Protection of Federal Office Buildings Against Terrorism

Committee on the Protection of Federal Facilities Against Terrorism, Building Research Board, National Research Council

ISBN: 0-309-56955-9, 60 pages, 6 x 9, (1988)

Protection of Federal Office Buildings Against Terrorism

Committee on the Protection of Federal Facilities Against Terrorism
Building Research Board
Commission on Engineering and Technical Systems
National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C. 1988

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competencies and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

The National Academy of Sciences is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Frank Press is president of the National Academy of Sciences.

The National Academy of Engineering was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Robert M. White is president of the National Academy of Engineering.

The Institute of Medicine was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government, and upon its own initiative, to identify issues of medical care, research, and education. Dr. Samuel O. Thier is president of the Institute of Medicine.

The National Research Council was established by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and of advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Frank Press and Dr. Robert M. White are chairman and vice chairman, respectively, of the National Research Council.

This report was prepared as part of the technical program of the Federal Construction Council (FCC). The FCC is a continuing activity of the Building Research Board, which is a unit of the Commission on Engineering and Technical Systems of the National Research Council. The purpose of the FCC is to promote cooperation among federal construction agencies and between such agencies and other elements of the building community in addressing technical issues of mutual concern. The FCC program is supported by 14 federal agencies: the Department of the Air Force, the Department of the Army, the Department of Commerce, the Department of Energy, the Department of the Navy, the Department of State, the General Services Administration, the National Aeronautics and Space Administration, the National Endowment for the Arts, the National Science Foundation, the U.S. Postal Service, the U.S. Public Health Service, the Smithsonian Institution, and the Veterans Administration.

Funding for the FCC program was provided through the following agreements between the indicated federal agency and the National Academy of Sciences: Department of State Contract No. 1030-621218; National Endowment for the Arts Grant No. 42-4253-0091; National Science Foundation Grant No. MSM-8600676, under master agreement 82-05615; and U.S. Postal Service grant, unnumbered.

For information regarding this document, write the Director, Building Research Board, National Research Council, 2101 Constitution Avenue, Washington, DC 20418.
Printed in the United States of America

BUILDING RESEARCH BOARD 1986-87

COMMITTEE ON THE PROTECTION OF FEDERAL FACILITIES AGAINST TERRORISM

Chairman

C. CHRISTOPHER DEGENHARDT, EDAW, Inc. San Francisco, California

Members

ROBERT A. CRIST, Wiss, Janney, Elstner Associates, Inc., Northbrook, Illinois
ROBERT A. DIERKER, Smithsonian Institution, Washington, D.C.
ROBERT W. MARANS, University of Michigan, Ann Arbor
PETER A. MICHEL, President, Brink's Home Security, Dallas, Texas
JOHN C. PIGNATO, Security Consultant, Groton, Massachusetts
WILLIAM L. PULGRAM, Associated Space Design, Inc., Atlanta, Georgia

Liaison Representatives

DONALD B. BALDWIN, U.S. Army Corps of Engineers, Washington, D.C.
ANTHONY BROWN, Naval Facilities Engineering Command, Alexandria, Virginia
MANMOHAN CHAWLA, General Services Administration, Washington, D.C.
ROBERT DIKKERS, National Bureau of Standards, Gaithersburg, Maryland
ROBERT J. FURLONG, U.S. Air Force, Washington, D.C.
TONY D. HINSON, Naval Facilities Engineering Command, Alexandria, Virginia
PATRICK LINDSEY, U.S. Army Corps of Engineers, Omaha, Nebraska
VINCE McCELLAND, U.S. Department of Energy, Washington, D.C.
WILLIAM STRICKLAND, U.S. Air Force, Tyndall AFB, Florida

Staff

JOHN P. EBERHARD, Director
PETER H. SMEALLIE, Project Director
DONNA F. ALLEN, Senior Secretary

Preface

By itself, the word terrorism connotes fear, violence, anger and frustration. Taken alone, terrorist attacks seem senseless, sudden, isolated and often, bloody. However, as a form of political warfare involving violence or the threat of violence, terrorism today is a recognized international phenomenon against which governments must institute protective measures.

Continued attacks during the 1970s and early 1980s against U.S. embassy buildings and personnel abroad led the U.S. Department of State to propose in 1985 a massive new construction program to build a new generation of secure embassy buildings. The Building Research Board of the National Research Council advised the State Department on new design criteria to integrate state-of-the-art security considerations with the unique design requirements of embassy buildings (National Research Council, 1986).

Participating in this year-long study were representatives from many of the 14 federal agencies of the Building Research Board's Federal Construction Council (FCC). Most, if not all, of the FCC agencies have some type of facility security program. By and large, these security programs are designed to protect against theft, vandalism and other types of transgressions. They are not necessarily directed against the occurrence of a terrorist act.

Recognizing this, the FCC asked the National Research Council to establish a committee of experts to develop a report that addresses measures and techniques to protect federal buildings, and the people and information within them, against acts of terrorism.

A primary purpose of this report is to stimulate and raise the awareness of owners and managers of federal buildings of the necessity for protective measures against terrorism. Addressing security is analogous to addressing the design of buildings to resist the effects of earthquakes where similar levels of risk exist. The risk may appear low or even negligable, but the consequences of even one severe occurence are so great that appropriate mitigating measures must be considered.

NOTE

National Research Council. 1986. The Embassy of the Future: Recommendations for the Design of Future U.S. Embassy Buildings, Washington, D.C.: National Academy Press.

Contents

Summary

In response to a request from the 14 agencies that comprise the Federal Construction Council, the Building Research Board established a committee of experts (including professionals in the fields of physical security, architecture, landscape architecture, urban planning, law, engineering, and behavioral research) to develop guidance for federal agencies to improve the security of persons, buildings, and information from terrorist attack. To do this, the committee first limited the scope of its concerns to existing federal office buildings (or similar types of facilities). It reviewed the history of terrorist attacks against federal facilities in this country and developed a methodology for assessing threats and analyzing a building's vulnerability. The committee developed security guidelines for buildings and sites, as well as guidelines for security management including guidelines for scaling back or removing security measures.

This report is directed primarily at the management of the Federal Construction Council agencies and, to a lesser extent, at the managers of individual facilities. While the report may be of interest to security specialists, the material is not intended to educate or convey state-of-the-art information to professionals in the security field.

As such, this committee offers the following recommendations:

1. An ongoing security program should be developed and implemented by agencies that own or lease federal office buildings.
2. Top management should be responsible for security policy and implementation.
3. Security strategies should be developed with a clear understanding and assessment of the threat.
4. A formal means of threat communication should be established.
5. Every federal office building should undergo a vulnerability analysis.
6. A base line or minimum level of protection should be established for each federal office building.
7. Temporary protective measures should be systematically reviewed.

1

Federal Office Buildings and the Threat of Terrorism

TERRORISM

The Federal Bureau of Investigation (FBI) defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (FBI, 1984). Within the FBI, terrorism is described as either domestic or international depending on the origin, base, and objectives of the terrorist organization. The Committee on the Protection of Federal Facilities Against Terrorism accepts this definition and, for purposes of this study, has limited its attention to terrorist attacks or the threat of terrorism within the United States, its territories, and its protectorates.

Terrorist Activity in the United States

The FBI indicated to the committee that terrorist activity in the United States today is considered low—both statistically and in terms of media attention—compared with terrorist activity in the early 1980s. In 1986 there were 17 domestic U.S. terrorist incidents. Of the 17 incidents in 1986, 10 involved bombings against buildings (9 of the 10 bombings were in Puerto Rico,

and 8 of these 9 were against federal facilities.) The number of international incidents—incidents with foreign involvement— that occurred in the United States in 1986 was low, with no bombings. However, in 1986 the level of anxiety and concern about terrorism was high within the government and the public at large, especially after the April 1986 raid on Libya by U.S. armed forces in retaliation for the bombing of a Berlin nightclub.

After review of the statistical evidence of terrorist activities against domestic federal facilities over the past several years, the committee observed that terrorist activities in this country exhibit a peak and valley pattern. The committee agreed that to base its findings and advice on the recent dearth of terrorist activities in this country would not be a wise course of action. However, the committee did learn that terrorist acts around the world are getting more violent and are claiming more lives, for example, incidents of suicidal truck bombs in the Middle East or embassy bombings. Therefore, the committee concluded that the consequences of even a single act of terrorism against an occupied federal building are significant enough to warrant action.

The committee also concluded that some anti-terrorist measures could be reversible or temporary, and should therefore be reviewed periodically. The committee has phrased its advice in these terms.

