

GAO

Report to the Chairman, Subcommittee on
Civil and Constitutional Rights,
Committee on the Judiciary, House of
Representatives

June 1988

DOMESTIC TERRORISM

Prevention Efforts in Selected Federal Courts and Mass Transit Systems



042525/136163



United States
General Accounting Office
Washington, D.C. 20548

**Program Evaluation and
Methodology Division**

B-229893

June 23, 1988

The Honorable Don Edwards
Chairman, Subcommittee on Civil
and Constitutional Rights
Committee on the Judiciary
House of Representatives

Dear Mr. Chairman:

In response to your June 19, 1986, letter, this report describes antiterrorism practices undertaken in two components of the nation's infrastructure—federal court facilities and mass transit systems. We present information on the current roles and responsibilities for antiterrorism policies; managers' perceptions of domestic terrorism threats; existing risk-assessment activities to identify threats and the criticality and vulnerability of assets; factors considered in selecting risk-reduction strategies, including the preservation of civil liberties; implemented strategies; and evaluation of the performance, effectiveness, and intrusiveness of preventive measures.

Copies of this report will be sent to the attorney general; the secretary of the Department of Transportation; the directors of the United States Marshals Service, the Federal Bureau of Investigation, and the Administrative Office of the United States Court; the administrator of the General Services Administration; as well as to other persons who request copies.

Sincerely,

A handwritten signature in black ink, appearing to read "Eleanor Chelimsky".

Eleanor Chelimsky
Director

Executive Summary

Purpose

Terrorist acts in the United States have thus far been too few to raise serious public concern, but the nation faces the dilemma of maintaining an effective level of protection without curtailing civil liberties. Concerned that security measures imposed without thorough study and planning may lead to measures that could be unintentionally repressive of civil liberties, the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary asked GAO to describe what was being done to protect against terrorism in two selected domestic infrastructure components—the federal courts and mass transit systems. GAO's study framework consisted of six elements: the roles and responsibilities of units and individuals involved; their perceptions of terrorism threats; the existence and quality of risk assessments; risk-reduction selection factors such as concern for civil liberties; implemented risk-reduction strategies; and evaluations of performance, effectiveness, and intrusiveness. Since GAO sampled only seven sites, used a case-study design, and focused on protective measures, the findings cannot be generalized to all federal courts or mass transit systems or to the totality of U.S. antiterrorism activities. (See pp. 17-23.)

Background

Terrorism is the threat or the use of violence to frighten people and governments into some ulterior political act. Targets include individuals, symbolic structures, political events, and various components of the nation's infrastructure, such as transportation systems, government buildings, and energy facilities. A planned antiterrorism approach could help prevent incidents or reduce losses, while ensuring the preservation of civil liberties. However, little is known about the antiterrorism planning and organizational responses of most U.S. organizations. (See pp. 10-17.)

Results in Brief

Court officials indicated heightened awareness of threats to security because of high-risk trials involving organized crime, drugs, and terrorist groups. The court districts GAO visited have programs to protect against high-risk and more general threats. Their programs include threat assessments, security surveys and plans, and security measures for various threat levels. When selecting risk-reduction strategies, most court officials seriously sought to preserve the openness of the court process and to protect the civil liberties of the general public, but the protection of the participants in judicial activities was paramount in high-risk situations. (See chapter 2.)

Transit officials had no direct experience of terrorist incidents, perceived the likelihood of incidents to be remote, and had no antiterrorism programs. The transit officials GAO talked to described terrorism as a rare emergency event much like natural disasters, for which they do have plans for response and recovery. They also had crime prevention and safety programs to protect people, property, and system operations as well as possible, given the open nature of transit facilities and operations. Transit officials expressed little awareness about the intrusiveness of their protective strategies vis-a-vis the civil liberties of the general public. (See chapter 3.)

Due to the lack of evaluations by both court and transit officials, it is difficult to determine how effective the current strategies are in regard to the threats they were designed to protect against, and what remains to be done to cope with terrorism threats in a manner that also preserves civil liberties. (See p. 84.)

