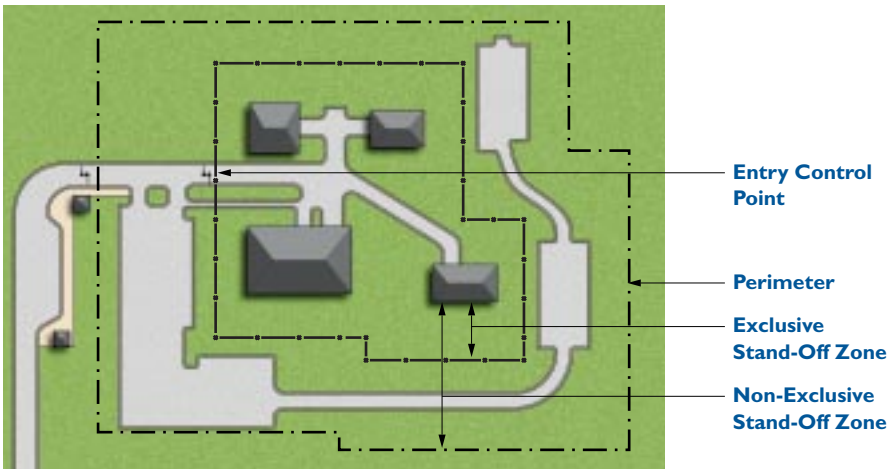
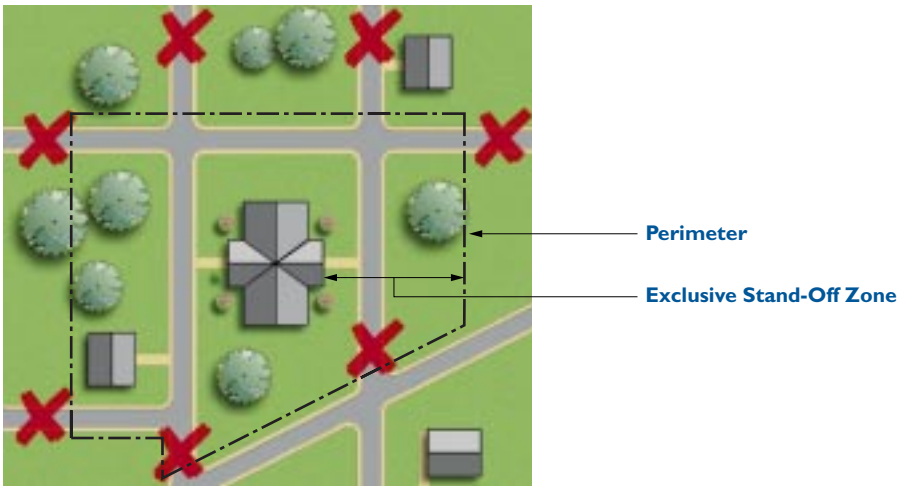
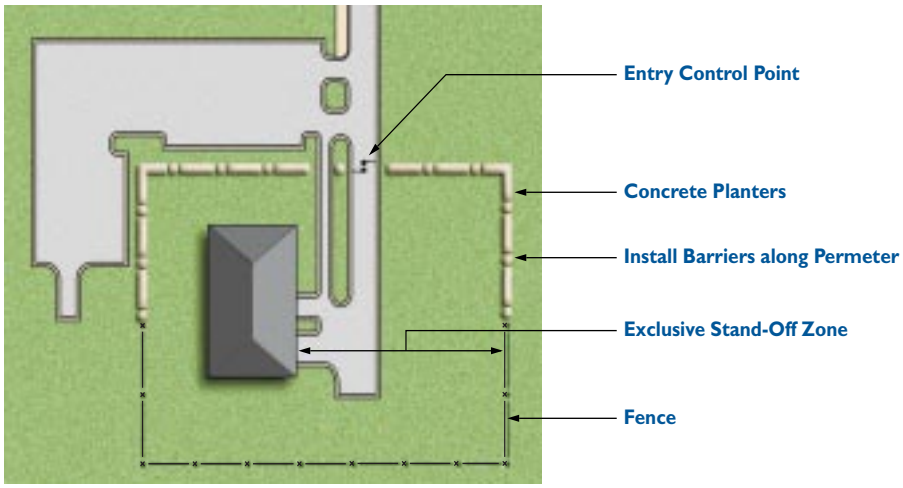


FIGURE 4.7
Using street closings to create an exclusive zone



Barriers used on the perimeter of stand-off zones are *passive barriers.* They are always in place and do not require any action to be employed. Perimeter barriers are selected differently for moving and stationary bomb tactics. Refer to Figure 4.8 for an illustration of the application of various perimeter barriers on a stand-off zone perimeter and *AFJMAN 32-1071, Volume 1, Chapter 5* for additional guidance on barrier selection.

FIGURE 4.8
Application of perimeter barriers



3 SURVEILLANCE

An additional level of protection can be provided for high-risk facilities by creating a *clear zone* within the exclusive stand-off zone (see Figures 4.9 and 4.10). A clear zone is an area immediately adjacent to the asset that is free of all visual obstructions or landscaping that could provide concealment. The clear zone facilitates visual detection of bombs placed near the facility. Minimum clear zone distances are defined in *AFJMAN 32-1071, Volume 1, Chapter 6 and DoD O-2000.12-H, Appendix EE, D. Physical Security Measures for an Installation.*

Clear zones can be extended if the building construction requires additional stand-off distance to resist the threat explosive. If required, the stand-off zone should be extended if building construction requires additional stand-off distance to resist the threat explosive. If required, extend the stand-off zone to accommodate an expanded clear zone. Walkways and other circulation features within a clear zone should be located so that buildings do not block views of pedestrians and vehicles.