FOCUS OF THE COMMITTEE'S EFFORTS

The original charge to the committee included developing recommendations for security-related design criteria for new federal facilities, as well as procedures for enhancing the security of existing facilities. At its first meeting in March 1987, the committee heard presentations from federal liaison representatives (see committee list, page iv) that led the committee to conclude that the greatest need for advice concerned how to improve security in the great number of existing federal office buildings in the United States.

The committee confined its focus to existing federal office buildings or similar types of structures that house U.S. government workers and that have requirements for public access. For example, a government supply warehouse is outside the scope of the committee's effort because it has limited, if any, public access and its primary function is not to house government workers.

However, an administrative building connected to or nearby the warehouse is covered. Military bases and other secure facilities are outside the scope of this report, except in cases of public access on a military base, such as a visitors center. However, the committee believes that the information in this report probably has a bearing on security of all structures. The committee and staff maintained close association with a similar effort being undertaken by the U.S. General Accounting Office (GAO) that is evaluating anti-terrorism measures for mass transit facilities and U.S. federal courthouses. *

While the focus of the committee's work is on the protection of federal office buildings, the primary consideration in protecting these buildings is to safeguard the people who work in or use the facility. Of secondary importance is the protection of information, often invaluable and irreplaceable, that might be contained in the building. The protection of the persons, information and the building itself requires a set of strategies that would include:

1. Temporary protective measures that are added to the building for a limited period of time when there is reason to believe that an attack might take place. For example, increased security forces might be added or certain doors may be barricaded in times of high threat levels.
2. Permanent protective measures that would be added if there is any reason to believe that the building might at some time be a target or if the threat is of a continuous nature. These measures could include relatively simple actions such as the protection of the entrance through placement of bollards or planters to more complex efforts such as redirecting roads away from the building. Permanent measures could also be added to a building at the time

* The GAO study focuses on anti-terrorism measures for selected domestic infrastructure components. It was requested by Congress through the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary. The subcommittee is interested in how agencies have responded to the threat of domestic terrorism against the nation's infrastructure. The GAO study focuses on mass transit systems and federal courthouses, and will provide information on anti-terrorism policies, assessments of vulnerabilitles and risks, protective measures and their potential impact on civil liberties, and evaluations of implemented measures. The report from this study will be available late in 1988.

major additions or renovations are made. This could include reinforced construction or the installation of major detection and warning devices for any tampering to HVAC or electrical systems.

The committee recognizes that the protection of high-visibility figures, such as through the use of body guards and armored vehicles, and the protection of valuable or sensitive information, such as classified documents, should receive equal attention from those responsible for overall security planning. This report, however, concentrates on the protection of the physical structure, the federal office building, in order to safeguard the lives of persons and the information with which they work.

NOTE

Federal Bureau of Investigation. 1984. FBI Analysis of Terrorist Incidents and Terrorist-Related Activities in the United States.

2

Guidelines for Security Management

INTRODUCTION

The committee believes strongly that each federal office building should have an ongoing building security program as part of its facility management function. It should be adopted and administered by the appropriate management element in the organization. The building security program should encompass basic building security matters (i.e., routine protection of persons, property, and information) as well as protection strategies against extraordinary events such as a terrorist act. A security program can be defined as a combination of systems, elements and people joined together to meet the specific needs of any business, industry, institution, or organization for protection, prevention, detection, enforcement, investigation, emergency service, or public service (Post and Schachtsiek, 1986).

MANAGEMENT OF A BUILDING SECURITY PROGRAM

The overall security of a federal office building and the persons and information housed within it is the responsibility of the organization that owns and occupies the building. With new buildings, the top management of organizations should insure that security

issues are addressed in the architectural programming and design phases. With all buildings, whether new or existing, management should ensure that appropriate procedures are developed to address all levels of terrorist threat.

Responsibility for security activities should be assigned to a security planning group and a security management team, established by top management. The security planning group should establish overall policy in terms of security issues, develop a building security program, and serve as the liaison entity with individuals or groups outside the organization such as the local police or the FBI. Membership in the security planning group should include those best able to assess the following: (1) mission criticality of the building or organizations within the building, (2) the likelihood that the building or organizations within the building would be a terrorist target, (3) requirements for the safety of employees, (4) requirements for classified material and other critical assets, and (5) legal and financial considerations of security measures.

The security management team should manage the day-to-day operation of a building security program. A security management team should consist of security specialists, the facility manager (or representative), and others deemed appropriate by the facility manager. In some cases, non-government tenants such as those that hold valuable assets on the premises (e.g., banks and jewelry stores) or government contractors that require certain mandatory security measures, may participate on the security management team.

The building security program should be prepared in collaboration with the building owner (even for non-government owned buildings), local law enforcement agencies, and outside consultants as needed. Since security programs frequently include modifications to the building (such as restrictions when and where people can enter and leave the building) life safety requirements should also be coordinated with the local fire department or other appropriate organizations.

A BUILDING SECURITY PROGRAM

Elements

A building security program consists of four major elements: (1) policies and procedures, (2) personnel, (3) facilities, and (4)

systems and equipment. The effectiveness of the program depends upon the interaction of these elements; relying on any one element to the exclusion of the others will compromise the program.

Policies and procedures, the formalized ways in which various security functions are carried out, are key to the entire security effort. They include security plans, threat analyses, instructions and manuals, standards of performance, and criteria for facilities and systems. For example, Table 2-1 shows a recommended table of contents for an office building security manual.

Retaining a team of personnel that is well equipped and highly motivated is essential to the success of a building security program. Personnel must be knowledgeable about potential adversaries and, most importantly, must be able to respond to surprises. Important considerations include recruitment, selection, training, and support.

The building itself is a key element of a security program, including the degree to which the building is hardened (physically strengthened to withstand greater levels of attack, such as bomb blasts), the designated entry and exit points, and the existence and location of vaults, secure rooms, response force facilities, barriers, and structures designed to withstand ballistic attacks.

Security technology in the form of systems and equipment is employed primarily to complement the capability of the human security force. Systems and equipment include personal security equipment (such as arms and munitions, vehicles, and communications equipment) and electronic security systems (such as intrusion detection systems, automated entry and access control systems, and surveillance and assessment equipment). Security systems and equipment can allow for more comprehensive coverage, earlier indication of an intrusion, quicker assessment of the nature of the attack, and a more tailored and focused response. Electronic security systems can also provide the opportunity for fewer individuals to be assigned to traditional guard duty activities. While security technology enhances the capability of the security force, it places greater demands on the alertness, judgment and training of security force personnel. The building security program should include a plan for continuous maintenance of the systems and equipment.

When selecting security systems and equipment for a particular building, it is important that the security force and the maintenance personnel be provided with adequate training to operate and maintain the systems and equipment. It is also important that

TABLE 2-1 Example of a Table of Contents for an Office Building Security Manual

GENERAL OFFICE BUILDING COMPLEX SECURITY MANUAL	
	Foreword
	Introduction
Part I:	General office complex: Its buildings, its people
	Organization chart: General office complex
	Organization chart: Security department
	Map of building locations
Part II:	Organization of security services
	Responsibilities of director of security, security sergeant, security officer
Part III:	General duties of the security force
	General outline of duties of members of security force
Part IV:	Authority as a special deputy
	Right to arrest
	Right to detain and question
Part V:	Deportment and general appearance
	Code of ethics
	Deportment
	Personal appearance
Part VI:	Special police equipment
	Use of baton, handcuffs, chemical mace, walkie-talkies
Part VII:	Preventive patrolling
	Preventive patrol, building patrol
	Aggressive patrol
Part VIII:	The things security officers must keep in mind
	Increasing your powers of observation
Part IX:	General orders for security officers General orders: How they are given and how they are to be carried out
Part X	Investigation report
	Daily security report
	Who, what, when, where, how
	Index to sample reports
	Sample reports
Part XI:	Special emergencies
	Fires
	Disasters, internal and external
	Bomb threats
	Summary

Source: Post and Schachtsiek, 1986.

the ergonomic design—the design of the workplace—encourage an alert and active security force.

Functions

A building security program has at least six functions: (1) deterrence, (2) delay, (3) detection, (4) alerting, (5) response, and (6) neutralization.

Deterrence is the ultimate goal of any building security program in that it discourages potential attacks because the building is so well protected. The delay function comes into play when an attack is launched and involves the combination of the security force and physical attributes such as barriers, locks, and traffic flow systems that will slow an attack in order to provide more response time.