Principal Findings

Federal Courts

The U.S. Marshals Service (USMS), with assistance from other executive and judicial agencies, safeguards federal court facilities and personnel. USMS programs were implemented in the district courts, where some resource and coordination problems were identified. Court officials expressed concerns of various kinds about the possibility of terrorism given the types, frequency, and duration of the high-risk trials that they conduct. (See pp. 24-32.)

The risk-assessment process established by USMS was implemented differently in the seven court districts GAO reviewed. Actual threats were formally assessed. Assessments of criticality were not explicitly conducted, but the vulnerable aspects of court facilities were identified. The courts had emergency response procedures, but placed more emphasis on prevention. (See pp. 32-42.)

Court officials emphasized the selection of risk-reduction strategies that would not negatively affect the openness of the judicial process. They stressed the need for facilities designed for security, emphasized the use of qualified security personnel, and considered the cost and technical quality of the equipment selected. The seven court districts had implemented most of a standard security package USMS provides and had

enhanced their security measures for threatening situations. (See pp. 42-52.)

GAO did not find evaluations of the overall effectiveness or potential intrusiveness of the court security systems. Some technical performance tests and special security surveys had been conducted, including assessments of the adequacy of selected security measures against particular threats. (See pp. 52-54.)

Mass Transit Systems

Local transit authorities are responsible for the safety and security of their transit systems. The Urban Mass Transit Administration (UMTA) has begun a technical assistance project on terrorism prevention and response strategies. Civil liberty issues, however, are not addressed. Local transit officials considered the threat of a terrorist attack to be minimal, and regarded their systems as only secondary targets. GAO found only one risk assessment that was specifically related to terrorism. However, transit officials pointed out numerous critical and vulnerable areas in their systems. (See pp. 55-66.)

Transit officials considered the prevention of accidents and common crimes more important than terrorism prevention. Officials stressed law enforcement for the protection of the public and basic security technologies for protecting transit property. Cost, safety, and practicality were mentioned as important factors in selecting strategies against criminal threats, but no formal selection process was described. An emergency preparedness structure had been established in each system for responding to crime and other emergencies, a structure that might be useful in responding to a terrorist incident. The issue of intrusiveness had been considered at two transit systems, not for the public but only as it related to labor union objections. (See pp. 66-73.)

Transit officials had generally not tested the performance, effectiveness, or intrusiveness of their security systems. A few surveys and studies had been conducted in response to specific security problems. Drills and exercises for responding to emergencies (especially fires) had been conducted, but civil liberties had not been addressed. (See pp. 73-74.)

Overall Planning and Evaluation

GAO found no one executive agency responsible for providing technical information and expertise to federal agencies regarding the planning, coordination, and evaluation of domestic antiterrorism strategies. GAO found neither uniform, systematic, and comprehensive planning efforts

nor sufficient attention being given to evaluating the effectiveness of current activities. (See pp. 84-85.)

Matter for Congressional Consideration

Congressional committees that are concerned about the need for careful planning against the threat of domestic terrorism and about the preservation of civil liberties may want to request that agencies provide information on the strategies they have developed to prevent and respond to terrorist acts. Of special interest would be the extent to which agencies have evaluated the effectiveness and intrusiveness of existing preventive measures, not only for threats in general but also for terrorism threats. (See p. 85.)

Agency Comments

In commenting on a draft of this report, the Department of Transportation found the information generally accurate and the findings reasonable. The Administrative Office of the United States Courts remarked on the report's comprehensiveness and usefulness and supported the need for a realistic, formal evaluation process by indicating plans to take action in this area. The Department of Justice (DOJ) made a number of comments that were helpful, and changes to the draft were made where appropriate. The General Services Administration (GSA) and DOJ contended that coordination problems were minimal. However, GAO found evidence of longstanding problems, such as the unresolved issue of which agency will provide perimeter security. Both GSA and DOJ also pointed to the lack of serious breaches of security as evidence that the present procedures are effective. GAO notes that a lack of incidents alone is not sufficient evidence to conclude that a system's performance is effective. Further evidence is needed before such a cause-effect relationship can be established. The letters from the four agencies and GAO's comments are printed in appendixes III-VI.