FIGURE 4.9
Clear zone used in conjunction with a stand-off zone

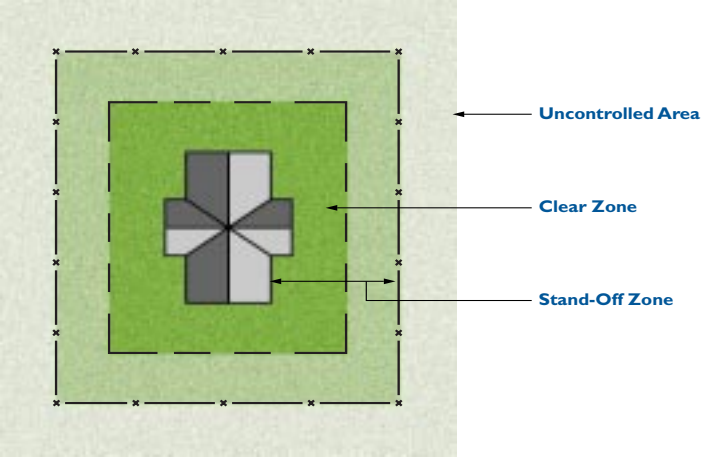


FIGURE 4.10
Clear zone with unobstructed views

B
FACILITY SITE DESIGN TOOLS

1 ORIENTATION OF BUILDINGS ON A SITE

- Deny aggressors a clear "line of sight" to the facility from on- or off-base. *(AFJMAN 32-1071,Vol.1, Ch. 7)*
  - Protect the facility against visual surveillance by aggressors by locating the protected facility outside of the range or out of view of vantage points.
  - Defend against attack by stand-off weapons (antitank weapons, mortars, etc.) by selecting perimeter barriers to block sightlines such as obstruction screens or hedges of trees and shrubs. Non-critical structures or other natural or man-made features can be used to block sightlines. *(AFJMAN 32-1071, Vol. 1, Ch. 7).*
- Create "defensible space" by positioning facilities to permit building occupants and police to clearly monitor adjacent areas.
- If roads are nearby, orient building so that there are no sides parallel to vehicle approach routes. *(AFJMAN 32-1071, Vol. 2, Ch. 3 Vehicle Bombs)*

2 RELATIONSHIP OF ROADS TO AN ASSET

- If possible, choose a site away from main thoroughfares.
- Locate facility away from uncontrolled vehicle access. *(AFJMAN 32-1071, Vol. 2, Ch. 3 Vehicle Bombs)*
- Minimize the number of access roads and entrances into a facility. *(Dod O-2000.12-H, Appendix EE, Table EE-4, Installation Clear and Stand-Off Zones)*

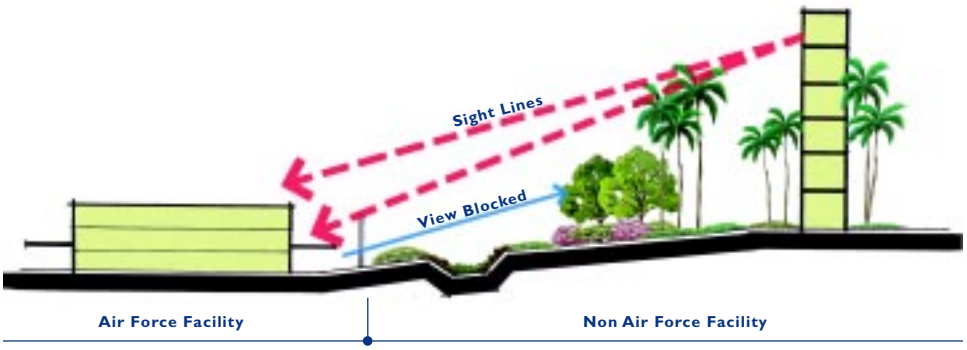
FIGURE 4.11
Blocking sightlines

3 LAND FORMS AND NATURAL RESOURCES

Depending on circumstances, land forms can be either beneficial or detrimental to force protection planning.

- Avoid siting the facility adjacent to:
  - Higher surrounding terrain, which provides easy viewing of the facility
  - Non Air-Force facilities that are unsecured
  - Vegetation, drainage channels, ditches ridges or culverts, which can provide concealment
- Maximize opportunities to use natural terrain features to deflect blasts.

FIGURE 4.12
Improper facility siting and view relationships



- Consider using bodies of water as a design feature to provide a stand-off zone. *(AFJMAN 32-1071, Vol.2, Ch.4)*

4 CONTROL POINTS AND PHYSICAL BARRIERS

- Select and design barriers based on threat levels. (*DoD O-2000.12-H, Appendix EE, Force Protection Design Considerations, par. E, Perimeter Barriers - Vehicle Barriers.)*
- If the limited availability of land precludes the creation of an exclusive zone, the use of screening surrounding the facility can be an alternative. (*AFJMAN 32-1071, Vol. 2, Ch.5)*
- Use a combination of barriers. Some barriers are fixed and obvious (fences and gates), while others are passive (sidewalks far away from buildings, curbs with lawn, etc.). *(DoD O-2000.12-H, Appendix EE, Force Protection Design Considerations, par. E, Perimeter Barriers - Vehicle Barriers.)*
- Where physical barriers are required, consider using landscape materials to create barriers that are soft and naturalistic rather than man-made.
- Vehicles can be used as temporary physical barriers by being placed in front of buildings or across access roads. *(DoD O-2000.12-H, Appendix EE, Force Protection Design Considerations, par. E, Perimeter Barriers - Vehicle Barriers.)*
- Maintain as much stand-off distance as possible between Moving Vehicle Bombs (MVBs) and an asset. (*AFJMAN 32-1071, Vol. 2, Ch. 3)*
  - Provide traffic obstacles near entry control points to slow traffic down. *(AFJMAN 32-1071, Vol. 2, p. 3-19)*
  - Consider vehicle barriers at facility entries and drives. *(AFJMAN 32-1071, Vol. 1, Ch. 3)*

- Offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed.
- When possible, position gates and perimeter boundary fences outside the blast vulnerability envelope.
- If the threat level warrants, provide a vehicle crash resistance system in the form of a low wall or earth berm.
- Consider checkpoints to screen vehicles entering a facility. *(AFJMAN 32-1071, Vol. 2, p. 3-25)*

- Provide passive vehicle barriers to keep Stationary Vehicle Bombs (SVBs) at a distance from the asset.
  - Use high curbs, low berms, shallow ditches, trees, shrubs and other physical separations to keep stationary bombs at a distance. *(AFJMAN 32-1071, Vol. 2, Ch. 3)*
  - Do not allow vehicles to park next to perimeter walls of the secured area. Consider using bollards or other devices to keep vehicles away. *(DoD O-2000.12-H, Ch. 9)*
- Provide adequate lighting to aid in threat detection. *(AFJMAN 32-1071, Vol. 3, Ch. 2)*
- Use closed-circuit television (CCTV) to monitor areas that cannot be staffed constantly. *(AFJMAN 32-1071, Vol. 3, Ch. 2)*