The building security program should include a detection capability so that, as soon as possible after an attack is launched, the security force can be activated. Once an attack is detected, a fourth function, alerting, comes into play. This involves communicating the nature and location of the attack using clear and quick methods.

The fifth function of a building security program is the response itself, the purpose of which is to interdict the adversary. Neutralization involves controlling the adversary, thus eliminating the immediate threat.

DEVELOPING, EVALUATING AND IMPLEMENTING A BUILDING SECURITY PROGRAM

The committee recognizes that all federal office buildings are not equally threatened. Highly visible or symbolic buildings (such as courthouses) and office buildings housing controversial agencies are subject to higher levels of threat. Office buildings can contain information (such as intelligence or military records) that may be a target. Buildings may house high ranking political or military leaders that could be targeted by terrorist groups. The level of threat against a particular building may change over time as conditions change. Because of this, agencies should develop a building security program that is frequently reviewed and revised to keep current with changes in the agency's mission, functions, personnel and facilities, and with changes in the the nature of the threat.

Developing a Building Security Program

A building security program should be developed by the security planning group. The planning group should consider calling on physical security specialists to assist in the development of the program. Regardless of the composition of the security planning group, the major steps in developing and maintaining an effective building security program follow:

1. Identify potential targets (people, information, the building itself) and evaluate their relative attractiveness to terrorists.
2. Establish priorities for protecting the targets identified.
3. Assess the vulnerabilities of the potential targets.
4. Evaluate the building security program in light of the nature of the threat, under routine security conditions as well as under actual threat (threat alert) conditions. Evaluate the program with respect to the four elements of the program (policies and procedures, personnel, facilities, and systems and equipment).
5. Implement regular training of security personnel and sensitize the security planning group to changes in the field.
6. Conduct periodic operational testing of the building security program (at least twice a year). The testing should involve the entire building, as well as outside support personnel who would be needed in the event of a hostile incident. Such testing should emphasize the internal and external communication networks involved in the security program.
7. Modify the building security program and renovate the building as needed.

Evaluating the Building Security Program

Evaluation of the building security program should determine the program's effectiveness with respect to the four major security program elements. In order to be effective, the security program should clearly describe how to identify potential terrorist targets, how to establish priorities for protection, how to assess the vulnerability of targets, and how to revise and maintain the building security program. The specific responsibilities of personnel should be clearly defined and the individuals responsible should be named, with telephone numbers provided. In addition, a building security program should be evaluated in terms of the training materials, programs and schedules that are provided to educate personnel on

the nature of the threat, and the security policies and procedures of the program.

Implementing the Building Security Program

Successful implementation of a building security program requires visibility, which is only possible through the active participation of the top management of the organization. In addition, effective implementation and execution of the program depend on everyone knowing his or her role and being able to execute it as a normal part of the daily routine. The smooth operation of a security program results from frequent training and rehearsal sessions organized by the security management team.

TEMPORARY SECURITY MEASURES

Changes in the nature and level of threats require that the security management team maintain a program of temporary security measures. These temporary responses are contingency plans for increased levels of security that are imposed when external conditions warrant. Examples of such temporary actions include closing non-essential access points, reducing the number of individuals granted access to critical areas of the building, increasing the number of personnel in the security force, and, if appropriate, establishing temporary barriers. When advised of a reduction in threat levels, measures put into place on a temporary basis should be reviewed. Those that substantially inhibit the functioning of the organization or the operation of the building should be removed. Temporary measures that enhance security without hindering individual or organizational performance should be considered for permanent incorporation in the building.

ROLES AND RESPONSIBILITIES OF A SECURITY MANAGEMENT TEAM DURING AND AFTER A HOSTILE ATTACK

Crisis management is essentially the management of surprise. It attempts to limit the damage from a surprise occurrence and to resume normal operations. Surprise occurrences include earthquakes, floods, industrial accidents, and fires as well as terrorist acts. The success of the response in each case is the direct result of

the thoroughness of prior contingency planning and training. The most critical requirement is to identify which agencies and individuals in those agencies are required to handle the consequences of these events. Quick communication between the security management team and these individuals, even in situations where conventional telephone and power systems are out of action, is essential.

The roles of each internal and external group (such as fire fighters, utility people, food service personnel, first aid and emergency medical teams) must be established in advance to insure quick and effective action. Operational testing of the building security program should be conducted and modified until the functions are clearly understood and major problems eliminated. Such operational tests are justified not only by the threat of a terrorist attack, but by the chance of any surprise occurrence or disaster which would require the same plans and resources.

TARGETS, PRIORITIES, AND VULNERABILITIES

Because terrorists use violence to further political or social objectives, targets are often selected to create a sense of outrage and shock. The publicity accompanying such acts provides the terrorist with an image of invincibility and impunity. As a symbolic act, it generates a greater sense of outrage when perpetrated against a national symbol, an activity of the government, or a popular or highly-placed citizen. Shock value increases if the target appears to the public as innocent in the political struggle and if the act is executed in a very violent fashion.

Terrorist methods include hostage taking, or assaults on personnel (including assassination), destroying or stealing records or valuable information, and damaging or destroying property, such as public buildings. Potential targets should be considered for their symbolic value, their functional value, the terrorists' accessibility to the targets, and the nature and location of protective measures.

A building security program should be organized in consideration of protection of persons in or around the building as the highest priority. It should also recognize that the terrorists may target a critical operational function for destruction (including destroying the building itself) to demonstrate that a government can

be crippled by not protecting a vital part of its operations. Priorities for protection must consider the importance of protecting human life and critical federal functions, as well as the accessibility of the building and the practicality of affording protection at a reasonable cost.

NOTE

Post, R.S. and D.A. Schachtsiek. 1986. Security Manager's Desk Reference. London: Butterworth Publishers.

3

Threat Assessment and Vulnerability Analysis

INTRODUCTION

This chapter provides guidance for federal agency administrators to obtain threat information relevant to an agency's buildings. The committee believes this should be undertaken through a formal means of threat assessment using liaison channels to disseminate information to appropriate personnel within the agency.

The building security program should also provide guidelines for the security management team to conduct a vulnerability analysis of the building. In this chapter, the committee offers vulnerability guidelines to help determine what elements of a building and its security program could be exploited by terrorists. Twenty-three areas of concern are listed; in Appendix A, these areas of concern are expanded into a sample checklist that illustrates how a vulnerability analysis could be conducted.

Other Reference Works

A great number of commercially available manuals and other documents exist to help security planners analyze the risk, conduct threat assessments, and undertake building vulnerability analyses. For example, Walsh and Healy (1987) is considered to be the basic

guide in private industry for threat and vulnerability analyses; material presented is appropriate for managers of buildings as well as security personnel. James Broder (1984) presents a thorough primer on the subject of risk analysis, including the identification of vulnerabilities and threats, measuring and quantifying risk, and quantifying and setting priorities for loss potential. Reber and Shaw (1980), in a book aimed primarily at executive (personnel) protection, presents vulnerability surveys based on past terrorist incidents against multinational corporations. Finally, Gigliotti and Jason (1984) discusses levels of physical security culminating in the concept of maximum security—the integration of a number of elements in a security program.

The committee urges security planners and managers to keep current, through the literature or otherwise, with developing security technologies and with new security management techniques.

THREAT ASSESSMENT

It is necessary to establish a base line or minimum acceptable level of protection for a federal office building to be able to determine an acceptable risk. Because the threat will change over the life of the building, it is important to establish this minimum acceptable level of protection that is required as the basis for any redesign or modification. For example, a minimum level of protection could require that all building exit doors to be secured, alarmed, or guarded.

The level of threat establishes the level of protection that is required, and it is the threat trend over a long period of time that should establish the level of building protection. For example, a building that is designed and constructed for today's identified threat does not take into account that the building will be in existence for 40 years or more.

Terrorism Threat Analysis

A terrorism threat analysis involves assessment, quantification, and measurement of the risks that a building will be the target of a hostile act. While it is difficult to anticipate the conduct of a terrorist acting in isolation, as soon as a terrorist acts in concert with others or acts in a repetitive fashion, opportunities exist for gathering information. In the hands of the right parties,

this information can be useful in assessing the threat against other buildings, and, therefore, in preventing the same terrorist from being successful a second time.

There are some obvious considerations: The pertinent information must first be gathered, and it must be made available (either routinely or upon request) to the party who can do something with it. Terrorism threat analysis involves intelligence gathering and sharing, which, if successful, may actually help reduce risk or prevent a terrorist incident.