Contents

Executive Summary	2
Chapter 1	10
Introduction	11
	Objectives, Scope and Methodology 17
Chapter 2	24
Antiterrorism	24
Practices in the	Perceptions of the Threat of Domestic Terrorism 29
Federal Courts	Risk Assessments 32
	Selection Factors 42
	Risk-Reduction Strategies 47
	Evaluations 52
Chapter 3	55
Mass Transit	55
Antiterrorism	Perceptions of Terrorist and Other Threats 58
Practices	Risk Assessments 61
	Selection Factors 66
	Risk-Reduction Strategies 68
	Evaluations 73
Chapter 4	75
Summary	77
Observations and	Threat Perceptions 78
Matter for	Risk Assessments 79
Congressional	Selection Factors 81
Consideration	Risk-Reduction Strategies 82
	Evaluations 83
	Conclusions 84
	Matter for Congressional Consideration 85
	Agency Comments and Our Response 85
Appendixes	
	Appendix I: Congressional Request Letter 88
	Appendix II: Antiterrorism Programs 90
	Appendix III: Comments From the U.S. Department of 98
	Transportation
	Appendix IV: Comments From the Administrative Office 99
	of the United States Courts

Appendix V: Comments From the General Services Administration	101
Appendix VI: Comments From the U.S. Department of Justice	104

Selective Bibliography	112
------------------------	-----

Tables	
Table 1.1: Objectives and Activities Associated With Four Levels of a Response to Terrorism	14
Table 1.2: Antiterrorism Program Elements and Six Study Questions	18
Table 2.1: Principal Departments, Agencies, and Individuals Involved in Federal Court Security	24
Table 2.2: Characteristics of District Court Threats	31
Table 2.3: Elements of the Court Environment That Are Either Critical or Vulnerable, or Both	41
Table 3.1: Types of Threats of Concern to Transit Officials	60
Table 3.2: Risk Assessment of Transit System Components	64
Table 3.3: Examples of Security Measures Used at Transit Systems in Our Review	70
Table 4.1: Antiterrorism Program Elements and Their Implementation	76
Table II.1: Components of an Antiterrorism Program	90

Figure	Figure 2.1: USMS Threat Response	38
--------	----------------------------------	----

Contents

Abbreviations

AOUSC	Administrative Office of the U.S. Courts
APTA	American Public Transit Association
CCTV	Closed circuit television
DOJ	Department of Justice
DOT	Department of Transportation
FALN	Puerto Rican Armed Forces for National Liberation
FBI	Federal Bureau of Investigation
GAO	U.S. General Accounting Office
GSA	General Services Administration
OS	Office of Safety
OSS	Office of Safety and Security
SWAT	Special Weapons and Tactics
TAD	Threat Analysis Division
UMTA	Urban Mass Transit Administration
USMS	U.S. Marshals Service

Introduction

Terrorism and the fear it creates present a challenge to an open, democratic society that is devoted to protecting its citizens while preserving their freedoms. Because of their concern that responses to the threat of terrorism should be planned with careful attention to the potential effects on the civil liberties of our citizens, the Subcommittee on Civil and Constitutional Rights of the House of Representatives' Committee on the Judiciary asked GAO to provide information on current efforts in two parts of the nation's infrastructure to protect against terrorist actions. (See appendix I for the letter requesting this study.)

Specific definitions of terrorism vary, but a common feature among them is the use of violence for political aims. For example, according to the Federal Bureau of Investigation (FBI),

"Terrorism is 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."¹

Jenkins defines terrorism in a broader context as

"violence or the threat of violence calculated to gain widespread attention by its inherent drama and to create an atmosphere of fear and alarm, which in turn causes people to exaggerate the strength of the terrorists and the importance of their cause. Terrorism is violence for effect, not necessarily for the physical effect on the actual target or victim of the violence, which may be of secondary effect to the terrorists, but rather it is violence for the psychological effect of the people watching."²

Wilkinson defines terrorism simply as the use of coercive intimidation to achieve political goals.³

Distinctions between acts of terrorism and other kinds of criminal acts or warfare are not always clear or easy to make and, as a result, terms such as "terrorist," "guerrilla," and "insurgent" are frequently used to describe the same thing. Fromkin's distinction is helpful in that it distinguishes terrorism from other criminal acts as "a strategy that aims to

¹Terrorist Research and Analytical Center, Terrorism Section, Criminal Investigative Division, Federal Bureau of Investigation, FBI Analysis of Terrorist Incidents and Terrorist Related Activities in the United States 1984 (Washington, D.C.: 1985), preface.