5 LANDSCAPE PLANTING

- Design landscape planting that permits building occupants to see out but does not allow outside monitoring of functions or people inside the building.
  - Vegetation in a clear zone should not exceed four inches in height. *(DoD O-2000.12-H, Appendix EE, Table EE-4)*
  - Use landscape planting appropriately to provide screening to protect the facility without creating concealment for covert activity. Vegetation can have both beneficial and detrimental impacts on security. With proper selection, placement, and maintenance of landscape planting, appropriate screening and greater field of vision can be accomplished.
  - Vegetative groupings and earth sheltering provide inherent blast effect reduction from external blast forces.
  - Minimize potential hiding places through placement of landscape materials, site furnishings, and screening elements for visually detractive elements, e.g., transformers, trash compactors, and condensing units.
- Use dense, thorn-bearing plant materials to create natural barriers to deter aggressors. *(AFJMAN 32-1071, Vol. 3, Ch. 2)*
- Screen play and outdoor recreation areas from public (off-base) view.
- Maximize opportunities to use berms to deflect blasts.
- Minimize signs that identify and locate assets.
- Place trash receptacles as far away from the facility as possible; trash receptacles should not be placed within 30 feet of a facility. *(AFJMAN 32-1071, Vol. 2, Ch. 2)*

6 PARKING

- If possible, do not allow parking beneath the facility. *(AFMAN 32-1071, Vol. 2, Ch.4)*
- If parking beneath a facility is unavoidable, access to the parking should be limited, secure, well lighted, and free of places of concealment.
- Do not authorize vehicles that have not been inspected to park under a building or within the exclusive zone, including at loading docks.
- If possible, locate visitor or general public parking near, but not on, the site itself. *(DoD O-2000.12-H, Ch. 9)*
- Parking within the secured perimeter of an asset should be restricted to employees. *(DoD O-2000.12-H, Ch. 9)*
- Parking should be located in areas that provide the fewest security risks to DoD personnel. *(DoD O-2000.12-H, Ch. 9)*
- One-way circulation within a parking lot can facilitate monitoring for potential aggressors. *(DoD O-2000.12-H, Ch. 9)*
- Locate parking within view of occupied facilities. *(DoD O-2000.12-H, Ch. 9)*
- Restrict parking from the interior of a group of buildings.
- Locate parking and service areas away from high-risk resources. *(Planning Air Bases for Combat Effectiveness, Base Comprehensive Planning Handbook, p. 4-18, b.(1))*
- Restrict parking within the stand-off zone. *(AFJMAN 32-1071, Vol. 2, Ch.4)*
- When establishing parking areas, provide emergency communication systems (intercom, telephones, etc.) at readily identified, well lighted, CCTV monitored locations to permit direct contact with security personnel. *(DoD O-2000.12-H, p. 9-17)*
- Provide parking lots with CCTV cameras and adequate lighting capable of displaying and videotaping lot activity. *(DoD O-2000.12-H, p. 9-18 and GSA Security Criteria, 6.B.1)*

7 SERVICE ACCESS

- Provide signage to clearly mark separate entrances for deliveries, visitors and employees. *(DoD O-2000.12-H, Ch.9)*
- If loading zones or drive-through areas are necessary, monitor them and restrict height to keep out large vehicles.
- Avoid having driveways within or under facilities.

8 SITE UTILITIES

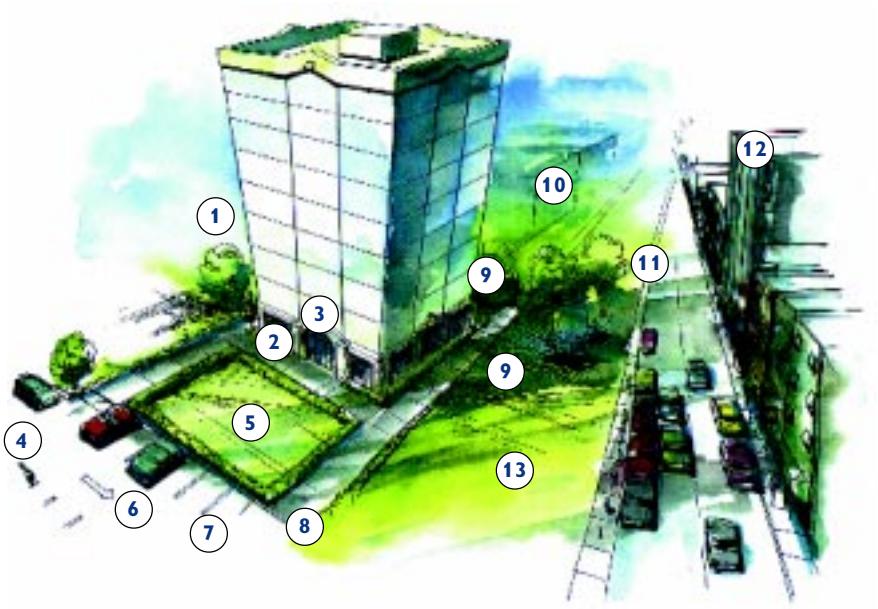
- Provide a site-wide public address system that extends from the interior to the exterior of facilities.
- Where possible, provide underground, concealed, and protected utilities.
- Provide redundant utility systems (particularly electrical services) to support site security, life safety, and rescue functions.
- Consider quick connects for portable utility backup systems if redundant sources are not available.
- Locate fuel storage tanks at least 100 feet from buildings.