The magnitude of the potential threat must be evaluated before resources are committed for either temporary or permanent security measures. This evaluation involves analysis of at least two categories of information: (1) those variables unique to each federal agency because of its nature or mission (real or perceived), and (2) consideration of the variables that pertain to all federal office buildings simply because they are that. The former may be viewed as the individualized aspects of a threat assessment effort, and the latter as the generalized.

The nature or mission of the federal agency is important to the extent that history may show a pattern of that agency's buildings being a target of terrorism. Quite obviously, a federal day care center would differ from a military intelligence office, and knowledge of the history of hostile acts against a type of federal agency may be among the most important components of a terrorism threat assessment. However, even when no evidence exists that a given type of federal agency previously has been targeted, a threat analysis is far from complete. Information regarding the existence and activities of terrorists whose expressed or logical aspirations are opposed to the federal agency may be as important as the consideration of historical patterns.

The foregoing factors—i.e., the nature of an agency, the historical pattern of terrorism against such an agency, and the existence of militant organizations with hostile intentions toward the agency—are the primary components of a terrorism threat assessment.

General considerations exist as well. Any federal agency can be a target of a terrorist with an undifferentiated hostility toward the U.S. government. The terrorist may strike merely because the agency or a federal building is: (1) the only federal presence in a community, (2) the most conspicuous physically, (3) the most conspicuous symbolically, or (4) the most vulnerable.

Moreover, because terrorism is cause-motivated and symbolic targets with a high publicity value are preferred, contemporary events and political incidents can increase or diminish the likelihood of a given building becoming a terrorist target. Therefore, generalized considerations can quickly become individualized considerations.

Who Has Jurisdiction?

Planning for and responding to many types of terrorist activities require the coordinated efforts of several federal law enforcement agencies, each with different subject matter jurisdiction. Additionally, because some federal office buildings are rented, or are on or adjacent to property not under the exclusive control of a federal tenant, the jurisdiction of local authorities may be involved. In other words, the statutory authority of a given enforcement body and the location of an incident may have an impact on both the preventive measures undertaken in advance of an anticipated hostile act and on the response in the event that one occurs.

These considerations may not only influence the effectiveness with which a hostile act is handled, but also may affect whether or not a terrorist who is apprehended can be prosecuted successfully. Therefore, it is prudent to address jurisdictional issues at the time that threat and vulnerability assessments are undertaken. Accordingly, once enforcement coordination issues are resolved from an operational standpoint, the agency in question should assure that jurisdictional complications are not likely to arise.

Who Has the Information Necessary to Make the Assessment?

Because a threat assessment involves generic information as well as information unique to each agency, the information that is critical for a proper assessment may repose in several locations. Local information (information unique to an agency and already in the agency's custody) is an internal information management matter. It is the responsibility of each federal agency to assure that information pertinent to a threat analysis is in the hands of the party responsible for making the analysis. * But in many

federal office buildings there may be several federal tenants, not all of which may possess critical information (either because it was developed by or is uniquely applicable to another tenant). The problem with this is that a hostile act, even though targeted at one federal agency, may cause equal damage to a neighboring agency. There may be critical information available in the hands of several different parties, but not necessarily all pertinent parties.

Domestic terrorism intelligence is currently the concern of the Federal Bureau of Investigation (FBI). The FBI's Domestic Terrorism Unit has access to intelligence regarding foreign terrorism. For example, the Deputy Assistant Secretary of State for the Diplomatic Security Service is required to "consult regularly with federal law enforcement and intelligence agencies, including the Federal Bureau of Investigation and United States Secret Service..." as well as with state and local law enforcement agencies with respect to certain security matters (22 C.F.R. Part 2a). That consulting should result in intelligence sharing and should transpire between all federal intelligence agencies and the FBI. Thus, the FBI, in most cases, should be privy to whatever pertinent information might exist.

Although the FBI has indicated that it does dispense specific terrorism threat information to agencies on an ad hoc basis, no formalized system or periodic reporting mechanisms are in place. * More noticeably, no obligation or system exists that would encourage, require, or even facilitate agencies or tenants of federal office buildings to share threat information with the FBI or other building tenants. This is not to say that information sharing is not done, but rather that in each instance whether it is done, when, by whom and to whom are all uncontrolled variables.

To summarize, intelligence pertinent to a terrorism threat may be in the possession of a specific federal agency, developed by itself or obtained from others. The intelligence, however, may not necessarily be in the hands of the proper parties within that agency. It may be in the hands of federal law enforcement and

* Walsh and Healy (1987) recommends that threat assessments should be in the domain of an organization's security planning group. This group might include representatives from each of the following organizational disciplines: security, legal, finance, personnel or human relations, communications, and international operations.

*Mr. Donald Wofford in his April 24, 1987 oral presentation to the committee.

intelligence agencies in general, and the FBI Domestic Terrorism Unit in particular. However, there does not now appear to exist a formal system for the reporting or sharing of such information between building occupants or enforcement agencies to the extent that it would be useable for effective threat assessment planning. The Domestic Terrorism Unit is the most likely central federal office to have responsibility for the coordination of information pertinent to a threat assessment

The committee believes that a formal means of threat communication should be established between the security management team (for the building occupants) and law enforcement agencies that possess the information.

Who Can Use the Information?

Information concerning threat assessments would be useful to at least the following: (1) the appropriate management official of each federal agency in the building, (2) the security personnel responsible for the building, (which may be under the control of an agency tenant, the General Services Administration, the building manager, or a contractor), (3) the building managers who may be federal employees or private sector employees in the case of leased space, and (4) individual employees, especially to the extent that their vigilance may help prevent an anticipated hostile act.

What Is To Be Done With the Information?

Perhaps the weakest link in the process of threat assessments is intelligence or information sharing. The issue is especially complicated by the fact that pertinent information is often classified, and those who need it most may not have appropriate clearances. Even if no classified information is involved, tedious bureaucratic processes, which may be tolerable in non-emergency situations, become intolerable in life-threatening situations. Finally, the wide dissemination of information, while desirable for obvious reasons, may be counterproductive because the terrorist may acquire information that will increase the probability of success.

When reliable information ends up in the hands of the right party, the threat assessment conclusions should be mated with other pertinent information, such as the building vulnerability

analysis and available observations regarding the consequences of a successful terrorist act.

Checklist for Threat Analysis

The following questions will help those responsible for preparing a threat assessment and will serve as a checklist that all elements are considered:

1. What factors about your agency and its mission invite potential hostility?
2. How conspicuous is your building?
3. How vulnerable does your building appear?
4. What current political event(s) may generate new hostility toward you?
5. Have buildings like yours or activities performing functions like yours been targeted in the past?
6. What groups exist with known violent propensities, whose social or political positions are antithetical to yours?
7. Is any group a current suspect in an investigation of any act of terrorism, foreign or domestic?
8. What information do federal law enforcement officials have with respect to your concern? What information do local law officials have?
9. Who else might be in a position to have pertinent information?
10. Who else should be notified of the information you have within your organization, within your building, near your building?
11. Have federal and local law enforcement officials been sufficiently involved in planning activities?
12. Do local medical or health facility officials need to be alerted or involved in your planning?

VULNERABILITY ANALYSIS

A definition of building vulnerability is any weakness in the physical plant, a flaw in the building security program, or a hole in the carrying out of the program. Simply put, vulnerability is anything a terrorist could take advantage of to carry out a threat. A terrorist threat can be one or a combination of at least four types: (1) to kill, injure, or kidnap (hold hostage) persons, (2) to damage

property, (3) to steal or destroy information or materials, or (4) to halt operations. Typical weapons used by terrorists include handguns, rifles, automatic weapons and improvised explosive devices. Tools and equipment for entry may include simple tools for barrier penetration, false credentials and communication equipment. Many terrorists are trained in weapons tactics, explosives manufacturing, forgery, codes and security.

Therefore, a vulnerability checklist should target the characteristics of the building and its personnel that terrorists could easily exploit. Vulnerabilities can be determined by any or all of the following four methods: (1) interviewing key personnel at the building, (2) conducting field inspections and observations, (3) reviewing documents, and (4) undertaking field testing of hardware and electronic systems. Reports of past incidents provide excellent data for the occurrence rates and probability determination. If these reports are not available, they should be recreated through interviews (Sennewald, 1985).

Any vulnerability analysis made by the security management team of a given building should consider that some agencies (e.g., those with a degree of public access) are more susceptible to a hostile attack than others, and that some agencies are at a relatively higher risk of being targeted than others. If an agency cannot be adequately protected in a particular building, or if the mere presence of such a relatively high-risk tenant imposes excessive security restrictions on other less-sensitive tenants, relocation of the high-risk tenant to a different building should be considered. Agencies that manage federal office buildings, such as the General Services Administration, should give careful consideration to the proposed agency occupancy mix when planning new buildings and relocating tenants.