²Brian M. Jenkins, "International Terrorism: Trends and Potentialities," in U.S. Congress, Senate Committee on Governmental Affairs, An Act to Combat International Terrorism, Report to Accompany S. 2236, Senate Report No. 95-908, 95th Cong., 2nd sess. (Washington, D.C.: U.S. Government Printing Office, 1978), pp. 143-144.

³Paul Wilkinson, Terrorism and the Liberal State, 2nd ed. (London: Macmillan, 1986), p. 51.

achieve its ultimate objectives not through violence but through terror."⁴ For example, when a violent criminal kills a government official, the end he has in mind is typically limited to the person of his victim. A terrorist, however, kills a government official for a reason that extends beyond his victim, that is, to create a climate of fear in which the original violence has only an instrumental role. Thus, it is the fear generated by violence rather than the violence itself that achieves the objective.

Terrorism in the U.S.

FBI statistics on domestic terrorism indicate that the annual number of incidents has generally declined during the 1980's. Between 1980 and 1982 there were 122 domestic terrorist incidents. From a high of 51 incidents in 1982, the number declined to 31 in 1983, 13 in 1984, and 7 in 1985. In 1986, 17 incidents were recorded, 9 of which were bombings or attempted bombings in Puerto Rico. Seven incidents were documented in 1987 and none so far in 1988.⁵ A number of groups with a known history of terrorism still exist in this country, but the arrests and convictions of several key members have been followed by a decline in activity. The arrests of members of the United Freedom Front (a leftist group responsible for a series of bombings in the Northeast) and of the Puerto Rican Armed Forces for National Liberation (known as FALN), a separatist group that claimed responsibility for several bombings in the 1970's, and the subsequent decline in the activity of these groups, are examples of this trend.

Although the United States is often perceived as being relatively free of domestic terrorist incidents, data collected by the Rand Corporation and Risks International indicate that this has not always been the case. Until the late 1970's, the United States actually experienced a greater number of terrorist incidents annually than all but a handful of other countries. What differentiates the United States from other countries, however, is that terrorist incidents in this country have tended to be far less severe than those experienced in other parts of the world. In addition, attacks by foreign groups (transnational terrorism) have occurred only rarely in this country, and the majority of incidents have been bombings of property rather than of people. Finally, terrorist incidents in the United

⁴David Fromkin, "The Terrorist Mind," *The New York Times*, June 28, 1987, p. 22.

⁵FBI statistics, however, are not necessarily comprehensive. To be counted as a terrorist incident by the FBI, the situation must involve two or more persons who are engaged in an enterprise involving violent or criminal acts committed in the pursuit of political or social goals. Using this criterion, the FBI excludes certain incidents that other analysts might define as terrorism, such as the bombing of abortion clinics. Despite these omissions, many analysts agree that the FBI statistics do accurately reflect a decrease in terrorist incidents in the United States.

States have tended to be overshadowed, partly because ordinary criminal activity is so prevalent.

The possible reasons for the current low level of terrorist activity in the United States are varied. Terrorism experts frequently mention that the arrest, prosecution and imprisonment of key members of terrorist groups for related criminal activity have kept major terrorist incidents from occurring. Several historical characteristics of American society have been identified as further possible contributing factors. For example, ethnic-based separatist movements have not been prominent in the United States, and domestic ideological splits have not led to the formation of broad-based extremist groups of the left or right. The opportunities for economic and political participation in the United States for virtually everyone also appear to inhibit the kind of frustration that leads to the nihilistic terrorism seen elsewhere. The American political system seems thus far to have been able to assimilate many different forms of dissension. The United States gives explicit constitutional protection to the freedoms of speech and assembly and provides a mechanism for peaceful change, thereby reducing the need for terrorist acts as a means of political protest. Another factor explaining the rarity of terrorist acts carried out by foreign groups on U.S. soil is the perception that it is easier to attack U.S. interests overseas. In addition, international terrorist groups may be wary of U.S. reaction to terrorist incidents directed against domestic targets.