TABLE 4.1
Threat & Protective Measures for Facility Site Design

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Ballistics Attack	Covert Entry	Mail & Supplies Bombs	Airborne Contamination	Waterborne Contamination
Distance									
Stand-off zone	■	■		■	■	■			
Exclusive zone/Non-exclusive zone	■	■				■			
Clear zone	■	■				■			
Orientation of Building on a Site									
Protect against unwanted surveillance			■	■	■	■			
"Defensible space"		■	■			■			
Vehicle access	■	■							
Relationship of Roads to an Asset									
Away from main thoroughfares	■	■							
Away from uncontrolled vehicle access	■	■	■						
Minimize access roads	■	■				■	■		
Land Forms and Natural Resources									
High surrounding terrain			■	■	■				
Distance from non-Air Force facilities	■	■	■	■	■	■		■	■
Areas which provide concealment		■	■	■	■	■			
Earth berms		■	■	■	■				
Bodies of water	■	■	■	■	■	■			
Depressions			■	■	■				
Control Points and Physical Barriers									
Control points	■	■	■	■	■	■			
Active barriers	■	■	■	■	■	■			
Passive barriers	■	■	■			■			
Lighting		■	■			■			
Active monitoring	■	■	■	■	■	■	■	■	■
Landscape Planting									
Dense thorn-bearing vegetation			■			■			
Vegetation screens		■	■	■	■	■			
Minimize signage	■	■	■	■	■	■	■	■	■
Location of trash receptacles							■		
Parking									
View of parking		■							
Parking under a building		■							
Parking at interior of facility		■							
Parking near high-risk areas		■							
Parking in exclusive zone		■							
One-way circulation	■	■	■			■			
Service Access									
Loading/unloading docks		■					■		
Driveways under facilities	■	■							
Site Utilities									
Public address system			■		■			■	■
Underground utlities	■	■	■	■					■
Redundant utlities	■	■	■	■	■				■
Quick connects	■	■	■	■	■				
Remote fuel storage	■	■	■	■	■				

■ **The symbols indicate which of the protective measures shown in the left-hand column can be effective in countering the types of threats indicated across the top of the chart.**

FIGURE 4.13
Elements of Minimum Protection for Site Design



1 Locate assets stored on site but outside of the facility within view of occupied rooms in the facility

2 Eliminate parking beneath facilities

3 Minimize exterior signage or other indications of asset locations

4 Locate trash receptacles as far from the facility as possible

5 Eliminate lines of approach perpendicular to the building

6 Locate parking to obtain stand-off distance from facility

7 Illuminate building exteriors or sites where exposed assets are located

8 Minimize vehicle access points

9 Eliminate potential hiding places near facility; provide an unobstructed view around facility

10 Site facility within view of other occupied facilities on the installation

11 Maximize distance from facility to installation boundary

12 Locate facility away from natural or man-made vantage points

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

CHAPTER 5

BUILDING SYSTEMS DESIGN

After all appropriate force protection measures have been considered at the comprehensive planning and site design level, measures must be considered to protect the ultimate terrorist target: the personnel within the facility. The measures described in this chapter are designed to minimize vulnerability to attack and loss of life through deterrence and detection and strengthening of the building against a variety of terrorist tactics. The design team must determine which measures are appropriate and cost effective to incorporate into the design. The designer must balance force protection measures with the requirements of the Americans with Disabilities Act Accessibility Guidelines (ADAAG), Uniform Federal Accessibility Standards (UFAS), National Fire Protection Codes (NFPA), and all applicable local building codes. The Installation Security Council should review all force protection measures incorporated into building systems design.

Since facilities occupied by Air Force personnel are often contained within a DoD or other U.S. Government installation, the physical security system for a facility can be structured to take full advantage of security resources already in place. Those facilities located outside a DoD or U.S. Government installation require more substantial local physical force protection measures for a given level of terrorist threat than comparable facilities located within a DoD or U.S. Government installation.

This chapter addresses building systems and their components. The force protection measures described are organized by building systems that correlate to design disciplines:

- Architectural
- Interior Design
- Structural
- Mechanical
- Electrical.

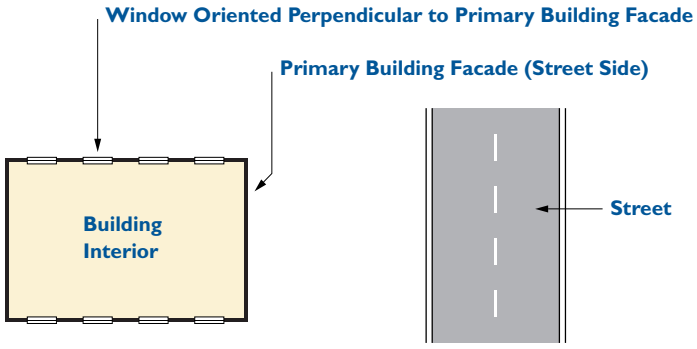
From a force protection standpoint, the primary goals of building systems design are two: 1) design a safe building that will not fail when attacked, and 2) permit rescue teams to evacuate victims during rescue operations. Some force protection measures may conflict with others. The relative risk and benefit of these guidelines vary based upon the asset and threat. The measures described here are not all-inclusive, and additional technical information for implementation can be found in the referenced documents.

For a graphic illustration of the relationship between protective measures and potential threats, refer to the matrix provided at the end of this chapter. The matrix summarizes the building systems design measures presented in this chapter and indicates their effectiveness against the potential aggressor tactics discussed in Chapter Two.

1 BUILDING FORM

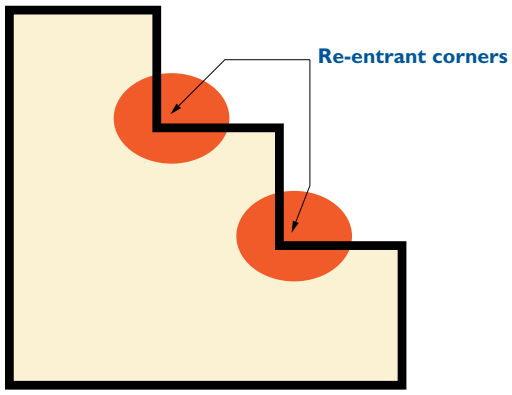
- Consider earth-sheltered design to reduce the asset's vulnerability to attack.
- Orient buildings horizontally rather than vertically to reduce the building's profile and exposure.
- Place the ground floor elevation of a building at four feet above grade to prevent vehicles from being driven to and into the facility.
- Avoid eaves and overhangs, since these can be points of high local pressure and suction during blasts. When these elements are used, they must be designed to withstand blast effects.
- Orient glazing perpendicular to the primary facade to reduce exposure to blast and projectiles.

FIGURE 5.1
Glazed areas



- Avoid having exposed structural elements such as columns on the exterior of the facility.
- Provide pitched roofs to allow launched explosives to roll off of the facility.
- Avoid re-entrant corners on the building exterior where blast pressures may build up.