The following list shows 23 areas of concern that a vulnerability survey should include. Appendix A presents an example of a vulnerability checklist that can be used by the security management team as a base line of information to be considered when developing the vulnerability analysis. The areas of concern are:

1. Security manager (general checklist/verification information)
2. General facility function and tenants

— Ownership or occupancy
— Number of employees

— Tenant agencies and missions

3. Building construction, perimeters and entrances.

— Envelope construction
— Number/type of entrances
— Type of perimeters and access to building

4. Vehicle movement and controlled areas

— Public/employee parking areas
— Traffic control zones

5. Lighting systems and locations

— Site lighting
— Building lighting
— Security lighting

6. Locking controls

— Keying systems
— Positive ID systems
— Area control systems

7. Alarms

— Locations
— Control personnel
— Devices

8. Guard force

— Number of guards and posts
— Terrorist training and review
— Guard functions and review

9. Employee and visitor controls

— Positive ID systems
— Visitor access procedures/clearance

10. Mail handling areas

— Processing areas
— Inspection procedures
— Outside storage areas

11. Information (control of classified)

— Check-out procedures
— Disposal

12. Trash pick up and scrap control

— Location of pick-up areas
— Fixed pick-up hours

13. Personnel security checks

14. Symbolic characteristics of the building

— VIPs in building
— Shrines, museums, etc.

15. Availability of anti-terrorist security force
16. Secured communication lines

— Primary/secondary

17. Response time of security force
18. Location in or outside of urban area
19. Geographic region and proximity to foreign borders
20. Access to the building by the public

— Roads
— Airfields
— Waterways

21. Surrounding terrain

— Built-up
— Mountainous/open

22. Utilities location

— Air intake
— Potable water
— Power: primary/secondary

23. Site analysis

— Vegetation
— Land use
— Circulation, (vehicles/people)
— Lines of sight
— Lighting (area/security)
— Services (police/fire/medical)

NOTES

Walsh, T.J., and R.J. Healy. 1987. Protection of Assets Manual. Santa Monica, California: The Merritt Company Publication.

Broder, J. 1984. Risk Analysis and the Security Survey. London: Butterworth Publishers.

Reber, J., and P. Shaw. 1980. Executive Protection Manual (Second Edition). Schiller Park, Illinois: MTI Teleprograms, Inc.

Gigliotti, R.J., and R.C. Jason. 1984. Security Design for Maximum Protection. London: Butterworth Publishers.

Sennewald, C.A. 1985. Effective Security Management (Second Edition). Boston: Butterworth Publishers.

4

Security Guidelines for Sites and Buildings

INTRODUCTION

This chapter provides guidelines for temporary and permanent measures to secure sites and buildings against hostile attack. It is important to recognize that security measures for sites and buildings may vary from temporary to permanent based on threat assessment. Temporary measures are those protective measures that can be added to the building for a limited period of time and then removed. Temporary measures are reversible in that once they are removed, the building reverts to its original state. For example, during a period of high threat alert, certain building entrances can be closed and barricaded. When the threat subsides, these entrances can be put back into use with no permanent effect on the building or its operations.

Permanent protective measures are lasting modifications to the building or its operations when the long-term threat level is high or continuous. For example, a temporarily closed and barricaded building entrance may be permanently secured through the placement of bollards or planters outside the entrance.

Temporary security measures or other modifications made in response to passing threats should be systematically evaluated for permanent continuation, reduction to some intermediate level,

TABLE 4-1 Example of an Office Building Threat Response Matrix

	Escalating Levels of Threat			
Possible Responses	VerbM Warnings/ Low-Level Indication	Bomb Threat/ Indication Increases	Active Bombing/ Attack on Similar Building	Anarchy/ Direct Threat to Building
• Alert building management	X	X	X	X
• Close all unguarded entrances	X	X	X	X
• Screen all people & bags	X	X	X	X
• Clear areas near windows		X	X	X
• Monitor structural focal points		X	X	X
• Cancel scheduled meetings			X	X
• Minimize staff			X	X
• Install portable barriers				X
• Cordon off surrounding streets				X
• Evacuate a wing or floor				X
• Close areas (e.g., day care centers)				X
•				
• (Other responses)				
•				
• Evacuate entire building until threat level subsides				X

or elimination. Table 4-1 shows an example of what could be considered a typical federal office building threat response matrix that could be used in cases of advance notice of different levels of threat. In this example, as the level of threat increases, the security measures increase. A matrix similar to this could be developed by a security management team and provided to the building's operator. The matrix would be updated as building changes occur (such as new doors installed) and would concentrate on actions to take in response to threats as opposed to minimum or base line security precautions.

The measures identified need to be used with judgment and practicality relative to the level of threat, the continuing function of the building, and aesthetic and environmental concerns. Legal implications of security measures must also be considered as explained in the following section.

LEGAL CONSIDERATIONS

Security planners and managers should realize that certain security measures, while appealing, especially in a time of crisis, may come into conflict with the constitutional rights of employees or the general public. Public officials who are responsible for the security of federal office buildings must satisfy federal constitutional standards. Private landlords, in contrast, must comply with applicable statutes, but not usually constitutional standards. In the area of security practices, the constitutional provisions most likely to arise are the First and Fourth Amendments.

Although not expressed precisely in these terms, the First Amendment to the Constitution is often construed as having created and guaranteed a right of privacy. Many state constitutions and statutes create the right expressly. Similarly, the Fourth Amendment guarantees all citizens the right to be free from unreasonable searches and seizures by government officials. What is a reasonable or unreasonable search may in turn depend on whether an individual has an expectation of privacy in the thing or place searched. It is the concept of privacy that draws the First and Fourth Amendments into a partnership that defines the limits of constitutionally permissible security practices.

The security practices that most frequently give rise to potential privacy intrusions are electronic surveillance including eaves-dropping and monitoring via closed-circuit television, parcel or personal inspections at building entrances and exits, and evidence gathering activities such as searching employees' desks or lockers. In addition to constitutional constraints, electronic surveillance practices are extensively regulated by federal statutes that include civil and criminal sanctions.

Individuals may be asked to waive their constitutional rights, within reason, in exchange for the privilege of receiving the benefits of government services. For example, admission to government buildings is often conditioned upon the willingness of an individual to consent to a cursory search of packages being carried, or upon his or her agreement to provide identification. Such consent is actually a waiver of constitutional rights. In order to be a valid waiver, it must be knowing, intelligent and voluntary. The posting of signs helps satisfy the “knowing” requirements of the law, and the fact that there are options (the person must be free to turn and walk away rather than submit) satisfies the “voluntary” requirements.

In all cases, security practices that are in potential conflict with constitutional rights should be the least intrusive possible in order to accomplish the legitimate interests of the government, while at the same time preserving individual freedoms.

Building modifications using electronic surveillance equipment (audio or video), the use of two-way mirrors, entrance inspection policies, desk or locker search policies, and all security practices used in locations where expectations of privacy might exist (such as restrooms) should be reviewed by counsel periodically to assure compatibility with current statutes and recent judicial interpretations of the Constitution.

Similarly, because the legal justification for such practices may depend upon the immediacy as well as the nature of the threat, a review of any security practice that impinges on privacy interests should be undertaken regularly to ascertain whether the need for the measure remains.

GUIDELINES FOR SITE SECURITY

Site planning and site design can be seen as discrete exercises for new facilities; however, when upgrading an existing building's site for security purposes, the two blend together. The following guidelines are intended to respond to security deficiencies that would be identified in the vulnerability analysis described in the previous chapter. They are presented as items for consideration. For many federal once buildings with minimal sites, such as in a congested downtown location, the guidelines will be less applicable.

Circulation

To minimize threats that originate outside of the building, movement in and around the building site must be controlled. The explosive laden vehicle is of greatest concern because of its potential for destruction. However, other hostile activities, from drive-by shootings to mob activity, can be mitigated by site circulation measures. Guidelines to be considered include:

1. Restrict vehicular approach to designated and controlled entry areas only.
2. Whenever warranted, the speed limit on all adjacent and intersecting streets should not exceed 30 miles per hour. Speed may be controlled using the following elements:

- speed bumps,
- sharp curves (horizontal alignment),
- steep grades (vertical alignment),
- narrowing the lanes of traffic,
- pavement material changes,
- signage,
- intersection signals, and
- pavement cuts.