The threat of terrorism in the United States thus appears to be minimal on the basis of recent domestic evidence. What has raised levels of concern about terrorism in the United States, however, is the potential for transnational terrorism. This concern is related to several factors: the large number of attacks against U.S. interests abroad; the continuing presence of the United States in Middle East and Latin American affairs; the statements by officials of the Iranian government containing threats to carry terrorist attacks to U.S. shores; the evidence that a portion of terrorism is state-sponsored and thus better funded and organized; and finally the possibility that terrorists may become attracted to an open society like that of the United States as a result of encountering more effective European efforts at fighting terrorism. The director of the FBI recently testified before Congress that the potential for significant terrorist violence against Americans by both foreign and domestic groups continues to be quite real both at home and abroad.

In the United States, potential targets of terrorism are not difficult to identify. Symbolic structures, such as government buildings and monuments, and politically significant contemporary events, such as a bicentennial celebration, are obvious targets. In addition, various parts of our society's technological infrastructure are vulnerable and thus could also become prime targets of terrorism. Transportation, energy, telecommunications, and other systems provide essential support to the economic, social, and political structure of the nation. Terrorist attacks could seriously disrupt these systems, and therefore measures to protect these infrastructure facilities against potential disruptions should be considered.

Responses to Terrorism

Terrorism is not a problem for which a solution can readily be found; rather, steps can be taken either to reduce the possibility that the problem will occur or, if it does occur, to reduce its consequences. Responding to terrorism is not a simple task. Terrorists have several advantages, such as the ability to choose among a broad range of targets, the selection of the time of attack, and the determination of the method of attack. In addition, terrorists are usually highly motivated, are often well-trained, and tend to have little regard for the consequences of their actions. These factors make it difficult for government institutions to determine what to protect and how to provide protection.

In order to respond to the threat of terrorism, governments such as that of the United States have developed a diverse set of objectives and activities. We found it conceptually useful to distinguish four levels of objectives and activities in the U.S. response to terrorism. (See table 1.1.) The first two levels include objectives and activities to prevent terrorist incidents from occurring (often referred to as antiterrorism efforts); the last two focus on activities to respond to incidents that have occurred (often referred to as counterterrorism efforts).⁶ In practice, however, the activities involved in the four levels are interrelated and, at times, overlap. For example, on the first level, one set of activities that attempts to address the sources of terrorism is the enacting of laws and policies designed to make domestic U. S. targets unattractive to

⁶The terms antiterrorism and counterterrorism were frequently used to distinguish between these types of prevention and response efforts, but we found no agreement on the precise use of the two terms. The Department of Defense's Joint Chiefs of Staff offer a formal definition of both terms: antiterrorism applies to defensive measures used to reduce the vulnerability of individuals and property to terrorism; counterterrorism is defined as offensive measures taken to prevent, deter, and respond to terrorism.

terrorists. However, some of these policies may be the same ones implemented after a terrorist incident occurs, which would place them on the fourth level of our conceptual scheme.

Table 1.1: Objectives and Activities Associated With Four Levels of a Response to Terrorism^a

Level of response	Objective	Activity
1 Addressing sources of terrorism	To thwart terrorist incidents before they occur	National and international deterrent policies and laws; monitoring of suspected terrorist groups; preemptive measures, including arrests for other criminal acts
2 Coping with terrorist threats	To prevent and deter and to provide a safe and secure environment with minimal intrusiveness	Plans for prevention, mitigation, and response; security measures to deter, detect, delay, communicate, and respond; intelligence for early warning; public education
3 Managing a terrorist incident	To minimize casualties and loss of property; to enhance ability to capture terrorists	Procedures for a crisis response; negotiation; use of incident and counterterrorist forces; public information; preserving evidence
4 Recovering from a terrorist incident	To restore operations, calm fears, and maintain public confidence in government	Resume operations; investigate and prosecute terrorists; modify prevention and response plans; retaliation (political, economic, military)