FIGURE 5.2
Re-entrant corners

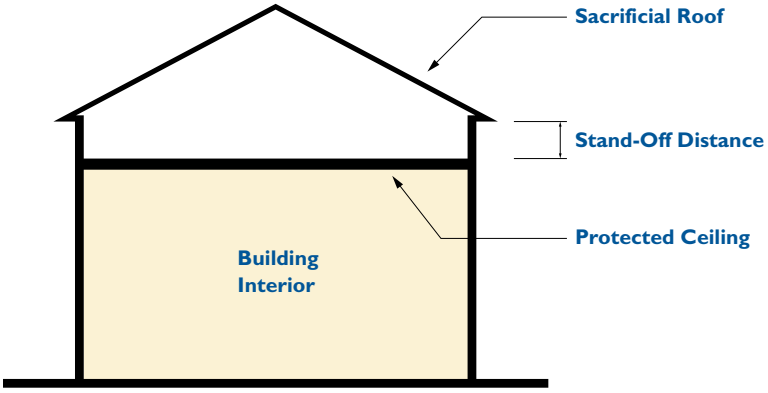


2 EXTERIOR ENVELOPE

- Substitute strengthened building elements and systems when stand-off distances cannot be accommodated.
- Use ductile materials that are capable of very large plastic deformations without complete failure.

- Make roof access hatches securable from the interior.
- Provide blast-resistant walls when a high threat is present.
- Design facilities with a sacrificial sloping roof that is above a protected ceiling. *(AFJMAN 32-1071,Vol. 2, Ch. 4, Table 4-1)*

FIGURE 5.3
Sacrificial roof

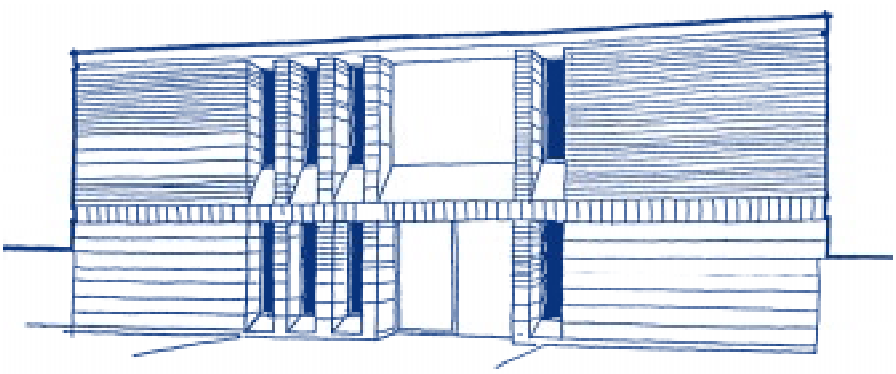


- Consider use of sacrificial exterior wall panels to absorb blast.
- Use earthtone-colored materials and finishes on exterior surfaces to diminish the prominence of a building.
- Consider reinforced concrete wall systems in lieu of masonry or curtain walls to minimize flying debris in a blast.
- Reinforced wall panels can protect columns and assist in preventing progressive collapse, as the wall will assist in carrying the load of a damaged column.

3 WINDOWS

- Eliminate windows adjacent to doors because the windows can be broken, allowing the door to be unlocked.
- Minimize the number and size of windows in a facade. If possible, limit the amount of glazed area in building facades to 15 percent. The amount of blast entering a space is directly proportional to the amount of opening on the facade.
- Consider using burglary- and ballistic-resistant glazing in high-threat areas.
- Consider using laminated glass in place of conventional glass.
- Consider window safety laminate (such as mylar) or another fragment-retention film over glazing (properly installed) to reduce fragmentation. *(AFJMAN 32-1071, Vol. 2, p. 4-5)*
- Consider placing guards, such as grills, screens, or meshwork, across window openings to protect against covert entry. Affix protective window guards firmly to the structure.
- Consider curtains, blinds and shades to limit entry of incendiary devices.
- Narrow recessed windows with sloped sills are less vulnerable than conventional windows. *(AFJMAN 32-1071, Vol. 2, Ch. 4)*

FIGURE 5.4
Narrow and recessed windows



- Windows with key-operated locks provide a greater level of protection than windows with simple latches. Stationary, non-operating windows are preferred for security. *(DoD O-2000.12-H, Ch. 10 and Appendix E, Lock Security)*
- The operable section of a sliding window should be on the inside of the fixed section and secured with a broomstick, metal rod or similar device placed at the bottom. *(DoD O-2000.12-H, Ch. 10 and Appendix E, Lock Security)*
- Provide horizontal windows six feet above the finished floor to limit entry.
- Windows can be hardened by steel window frames securely fastened or cement grouted to the surrounding structure.

4 DOORS

- Provide hollow steel doors or steel-clad doors with steel frames.
- Provide blast-resistant doors for high threats and high levels of protection.
- Permit normal entry/egress through only one door, if possible.
- Limit exterior doors to a minimum while accommodating emergency egress. Doors are less attack-resistant than adjacent walls because of functional requirements, construction, and method of attachment. *(DoD O-2000.12-H, Ch. 10 and Appendix E, Lock Security)*
- The weakest part of a door system is the latching component. Replace externally mounted locks and hasps with internally locking devices. *(DoD O-2000.12-H, Ch. 10 and Appendix E, Lock Security)*
- Where practical, doors should present blank, flush surfaces to the outside to reduce their vulnerability to attack.
- Locate hinges on interior or provide concealed hinges to reduce their vulnerability to attack. *(DoD O-2000.12-H, Ch. 10 and Appendix E, Lock Security)*
- Emergency exit doors should only facilitate exiting movement.
- Equip any outward-opening double door with protective hinges and key-operated mortise-type locks.
- Provide solid doors or walls as a back-up for glass doors in foyers.
- Strengthen and harden the upright surfaces of a door jamb into which the door fits.