3. As necessary, the direction of circulation on adjacent streets should be controlled.
4. Circulation routes and attempts to leave the roadway can be controlled using high curbs, at least along all portions of the site perimeter fronting a street. Median strips, bollards, barriers, or planters can be used to block possible direct cross street access that is created by a curb cut from an alley or property access across from the site.
5. Breaks-in curbs, medians, or barriers should be provided only at controlled entry points to the site.
6. Wherever necessary, detection and monitoring devices can be employed to detect excessive speed or movement in the wrong direction, or to indicate the presence of a vehicle. Such devices include closed-circuit television, electronic detection loops, radar, photoelectric cells or laser-bar codes.

Access and Egress

Site access points are perhaps the most important component of the perimeter security system and, as such, must address a variety of requirements. Entry responsibilities include observation, detection, deployment of security measures, inspection, access control, access denial, and containment of a threat to the entry area only. Guidelines include:

1. Vehicular access points should be limited to one entrance for ceremonial uses and one entrance for service uses.
2. Wherever warranted, vehicular entrances should be closed on highly traveled streets, or on any side of the site that could be approached with a vehicle at a high rate of speed.
3. Where vehicular entrances are located directly opposite an intersecting street, alley, or curb cut, or at the terminus of a street where a vehicle might be capable of a high-speed approach to

the entry, access should be restricted through the construction of medians, bollards, or barriers that block the vehicular approach path and that are capable of stopping the vehicle.

4. To facilitate early detection of a hostile attack, site entrances can be designed so that all exiting vehicles have a clear field of vision as they approach the roadway. To achieve this objective, the perimeter wall can be recessed or angled away from the entry approach. Stacking of cars in an entry lane should be allowed to prevent congestion on the street.
5. The entry can employ various barriers to augment the protection of the site entry gates, to control movement, or to deny access. Inspection points should be on the property but not adjacent to or inside the building. Static barriers (or operable barriers, when necessary) can be used to prevent vehicles from circumventing the entry gate or to control the pattern of approach to it. Also, static barriers can be stored on-site for deployment in times of increasing threat or emergency. Operable barriers can be located inside the entry gates.
6. To prevent accidental contact with a barrier that has been deployed in an emergency, the entry can be so designed that anyone traveling at a low rate of speed toward the gate or barrier areas can determine if a barrier is deployed before reaching it. Alarms, signage, warning lights, or a gate located before the barrier can be used as deployment indicators.
7. The site entry and its approach should be evenly lit with all light levels sufficient for detection and inspection.
8. Vehicular and pedestrian entrances should be separate, if possible.
9. Visitor and employee pedestrian entrances should be separately located, if possible.

Parking

1. If possible, restrict vehicle access to the site by providing off-site parking lots. On-site parking could be provided for employees only and should be accompanied by an adequate security and identification system.
2. On-site parking areas should be evenly lit; dark areas that could provide hiding places should be eliminated.

3. Wherever possible, parking should not be permitted along streets adjacent to the site to reduce the possibility of a preset vehicle bomb.
4. Pedestrian access to and from off-site parking areas should be protected with surveillance, lighting, and protective devices wherever possible.

Perimeter

The site perimeter is the first line of defence against a hostile attack. Its function is to confine a given threat outside the perimeter. This is particularly true for bombs, whether they are planted or are in a vehicle.

It has been frequently shown that no perimeter is totally impenetrable given a determined attacker with adequate time and proper equipment. Consequently, the perimeter should also serve to delay intruders sufficiently to permit detection and allow for an appropriate response.

Most buildings in urban areas do not have a perimeter other than the building wall itself. In such circumstances, it may be necessary to create a perimeter through the closing of streets and enclosing adjacent open space.

Examples of perimeter barriers include stationary trucks, concrete road barriers, berms, walls, fences, ditches, and hedges. Trucks and concrete road barriers (such as have been used around the White House) should be considered temporary measures to be used only until the threat level subsides or permanent solutions can be constructed.

Site perimeter security guidelines follow:

1. The location of the perimeter is critical to the effective protection of the building. The perimeter should be at the maximum feasible distance or that distance such that any anticipated explosion will not cause major damage to the building. It has been clearly established that the impact of an explosive device is a function of its pounds TNT equivalent and the distance of the detonation from the target.
2. The site perimeter should be designed to confine hostile activities outside the perimeter barrier.
3. Perimeter features should be installed to deny completely or to delay sufficiently any unauthorized site access.

4. The site perimeter should be designed to facilitate observation and detection functions.
5. The site perimeter should withstand and protect the building and its inhabitants from standoff or drive-by attacks, and from explosive devices.
6. Whenever possible, the perimeter should use a combination of barrier techniques. With a combination of elements, it may be possible to design each individual component in a less restrictive manner, a method that may prove to be more economical. This type of approach also offers a certain amount of redundancy; if one of the components fails, it does not necessarily mean that the entry is compromised. However, the total strength of the combined barriers should meet the original design objective. Walls, berms and planting, bollards, static barriers, fences, embankments, tire traps, and ditches can be used.
7. The primary wall or fence at the perimeter should be at least 10 feet from any trees, poles, or buildings that could help would-be intruders scale the perimeter.
8. The perimeter wall or barrier should be as high as possible. (If a berm is also used, this height is not measured from the base of the berm but from the base of the wall or fence.) A 9-foot barrier is considered to be a deterrent to most climb-over attempts, but the wall or fence should also be designed to support the use of concertina wire for additional height.
9. The site perimeter should be well lit for observation and detection functions. When appropriate, glare lighting should be used as a deterrent to intruders. However, the perimeter lighting should illuminate only intruders and not the security force or interior activity areas.
10. The site perimeter should be designed to facilitate on-site surveillance objectives; the construction of walls, fences, berms, plantings, etc. should not create potential hiding places for would-be intruders who cannot be seen from observation points. Any area that cannot be physically monitored should be monitored by electronic observation devices or by alarm-activated devices.

Vehicle Barriers

The following guidelines are security design assumptions for vehicle barriers when such barriers are appropriate for use:

1. The barrier should be designed to arrest a vehicle of a specified gross weight going at a specified speed. For example, a vehicle of 15,000 pounds gross weight going 30 miles per hour provides a kinetic energy level of 450,000 foot-pounds. This could be considered a minimum level against which a barrier should be designed.
2. The barrier should be designed to arrest a vehicle within a specified distance from the point of impact. Flexibility in the requirement should be based on the barrier's location with respect to the object it is designed to protect. For example, a barrier located three feet from the exterior wall of a building must stop a vehicle within three feet of impact, but a barrier located 100 feet from the building can have greater flexibility from the point of impact.
3. Static barriers may be used and include the following:
   - barbed-wire fencing,
   - chain-link fencing,
   - metal guardrails,
   - sectional steel fencing,
   - angled posts,
   - bollards,
   - concrete shapes,
   - concrete-reinforced fencing,
   - earth-filled barriers (such as planters),
   - excavations or ditches,
   - earth berms, and
   - reinforced concrete walls.
4. Active barriers may be used and include the following:
   - crash beams,
   - cable barriers,
   - tire shredders,
   - steel gates,
   - ramp barricades,
   - operable bollards,
   - pits,
   - pop-up barricades,
   - blades,
   - plow barricades,

- anti-crash gates, and
- nets.

Lighting

Exterior site lighting is an essential component of the site security system when there is insufficient daylight to perform necessary security operations and achieve security objectives. Such lighting must facilitate observation and inspection, and it should meet the goals of deterrence and safety. Guidelines include:

1. The site perimeter must have continuous lighting of an intensity that permits observation, inspection, detection, and deterrence operations.
2. The lighting of the site perimeter should promote the safety of the facility and its inhabitants.
3. The location of perimeter lighting fixtures should facilitate the lighting of both sides of the perimeter wall or fence.
4. Perimeter lighting fixtures and lamps should resist damage from gunfire, blast fragments or vehicle impact.
5. Perimeter lighting should be designed for emergency operating conditions.
6. Lighting should be designed with enhancement options for times of emergency, intrusion, or attack.

Planting

Any planting should enhance security objectives and should not interfere with security operations. Guidelines include:

1. Plant materials should be located, wherever possible, to deter climb-over attempts.
2. Planting areas should not provide hiding places for would-be intruders.
3. Wherever possible, plant materials should screen the site entry, on-site parking areas, building entrances, outdoor activity areas, mechanical and electrical equipment areas, or any other vulnerable site areas from off-site observers. This visual screening should not provide an opportunity for concealment of intruders.