^aGAO limited its study to level 2 of this four-level response to terrorism

Antiterrorism Programs

Although all four levels are important in a comprehensive approach to combating terrorism, the focus of this report is limited to the second level—those activities undertaken to cope with terrorist threats. As noted earlier, activities at this level are often considered to be “antiterrorism” efforts, and antiterrorism is a term we will use in this report.

Although antiterrorism programs have been developed in a few infrastructure areas such as airports and nuclear energy facilities, very little is known at the present time about what antiterrorism policies, plans, or programs, if any, are used by most other infrastructure organizations. Numerous articles and books have appeared in recent years on the nature of terrorism: What causes it; what its effects are; and how governments should respond to it. However, only limited empirical information has been produced about what institutions have done to protect their people and facilities against terrorism.

The approach we have taken in our review of antiterrorism efforts starts from the principle that institutions need a planned, structured program to protect their people and facilities against terrorism. There are many benefits of a planned program. Chief among these are: the increased possibility of prevention and deterrence of terrorist incidents; the likelihood of increased effectiveness of response if an incident occurs; the ability to build-in safeguards and restraints to maximize the

preservation of civil liberties; and the opportunity to organize and coordinate activities among a host of different actors and agencies. Lack of planning increases the likelihood that actions taken by authorities after an incident occurs will involve unnecessary disruption, lessened effectiveness, and potentially greater damage to civil liberties.

An organized program for coping with terrorist threats can be viewed as similar to, and perhaps would be included within, programs for coping with other threats, such as common crimes. Such an antiterrorism program, like other anti-crime programs, would be based on a perception of likely terrorist threats and would involve assigning responsibilities to appropriate offices and individuals. In addition, a series of logically linked efforts would be required in order to develop specific plans and procedures. To initially determine how much protection is needed would involve an assessment of risk. This assessment would begin with a careful analysis of the nature and seriousness of the threat and would also involve analyses of critical and vulnerable targets. Appropriate security or emergency preparedness measures to counter unacceptable risks could then be identified. Measures for the particular environment would then be selected, developed, and implemented, considering such factors as effectiveness, cost, and effect on civil liberties. These measures might include not only preventive ones but also preparations for responding if an incident occurs. The latter efforts may indirectly have deterrent effects and, if implemented, should at least reduce losses from a terrorist incident. Once these measures are in place, their effectiveness could be evaluated. (A more detailed discussion of these elements of an antiterrorism program is provided in appendix II.)

Civil Liberty Considerations in Antiterrorism Programs

Terrorism poses a threat to civil liberties both from those performing terrorist acts and from those acting to protect or react against terrorism. Terrorists exploit democratic rights and often aim to disrupt the governmental and societal systems that guarantee those rights. Such basic democratic rights as those of due process, free association, freedom of movement, and privacy can be threatened and even violated by steps taken against terrorist movements. One costly aspect of terrorism, besides the destruction of physical property and loss of life, is—as terrorists intend—the weakening of the social and political foundations of our democratic society.

According to some experts, the challenge to democracies is to maintain the delicate balance of protecting citizens from terrorist action and the fear it causes while at the same time protecting both the collective and

the individual civil liberties that together ensure the continuation of a democratic society. It is essential for public confidence and cooperation that democratic governments be seen as employing only those security measures necessary to protect the lives and property of their citizens from terrorist attack. However, it is also important that programs to prevent terrorism be examined closely to see what their effects are on civil and constitutional rights. Physical security measures, for example, may affect civil liberties such as those of free access and privacy. Erecting barriers around buildings or checking the identification of those entering buildings may limit public access to and use of buildings. Increased security checks and greater police surveillance and search-and-seizure powers may lead to infringements of the individual's right to privacy. The use of closed circuit television cameras to monitor employees within a building, and of electronic detection devices to search those entering a building, are examples of security measures that may violate the individual's right to privacy.