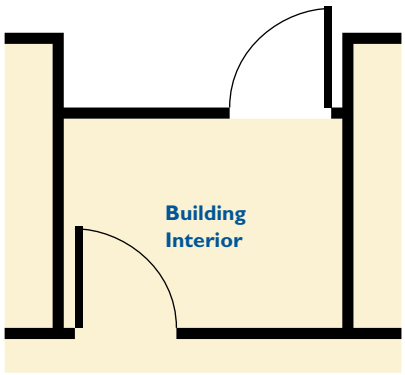
5 MISCELLANEOUS

- Make roof access ladders removable, retractable or lockable.
- Protect utility openings to a facility from covert entry by installing screens or grates or attaching intrusion detection systems (IDS) sensors. *(DoD O-2000.12-H, p. 9-19)*

1 SPACE PLANNING

- High-risk facilities should not be co-located with lower risk tenants. For example, a post office or supply center/room should not be located in the same building as a childcare facility. *(GSA Security Criteria, 1.H and AFJMAN 32-1071, Vol. 1, Ch. 11, Mail and Supplies Bomb Delivery Tactics)*
- Locate assets as far into the interior of a facility as possible.
- Place mailrooms on the perimeter of a facility to minimize the damage caused by a mail bomb. Also, consider hardening the walls and ceiling of mailrooms.
- Place areas of high visitor activity away from assets.
- Locate critical assets in spaces that are occupied 24 hours per day.
- Locate assets in areas where they are visible to more than one person.
- Eliminate hiding places within the building.
- Use interior barriers to differentiate levels of security within a facility. (*DoD O-2000.12-H, Ch.10)*
- Stagger doors located across from one another in interior hallways to limit the effects of a blast through a structure.
- Provide foyers with reinforced concrete walls, and offset interior and exterior doors from each other in the foyer. *(AFMAN 32-1071, Vol. 2 Ch. 3)*

FIGURE 5.5
Foyer design



- The innermost layer of protection within a physical security system is the *safe haven*. Safe havens are not intended to withstand a disciplined, paramilitary attack featuring explosives and heavy weapons. The safe haven should be designed such that the time that attackers need to penetrate the protected area is greater than the time that response forces need to reach the protected area. *(DoD O-2000.12-H, Ch. 10 and Appendix EE, Force Protection Design Considerations)*

2 DETAILING

- Minimize interior glazing near high-threat areas.
- Connect interior non-load bearing walls to structure with non-rigid connections. *(AFJMAN 32-1071, Vol. 2, Ch. 4)*
- Interior walls should be painted in light colors to improve illumination. *(GSA Security Criteria, 3.A.8)*
- At windows, consider blast curtains or heavy drapes in high-threat areas.

3 CIRCULATION

- Design circulation routes to provide unobstructed views of people approaching controlled access points.
- Consider the use of access controls, such as a card key locking system, into secured areas of the facility. *(GSA Security Criteria, 3.C.3)*
- Pedestrian paths should be planned to concentrate activity to aid in detection. *(GSA Security Criteria, 3.A.5 and AFJMAN 32-1071, Vol. 2, Ch, 3)*
- Consider the use of access controls from one area of the facility to another to slow down intruders. This will provide more time for security to react. A combination of programmable magnetic swipe cards and personal identification numbers (PIN) is more secure than either a PIN or swipe card used alone.

4 SIGNAGE

- Consider using street addresses or building numbers in lieu of detailed descriptive information.
- Post clear signs to minimize accidental entry by unauthorized personnel into critical asset areas.
- Eliminate or minimize signage identifying critical facilities to downplay their critical nature.

- Buildings should be designed against progressive collapse. *(GSA Security Criteria, 4.B.1 and U.S. Dept. of State, Bureau of Diplomatic Security, Structural Engineering Guidelines for New Embassy Office Buildings)*
- Structural damage without collapse of the facility is an acceptable and practical design parameter. *(AFMAN 32-1071, Vol. 2, Ch. 3,4 and U.S. Dept. of State, Bureau of Diplomatic Security, Structural Engineering Guidelines for New Embassy Office Buildings)*
- Consider incorporating internal damping into the structural system to absorb the blast impact. *(AFMAN 32-1071, Vol. 2, Ch. 3,4 and U.S. Dept. of State, Bureau of Diplomatic Security, Structural Engineering Guidelines for New Embassy Office Buildings)*
- Symmetric reinforcement can increase the ultimate load capacity of the structure. *(GSA Security Criteria, 4.E.2 and U.S. Dept. of State, Bureau of Diplomatic Security, Structural Engineering Guidelines for New Embassy Office Buildings)*
- Ductile details should be used for structural connections to absorb the energy of a blast. (Many times the ductile detailing requirements for seismic design can help prevent progressive collapse after a bomb attack.) *(U.S. Dept. of State, Bureau of Diplomatic Security, Structural Engineering Guidelines for New Embassy Office Buildings)*

- Redundancy and alternative load paths can help mitigate blasts and reduce the chance of progressive collapse. *(GSA Security Criteria, 4.E.2)* The Murrah Federal Building's structural system did not have any redundancy for the slab and beam systems. *(U.S. Dept. of State Structural Engineering Guidelines for New Embassy Office Buildings)*
- Strengthening the structural system can help in resisting the effects of a blast.
- Consider wire mesh in plaster to reduce the incidence of flying fragments.
- Avoid the use of masonry when blast is a threat. Masonry walls break up readily and become secondary fragments during blasts. *(DoD O-2000.12-H, Appendix DD, Calculated and Analyzed Blast Effects)*
- The use of multiple barrier materials and construction techniques can sometimes accomplish the same goal with less expense than a single material or technique.

D
MECHANICAL

- The primary goal of a mechanical system after a terrorist attack should be to continue to operate key life safety systems.
- Mechanical penetrations through exterior walls, such as intake louvers, should be mounted as high as possible to minimize their vulnerability. *(GSA Security Criteria, 5.A.1 and AFJMAN 32-1071, Vol. 3, Ch. 8)*
- Do not mount plumbing, electrical fixtures or utility lines on the inside of exterior walls. When mounting along exterior walls is unavoidable, mount fixtures on a separate wall at least six inches from the exterior wall face.
- Avoid placing plumbing on the roof slab.
- Avoid suspending plumbing fixtures and piping from the ceiling.
- Reduce the number of utility openings, manholes, tunnels, air conditioning ducts, filters, and access panels into the structure.
- Locate utility systems away from likely areas of attack, such as loading docks, lobbies, and parking areas. *(GSA Security Criteria, 5.B.1 and AFJMAN 32-1071, Vol. 3, Ch. 8)*
- Protect building operational control areas and utility feeds to lessen the negative effects of a blast.
- Design operational redundancies to survive all kinds of attack.
- Use lockable systems for utility openings and manholes where appropriate. Infrequently used utility covers/manholes can be tack-welded as an inexpensive alternative to locking tamper-resistant covers.
- Depending on assessed level of threat, install either a manually activated or a continuously active air filtration system to reduce the risk from airborne contaminants. (*AFJMAN 32-1071 Vol.2, par. 10-3)*