GUIDELINES FOR BUILDING SECURITY

Occupancy Types

In the building security program for a multitenant building, each portion of the building should be assigned a designated risk factor, ranging from high to low, based on the type of tenant in that portion of the building. Some agencies such as the Federal Bureau of Investigation and the Internal Revenue Service, for example, appear to be higher risk tenants than the Agriculture Department or the Department of Health and Human Services. While there is no guarantee that this relative risk assignment will remain constant over time, it is prudent for building planners to attempt to segregate high-risk and low-risk tenants into separate facilities.

Where it is not possible to segregate high- and low-risk agencies in separate buildings, segregation by each risk category within the same structure should be undertaken. Access to each risk class should be separated, with the high-risk tenants afforded greater physical security. Whenever possible, high-risk tenants should be located in government-owned, rather than leased, buildings. Buildings housing only high-risk tenants should not be located close to non-government owned or controlled buildings, which could be used by terrorists to cover or enhance their attack on the target building (for example, placing a bomb in an unsecured, non-government building in close proximity to the target structure).

In buildings housing high-risk tenants, publicly accessible areas, such as waiting rooms and restrooms, should be observed within legal limits and access to these areas should be carefully controlled. In no event should waiting rooms and restrooms be located adjacent to sensitive installations, such as electronic equipment rooms, guard rooms, and mechanical support equipment.

In buildings housing high-risk tenants, incoming mail and other parcel traffic should be screened in an area outside of the main facility. Interior layouts in structures housing high-risk tenants should be designed so as to minimize hiding places for bombs and incendiary devices. Alcoves in areas that are difficult to observe by security surveillance systems, trash containers located both inside and outside the structure, unobserved underground parking areas, and unsecured utility rooms used by cleaning staffs

are typical weak points that can, and often are, exploited by terrorists.

Planning and Layout

Within the area of a building occupied by a government agency, security can be enhanced by defining the occupants' needs and implementing appropriate planning procedures. Guidelines include:

1. Functions that require controlled access to high-risk areas should be identified in the building security program and should consider the need and location for measures such as:
   - assignment of security force personnel,
   - metal detectors,
   - closed-circuit television monitors,
   - card entry access,
   - locking devices, and
   - one-way glass panels.
2. The requirement for assembly areas should be identified, and such areas should be located with consideration for:
   - anticipated attendance by staff and/or visitors,
   - requirements for restricted access,
   - visual and/or acoustical security,
   - life-safety requirements.
3. Privacy requirements for individuals or groups should be identified, especially with regard to:
   - access,
   - visual privacy,
   - acoustical privacy, and
   - electronic equipment (power, signal and communications).
4. Areas to generate, disseminate and store confidential or classified materials should be identified.

Building Zoning

Building zoning can facilitate implementing security measures at specific locations within the building. The following guidelines are offered:

1. The building should be compartmentalized to separate functions that generate heavy visitor traffic. This compartmentalization should also take into consideration the level of sensitivity requirements.
2. Security zoning should be extended to include all building service areas and circulation systems; it should prevent the spread of spillover of fire, blast or other effects of hostile activities.
3. The location of storage areas for hazardous materials and equipment, and industrial-type functional areas that could facilitate the concealment of incendiary or explosive devices should be assessed.

Building Exterior Envelope

The building exterior envelope represents one of the most challenging areas of consideration because of the variety of threats involved against the exterior and because so many interrelated elements are involved. The security management team must account for the response of exterior building surfaces and functional elements such as walls, roofs, doors, and windows to hostile actions. The following guidelines are offered:

1. Measures to reduce the number of access points (e.g., entrances and doors) permanently or to minimize the number of access points temporarily should be considered. Permanent or temporary installation of access restrictions, guards, closed-circuit television monitors, screening monitors, and limited access to elevators and stairs should also be considered in light of life-safety requirements and legal concerns.
2. The potential for forced entry and potential breach in locations other than designated access points should be considered. The accessibility of such openings (e.g., windows or vent shafts) should be evaluated and consideration should be given to some permanent closures where possible, as well as measures for temporary closures (such as bars, grills and shutters). The adequacy of existing protection for openings should be evaluated. These include installation details (anchorage) of existing vent covers, locking mechanisms and other security measures on stairwell doors, or skylights accessible from the roof.
3. Fire and blast protection can be enhanced by the evaluation of exterior building surfaces for resistance to deliberately set fires.

4. Modifications to exterior wall configurations should be considered to prevent opportunities for the concealment of destructive devices.
5. All openings such as ventilators should be evaluated for possible infiltration by liquids and fumes. Consider preventive measures such as closing existing openings or pressurizing the building to prevent undesired infiltrations.
6. Windows and other exterior openings should be evaluated for aesthetic value and functional requirements, and consideration should be given to possible security modifications, as warranted, such as:
    - Ventilation: Operational windows could be replaced by smaller and more easily protected openings in exterior wall, or by internal mechanical ventilation system.
    - Illumination with daylight: Windows could be replaced by smaller openings along with the installation of daylight reflectors on the interior of openings to achieve equivalent illumination.
    - Broken glass: Damage from the shattering of windows can be reduced by the application of a protective film on the interior of the glass surfaces, or the installation of a variety of transparent, translucent, or bullet-resistive glazing materials.
    - Privacy: Visual and acoustical privacy can be enhanced by the installation of translucent materials, interior glass shading devices, and sound-proof glazing systems.

Structural Systems

Renovating structural systems can vary from simple mechanical ties to replacement of main structural members and connections. It may be assumed, until proven by a condition survey, that distressed areas in structures as exhibited by cracking, settlement, broken windows, jammed doors and openings would also be susceptible to structural damage from a hostile attack. Distressed areas should be given high priority in the renovation process.

During regular maintenance activities, attention should be paid to upgrading or repairing the structural system. Simple and low-cost modifications can be made in the maintenance process. Items such as tying door and window frames to walls and tying facades to main structural carrying members increase the capacity of the system, thus increasing its resistance to attack.

Several critical guidelines should be followed in renovating and upgrading structural systems. These guidelines refer to strengthening the structure to resist extreme and sudden loadings.

1. Avoid progressive collapse of the structure due to the dependence of the structure on one or two key elements. Avoid weak-link chain systems where if a link is destroyed, the chain strength is destroyed. Examples of strengthening to resist progressive collapse are:
   - Continuity is created between structural members where load can be transferred from beam to beam, beam to column, floor to beam, etc.
   - Floor and roof systems are tied to all wall systems at their boundaries.
   - Redundancy is created where members that are not carrying loads do so by connecting them to the load carrying members.
   - Access is restricted to key supporting members where the system cannot be strengthened to resist progressive collapse.
2. Adequate connections should be provided from the building facade or envelope to the structural frame so that load is transferred from the facade members to the structural frame. Avoid collapse of the facade members between the structural frame members.
3. Vehicular traffic should be routed away from direct contact with main carrying structural members, such as columns and walls on the ground floor.
4. When designing structural systems in the renovation process, consideration should be given in the design for loading of members in several directions. Where loading is normally considered to cause compression, there may also be tension, thus indicating that the structural systems should be adequate in more than one direction or that other accommodations should be made.

Building Systems

It is extremely difficult to adjust building systems at the time of an actual threat alarm. Therefore, the following guidelines are recommended for consideration in the course of an ongoing building maintenance or renovation program, all as warranted by the threat assessment. If permanent adjustments are not possible

in a timely manner, temporary measures to accomplish similar goals should be considered.

1. Connections to the outside water supply, as well as mechanical and electrical sources of supply, should be located in a secure area of the building and not accessible to unauthorized persons.
2. All building service equipment should be located in a secure area of the building.
3. Back-up services for electric power, communications and water should be provided to ensure continued operation of critical functions in case of emergency.
4. Positive pressurization inside the building should be made possible, if needed, to eliminate infiltration of contaminated air from outside.
5. A system of emergency egress and safe subsequent re-entry for building occupants should be developed to ensure the prompt evacuation of building occupants and visitors, as well as a screened re-entry of only authorized building occupants.
6. Building signage requirements should be reviewed and modified as needed to facilitate an effective evacuation of all permanent and temporary building occupants, including handicapped and other special need users.

5

Conclusions and Recommendations

The committee carefully considered a number of strategies for protecting federal office buildings against the threat of terrorism. In its deliberations, the committee urged that security issues be considered as paramount as other building requirements. For example, if a building is to undergo minor modifications, security upgrades could be designed in at little extra cost. The committee realizes that major fortress-like upgrades for every federal office building is neither desirable nor likely.

With this in mind the committee makes the following conclusions and recommendations, and urges agency administrators to carefully consider each.