Some experts point out that in addition to their possible immediate and direct effects on civil liberties, highly visible security measures adopted in response to terrorist threats or incidents can, ironically, intensify the climate of fear and intimidation and, at the same time, lead the public to a false sense of security if the measures are not truly effective. Obvious and obtrusive security measures also can demonstrate both the power of the terrorists to attack at any time and at any place, and the difficulties the government and its security forces face in attempting to protect every likely target all of the time against every type of terrorist attack. Further, terrorists often seek to force the government into undertaking costly security measures that by their inconvenience and their disruption of daily life and commerce serve to alienate the public. Excessive antiterrorist measures may also leave the terrorists with a feeling of having achieved some measure of victory. In a broader sense, security measures that restrict access to and use of public areas could curtail the openness of our institutions, leading to reductions in our ability to accommodate group protest and divergent political and social views—an ability, some analysts suggest, that may have contributed to the current low incidence of domestic terrorism in the United States.

How much security is enough, and to what extent the various security measures are considered intrusive, are questions that are not easily answered in objective terms. The answers depend, to a great extent, on the context at any specific time—that is, on the current perception of the threat of terrorism and the level of fear and alarm that this perception generates, as well as on people's expectations of living in a social

environment that is protective of individual liberties. Some analysts point out that what the public regards as an infringement of civil liberties in the absence of specific terrorist incidents, or at least of a perception of a threat of such incidents, may be demanded as a protection in the presence or even fear of terrorist activity. For example, Department of State officials have stated that video monitors in the reception areas of overseas embassies were carefully concealed as recently as ten years ago to avoid affronting the citizens of the host country. Today, the occupants of those reception areas are uncomfortable unless the cameras are readily visible as evidence that the embassy is interested in ensuring their safety. The challenge to democratic societies is to take necessary precautions while at the same time preventing the enormous erosion of civil liberties that could be made to seem rational in a climate of fear generated by terrorist incidents or even threats.

In summary, in an open society like that of the United States, the ad hoc imposition of security measures may result in an unnecessary level of intrusiveness or some other infringement of individual liberties. Planned measures, by contrast, can be designed to ensure an effective level of protection without destroying democratic freedoms in the process.

Objectives, Scope and Methodology

Objectives

Concerned that responses to the threat of terrorism should be effective while at the same time preserving the civil liberties of our citizens, the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary requested that GAO provide information on current efforts to protect against domestic terrorist actions. In particular, the Subcommittee is aware of the possibility that an ad hoc response to terrorism could be overly repressive of the civil liberties of the general public. The Subcommittee also believes that a way to preclude such overreaction might be to have previously developed plans in place that deal with the issue of intrusiveness in a more careful way than would be possible in time of crisis. (See appendix I for the letter requesting this study.)

Because intrusiveness is a relative concept and therefore difficult to objectively measure, and because there is a lack of available information

about existing efforts to protect infrastructure facilities against the threat of terrorism, it was decided, after consultation with the Subcommittee staff, that we would conduct an exploratory study that would describe antiterrorism programs currently in place at a sample of sites, focusing on two components of the nation's infrastructure—federal court buildings and mass transit systems. Six study questions were developed to guide our data collection. These questions are presented in table 1.2 and described in greater detail in appendix II.

Table 1.2: Antiterrorism Program Elements and Six Study Questions

Element	Question
Roles and responsibilities	Who is responsible for antiterrorism policies and for their implementation?
Perceptions of terrorism threats	What is the current perception of the nature and level of the threat of domestic terrorism among those responsible for countering this threat?
Risk assessments	What processes, methods, or procedures are used to assess the risk of terrorism—including assessments of the threat, the criticality of facilities and operations, and their overall vulnerabilities?
Selection factors	What factors—such as costs, safety, impacts on civil liberties, or on the environment—are considered when selecting antiterrorism strategies?
Risk-reduction strategies	What risk-reduction strategies are being used? (Strategies include structural, design and space use aspects of facilities; policies and procedures; and security measures involving personnel, systems, and equipment.)
Evaluations	How are the implemented risk-reduction strategies evaluated concerning their technical performance, operational effectiveness, and possible intrusiveness on civil liberties?