E
ELECTRICAL

- Use electronic systems for intrusion detection, access control, and assessment such as door alarms and CCTV when appropriate.
- Illuminate building access points to aid in threat detection. (AFJMAN 32 1071, Vol. 2, Ch. 4 and DoD O-2000.12-H, Ch. 8)
- Self-contained battery lighting should be provided in stairwells and for exit signs. (GSA Security Criteria, 6.B.3 and DoD O-2000.12-H, Ch. 8)

- Avoid suspending electrical conduit from the ceiling.
- Consider using manually activated duress alarms. An audible alarm can frighten away an intruder.
- Provide secured dedicated telephone lines between secured areas and security response force.
- Provide a manually activated and controlled warning and evacuation system. This can consist of warning systems that can ring in short bursts as a warning to evacuate the building in the event of an impending explosion.
- Provide security monitoring through closed-circuit television systems (CCTV).
- Provide adequate lighting of perimeters and parking areas to aid in visual surveillance and to support the use of CCTV.
- Provide an internal public address system.
- When risks are high, consider the use of x-ray screening systems in mailrooms and at supply facilities.

TABLE 5.1
Threat & Protective Measures for Building Systems

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Ballistics Attack	Covert Entry	Mail & Supplies Bombs	Airborne Contamination	Waterborne Contamination
ARCHITECTURAL									
Building Form									
Earth sheltered design	■	■	■	■	■				
Horizontal building orientation	■	■	■	■	■				
Elevated ground floor	■		■						
Avoid eaves & overhangs	■	■	■						
Windows perpendicular to facade	■	■	■	■	■		■		
Avoid exposed structural elements	■	■	■	■			■		
Pitched roofs			■	■	■	■			
Avoid re-entrant corners	■	■	■	■			■		
Facade setbacks	■	■	■	■			■		
Exterior Envelope									
Ductile materials	■	■	■	■			■		
Secure roof hatches			■			■			
Secure roof access ladders			■			■			
Blast resistant walls	■	■	■				■		
Avoid masonry	■	■	■	■			■		
Sacrificial wall panel	■	■	■	■			■		
Sacrificial roof	■	■	■	■			■		
Windows									
No windows adjacent to doors			■	■	■	■			
Limit glazed area to 15% of total area	■	■	■	■	■	■	■	■	■
Fragment retention film on glass	■	■	■	■			■		
Alternative glazing	■	■	■	■	■		■		
Guards across windows			■			■			
Minimize number & size of windows	■	■	■	■	■	■	■	■	■
Skylights	■	■	■	■			■		
Narrow recessed windows	■	■	■	■			■		
High horizontal windows	■	■	■	■			■		
Reinforced window frames	■	■	■	■	■	■	■		
Doors									
Steel doors & frames	■	■	■	■	■		■		
Blast-resistant doors	■	■	■	■			■		
Minimize number of exterior doors	■	■	■	■		■	■	■	■
Backups to glass foyer doors	■	■	■	■	■	■	■		

TABLE 5.1
Threat & Protective Measures for Building Systems *continued*

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Ballistics Attack	Covert Entry	Mail & Supplies Bombs	Airborne Contamination	Waterborne Contamination
INTERIOR									
Space Planning									
Assets located toward interior	■	■	■	■	■	■		■	■
Building layout to minimize blast effects	■	■		■		■	■		
Mailroom on perimeter			■				■		
Separate visitor activity from assets		■	■			■	■		
Critical assets in occupied space		■	■			■	■		
Critical assets where visible	■	■	■			■	■		
Eliminate hiding places		■				■			
Foyers with offset doors, reinforced walls	■	■	■	■	■		■		
Unobstructed views, controlled access	■	■	■			■	■		
Safe haven	■	■		■		■		■	■
Detailing									
Non-rigid connections of partitions	■	■		■			■		
Heavy curtains or drapes	■	■	■	■		■	■		
Minimize interior glazing	■	■					■		
Signage									
Use numbers rather than names	■	■	■	■	■	■	■		
Use signs to limit accidental entry			■			■			
Minimize identification of critical facilities	■	■	■	■	■	■	■		
STRUCTURAL									
Design against progressive collapse	■	■		■			■		
Symmetric reinforcement	■	■		■			■		
Ductile detailing	■	■		■			■		
Reinforce structure around windows	■	■	■	■			■		
Internal damping	■	■		■			■		
Wire mesh in plaster	■	■		■			■		
Added reinforcement in masonry	■	■	■	■			■		
MECHANICAL									
Raise mechanical penetrations	■	■	■			■		■	
Avoid locating fixtures on exterior walls	■	■	■			■		■	
Minimize utility exposure	■	■	■	■		■		■	■
Air filters								■	
ELECTRICAL									
Intrusion detection systems			■			■	■		
Illuminate access points	■	■	■			■	■		

■ **The symbols indicate which of the protective measures shown in the left-hand column can be effective in countering the types of threats indicated across the top of the chart.**

GLOSSARY

Antiterrorism Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

Antiterrorism Awareness Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism. See also antiterrorism.

Area Commander A Military Service-designated commander with authority in a specific geographical area.

Area of Responsibility The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. Also called AOR.

Asset Any potential target of terrorist attack, most commonly people, equipment, a building, or an outdoor venue (in whole or in part).

Blast Curtains Heavy curtains made of blast resistant materials that could protect the occupants of a room from flying debris.

Blast Vulnerability Envelope The resources around an explosive device that will be damaged by the blast.

Clear Zone An area that is clear of visual obstructions and landscape materials that could conceal a threat or perpetrator.

Commander Any commanding officer, installation commander, or other appropriate command authority, or civilian supervisor in a comparable position.

Counterintelligence Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs.

Counterterrorism (CT) Offensive measures taken to prevent, deter, and respond to terrorism.

Domestic Terrorism Terrorism perpetrated by the citizens of one country against fellow countrymen. That includes acts against citizens of a second country when they are in the host country, and not the principal or intended target.

Ductile Materials Materials that are malleable and will absorb impact loads without breaking.