Conclusion 1 While incidents of terrorism in the United States are currently few in number, the committee believes that the consequences of even one serious act of terrorism against a federally owned or leased office building would be significant. It is the responsibility of those agencies that own or lease office facilities to consider security measures to protect persons, information and property, including the building itself, from a terrorist act.

Recommendation 1 Agencies that own or lease office facilities should develop and implement an ongoing security program for

each building as part of that building's facility management function. This security program should cover routine security matters as well as provide for consideration of extraordinary events that threaten persons, information or property. Full-scale operational testing of the security program should be conducted periodically.

Conclusion 2 Setting policy and implementing procedures for security-related concerns can affect the work routines of building occupants, the operations of the building, and the degree of public access to the facility.

Recommendation 2 The responsibility for security policy and implementation should reside with top management of the agency or agencies that own or occupy the building. Management should consider establishing a security planning group to develop a building security program and a security management team to oversee the day-to-day operation of the program. In buildings housing more than one agency, a senior agency should be designated to take the lead responsibility on security matters.

Conclusion 3 A threat against a federal office building and the people and information housed within it can take many forms and have many purposes. Certain buildings themselves may be symbolic targets, for example, federal courthouses. The information contained within the building may be a target or people who work in the building may be targets, from high ranking officials to innocent bystanders. Threats can be of a long-term or constant nature, or can have short-term implications, such as a direct threat on a specific agency in a certain city.

Recommendation 3 In order to offer the greatest degree of protection possible for the persons, information and property housed within a federal office building, security strategies should recognize the nature of the threat and plan building modifications accordingly. These strategies would include permanent security modifications that are expressly undertaken in response to a constant security threat, permanent security modifications that are undertaken when a building is renovated or major work is undertaken, and temporary security measures that are implemented when there is reason to believe an incident may occur.

Conclusion 4 The dissemination of threat information currently is subjected to uncontrolled variables with the result that proper and timely information may not reach the appropriate parties within an agency.

Recommendation 4 A formal means of threat communication— including the reporting and sharing of information—should be established between the building occupants (through the security management team) and the law enforcement agencies, including the FBI, that possess the information.

Conclusion 5 It has been shown that existing federal office buildings offer potential targets for terrorists and that if an incident was to occur, the consequences would be great. In a multitenant federal offce building, certain agency tenants may be more vulnerable to a terrorist act than others. A vulnerability analysis of a building can reveal strengths and weaknesses of a building from a security standpoint.

Recommendation 5 A vulnerability analysis for every federal office building should be undertaken as the first step in the implementation of a building security program. This vulnerability analysis should be a dynamic document and should undergo systematic and ongoing reviews. The analysis should consider the mix of agency occupants especially regarding those agencies at higher risk of being targeted than others.

Conclusion 6 Effective and coordinated analysis of threat information and building vulnerability will determine what, if any, security modifications should be implemented.

Recommendation 6 Government agencies that own or occupy office buildings should initiate procedures to adopt security measures, where appropriate, and respectful of legal considerations concerning the rights of those who use or visit the building. Each federal office building should have a base line or minimum level of protection established for its use. It is the responsibility of the security management team to determine the minimum level of protection.

Conclusion 7 In response to a threat assessment, several levels of security measures can be undertaken varying from temporary to permanent.

Recommendation 7 When temporary security measures are taken in response to a threat assessment, they should be systematically reviewed for removal upon withdrawal of the threat. The review should also evaluate whether the security measure should be left in place where such measures do not impair the functions of the building.

Appendix A

VULNERABILITY CHECKLIST

The following checklist is provided as an example of information required for a vulnerability analysis. The committee recognizes that agencies may have different requirements for such an analysis, but the information gleaned from such a checklist could serve as a base line for a vulnerability analysis.

1. Security manager

(a) Date _____

(b) Facility _____

(c) Address_____

(d) Manager _____

(e) Phone number ( )-_____

2. General facility function and tenants

(a) Leased or owned _____

(b) Number of employees _____

(c) Hours of operation

Mon-Fri.	Shifts		Sat-Sun	Shifts
___	___	open	___	___
___	___	closed	___	___

(d) Tenant agencies of facility

_____
_____
_____

(e) Identify critical missions, functions and personnel

_____
_____
_____
___

3. Building construction, perimeters and entrances

(a) Exterior walls (floors 1 thru 5)

1. Thickness: 1-___ 2-___ 3-___ 4-___ 5-___
2. Material: 1-___ 2-___ 3-___ 4-___ 5-___

(b) Framing system _____
(c) Total building height _____
(d) Exterior door construction _____
(e) Window size and type _____
(f) Number of entrances _____

1. Delivery ___ Controlled ___
2. Employee ___ Controlled ___
3. Public ___ Controlled ___

(g) Fences

1. Type ___
2. Height ___ft
3. Distance from building ___ft

(h) Clear zone ___ft
(i) Secured zone ___ft
(j) Blast zone ___ft
(k) Overhead or underground passage ways _____
Controlled _____
(l) Window height above grade _____
(m) Percent of wall area in windows _____
(n) Roof and utility openings _____
(o) Tenants adjacent to facility _____

_____
_____

(p) Height of adjacent buildings _____

_____
_____

4. Vehicle movement and controlled areas

(a) Locate public and employee parking areas

_____

_____

(b) Distance from facility that vehicles can park___

_____

(c) Authorized vehicles marked with permits_____

(d) Public parking under or adjacent to facility_____

(e) Security force controls traffic flow_____

5. Lighting systems and locations

(a) Perimeter lighting _____

(b) Parking area lighting_____

(c) Entrances lighted_____

(d) Interior lighted after hours_____

(e) Security lighting system

(1) Perimeter system_____

(2) Back-up system_____

6. Locking controls

(a) Facility keys controlled_____

(b) Positive ID issued_____

(c) Compartmentalized facility_____

(d) Area control system_____

(e) Key control system_____

7. Alarms (Note if interior or exterior)

(a) Type_____

(b) Location_____

(c) Maker_____

(d) List of authorized alarm control personnel_____

_____

(e) Closed-circuit television_____

(f) Motion detection_____

8. Security force

(a) Number of guards_____

(b) Number of posts_____

Roving ___ Fixed ___

Checkpoints _____

(c) Hours facility is under protective service

Mon-Fri ___ Sat-Sun ___

(d) Guards reviewed_____

How often_____

(e) Updated on terrorist threat ___ How often _____

1) Evacuation routes ___ Reviewed _____
2) Door closings/monitoring ___ Reviewed _____
3) Areas to be searched ___ Reviewed _____ and sequence
4) Notify local law ___ Reviewed _____ enforcement

9. Employee and visitor controls

(a) Is there a vistor check-in post _____
Where is it located___

(b) Are visitors escorted through the facility
_____

(c) Positive ID systems used_____
Types and locations_____
_____

(d) List of other companies and their employees allowed to enter the facility

Company	Employees
___	___
___	___

10. Mail handling areas

(a) Single handling area_____
(b) Multiple areas___
(c) Procedure for checking for letter/package bombs ___
(d) Are incoming deliveries on sealed trucks
_____
(e) Are seals checked_____
_____
(f) Inspection of supplies and materials_____
_____
(g) How close are outside storage areas to the facility
_____

11. Information (control of classified)

(a) Is classified material checked out by a single individual
_____
(b) Paper waste disposal_____
(c) Daily check_____

12. Trash pickup and scrap control

(a) Are vehicles checked in or inspected upon entry to facility _____

(b) Are containers next to facility_____

(c) Are pick up hours and dates fixed_____ _____

13. Personnel security checks

(a) Are background investigations conducted_____
How often_____

(b) When are keys and positive ID devices given to new employees _____

14. Symbolic characteristics of the facility

(a) High ranking or very important persons in facility _____ _____

(b) Facility open ___ closed ___

(c) Shrines, museums housed in facility_____

15. Availability of anti-terrorist security force_____ _____

16. Secured communication lines

(a) Primary_____

(b) Back-up communication system_____

17. Response time of security forces
Distance ___(mi) Time ___(hrs)

18. Location in or outside of urban areas
Distance to urban areas ___(mi)
Time ___(hrs)

19. Geographic region and proximity to foreign borders
Description_____
Distance ___(mi) Time ___(hrs)

20. Access to the facility by the public

(a) Roads: Type ___ Distance ___(mi)
Time ___(hrs)

(b) Airfields: Type ___ Distance ___ (mi)
Time ___ (hrs)

(c) Waterways: Type ___ Distance ___ (mi)
Time ___ (hrs)