Electronic Security Systems (ESS) That part of physical security concerned with the safeguarding of personnel and property by use of electronic systems. These systems include, but are not limited to, intrusion detection systems (IDS), automated entry control systems (AECS), and video assessment systems.

Exclusive Zone An area around an asset which has controlled entry with highly restrictive access.

Force Protection Security program designed to protect Air Force personnel, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

High-Risk Target Any U.S. material resource or facility that, because of mission sensitivity, ease of access, isolation, and symbolic value, may be an especially attractive or accessible terrorist target.

Installations Air Force including bases, stations, and annexes (both contractor and Government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes. Also includes any activity of the Air Force that employs members of the work force in peacetime or will employ them in the event of mobilization.

Internal Damping Anything that absorbs some or all of the impact from a blast.

Military Facility A facility subject to the custody, jurisdiction, or administration of any DoD Component. This term includes, but is not limited to, military reservations, installations, bases, posts, camps, stations, arsenals, or laboratories where a DoD Component has operational responsibility and has responsibility for facility security and defense.

Non-Exclusive Zone An area around an asset that has controlled entry but less restrictive access than a exclusive zone.

Nuclear, Biological or Chemical Weapons (NBC) Also called Weapons of Mass Destruction (WMD). Weapons that are characterized by their capability to produce mass casualties.

Physical Security The part of security concerned with measures/concepts designed to safeguard personnel; to prevent unauthorized access to equipment, installations, materiel, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Sacrificial Roof or Wall Walls or roofs that can be lost in a blast without damage to the primary asset.

Safe Haven Secure areas within the interior of the facility. A Safe Haven should be designed such that it requires more time to penetrate by terrorist than it takes for the response force to reach the protected area to rescue the occupants.

Stand–off Weapons Weapons that are launched from a distance at a target (anti-tank weapons, mortars, etc.).

Stand-off Distance The distance between an asset and a threat.

Terrorism 1. The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. 2. The unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives.

Threat Analysis In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment. See also antiterrorism.

Vulnerability 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment.

BIBLIOGRAPHY

FEDERAL GUIDANCE

- GSA *Security Criteria,* Final Working Version 17 June 1997 (Limited official use only)
- U.S. Department of State, Bureau of Diplomatic Security, *Structural Engineering Guidelines for New Embassy Office Buildings* (Limited official use only), August 1995
- U.S. Department of State, Bureau of Diplomatic Security, *Physical Security Standards Handbook,* 7 January 1988 (Limited official use only)

DEPARTMENT OF DEFENSE GUIDANCE

- DoD Directive 2000.12, *DoD Combating Terrorism Program,* 15 September 1996
- DoD Instruction 2000.16, *DoD Combating Terrorism Program Standards,* 21 July 1997
- DoD Instruction 2000.14, *DoD Combating Terrorism Program Procedures,* 15 June 1994
- DoD Instruction 4270.1, *Planning, Design, Engineering, and Construction of Facilities,* August 1997 [draft] (Replaces MIL-HDBK 1190, *Facility Planning and Design Guide*)
- DoD O-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence: Mandatory Standards and Implementing Guidance,* February 1993, with change 1 dated 21 May 1993 and change 2 dated 21 July 1997
- DoD 5200.1R, *DoD Information Security Program Regulation*
- DoD 5200.8R, *Physical Security Program Regulation*
- DoD *Report to the President: The Protection of U.S. Forces Deployed Abroad,* 15 September 1996
- FM 5-114, *Engineer Operations Short of War*
- FM 100-37, *Terrorism Counteraction,* 1987
- MIL-HDBK 1013/1A, *Design Guidelines for Physical Security of Fixed Land-Based Facilities,* October 1987
- Naval Civil Engineering Laboratory (NCEL), *Terrorist Vehicle Bomb Survivability Manual (Vehicle Barriers),* March 1986
- *Remarks by General John M. Shalikashvili, Chairman, Joint Chiefs of Staff, to the Joint Staff and Defense Special Weapons Agency, Force Protection Symposium,* 19 November 1996
- TM 5-853 Vol 4, *Security Engineering, Electronic Security Systems,* 12 May 1994
- Wright Laboratory Report, *Expedient Hardening Methods for Structures Subjected to the Effect of Nonnuclear Munitions,* October 1990

AIR FORCE GUIDANCE

- AFH 10-222, Vol 3, *Guide to Civil Engineer Force Protection,* 1 June 1997 [draft]
- AFH 31-223, *The Air Force Resource Protection Program,* February 1997
- AFH 32-1084, *Standard Facility Requirements Handbook,* July 1994
- AFI 31-101, Vol 1, *The Air Force Physical Security Program,* December 1996
- AFI 31-209, *The Air Force Resource Protection Program,* 10 November 1994
- AFI 31-210, *The Air Force Antiterrorism (AT) Program*, 1 July 1995
- AFI 32-1021, *Planning and Programming of Facility Construction Projects,* May 1994
- AFI 32-1024, *Standard Facility Requirements,* 31 May 1994
- AFI 32-1032, *Planning and Programming Real Property Maintenance Projects Using Appropriated Funds (APF),* May 1994
- AFI 32-7062, *Air Force Comprehensive Planning,* April 1994
- AFJMAN 32-1055, Design and Analysis of Hardened Structures to Conventional Weapons Effect, April 1997 [draft]
- AFJMAN 32-1071, Vol 1, *Security Engineering Project Development,* 12 May 1994
- AFJMAN 32-1071, Vol 2, *Security Engineering Concept Design,* 12 May 1994
- AFJMAN 32-1071, Vol 3, *Security Engineering Final Design,* 12 May 1994
- AMC *Flightline Security Standards,* April 1996
- AMC *Passenger Terminal Design Guide* [draft]
- Air Force Office of the Civil Engineer memo, *Anti-terrorism (AT) Protective Features for Facilities and Installations*, 2 December 1996
- *Area Development Planning Bulletin,* October 1991
- Base Comprehensive Planning Handbook, *Planning Airbases for Combat Effectiveness,* December 1993
- ETL 86-10, *Antiterrorism Planning and Design Guidance,* 13 June 1986
- ETL 90-3, *TEMPEST Protection for Facilities,* 23 March 1990
- ETL 91-2, *High Altitude Electromagnetic Pulse,* 4 March 1997