Scope

Prior to selecting two components from our nation's infrastructure for our case studies, we considered a number of different components, including public (federal) buildings, ports and ships, airports, railroads, mass transit, electric power, water resources, pipelines and storage facilities, and telecommunications. In consultation with Subcommittee staff, we chose federal buildings and mass transit systems because both have traditionally maintained open access to the public.⁷ These two components were also chosen because they are quite different in their overall operations, the number and level of government agencies involved in their management, and security programs in place.

⁷Other areas of major interest, such as airports and nuclear power facilities, were excluded because they were the subjects of other studies.

We later narrowed the scope of our work from public buildings to federal court facilities for our first case study. Many experts view the United States court system as a potential target of terrorism on account of both a general threat related to the symbolic nature of the courts as reflective of democracy in our society, and a more specific threat related to the role of the courts in trying alleged terrorists.

If a terrorist group wanted to make a statement about the "system" in this country, the courts present a very visible target due to their important and highly symbolic role. Further, the courts are a logical target of terrorism, as they have been in Europe and South America, on account of the desire of terrorist groups to obtain the release of their members either before or after sentencing. In recent years, a number of domestic terrorist group members have been brought to trial, found guilty, and sentenced to significant prison terms. These terrorists or their sympathizers may plan to disrupt trial proceedings or plan retaliatory attacks against those courts in which they were convicted. Threats against jury members, judges, witnesses, or attorneys are not uncommon in such trials. Terrorism trials can also lead to increased risk for other targets. Terrorists affiliated with those standing trial may initiate terrorist incidents elsewhere in the hope of asserting some influence over trial outcomes or government policies toward terrorism.

The recent legislation expanding the extraterritorial jurisdiction of United States courts over criminal acts committed against Americans abroad, while important for bringing terrorists to justice, may also increase the threat of terrorism directed against the courts and other domestic targets. Although no international terrorist has yet been extradited, court officials indicated that several extradition requests are currently pending. The Lebanese terrorist Fawiz Younis, though not the subject of a extradition proceeding, was nonetheless seized abroad and brought to the United States to stand trial.

In our second case study, we narrowed our focus to urban rapid rail systems. These systems can be viewed as a possible target of terrorism for a variety of reasons: They carry large numbers of people within concentrated areas and timeframes; they are designed to provide easy access for users and are therefore highly vulnerable; they are networks which cover extensive geographic areas using bridges, tunnels, track and roadways; rapid-rail security systems that would effectively address threats such as terrorism are often not practical; and any major disruptions to service could have serious economic effects on some local communities. If the objective of terrorism is to compel action on behalf

of some identified political cause through fear achieved by violence or its threat, then an attack on a rapid-rail mass-transit system could conceivably generate the desired level of public panic. While rapid rail systems in this country thus far have not been subjected to terrorist attack, their security, safety, and emergency preparedness are manifestly important issues.

In summary, we chose federal court facilities and urban rapid rail systems for this study because they are different in their functions, management, and operations and thus can provide some variation in regard to our six evaluation questions, but also because they are similar in being both highly vulnerable to terrorist attack and also difficult to protect without inconveniencing the public and threatening their civil liberties.

Methodology

In order to gain an understanding of programs for combating terrorism, we first reviewed the literature on terrorism, focusing on domestic terrorism issues. (A selected bibliography is included at the end of this report.) Next, in addition to interviewing experts on terrorism and related issues, we met with representatives of those federal executive departments and agencies with some role concerning terrorism issues, such as staff of the National Security Council that had worked on the Vice President's Task Force on Combatting Terrorism, Office of Management and Budget, Federal Emergency Management Agency, FBI, and the Interdepartmental Group on Terrorism at the Departments of State, Defense and Energy. We also talked with officials from several departments and agencies that have responsibility for different infrastructure components to obtain information about their mandates for dealing with security in general and terrorism in particular. These officials included representatives from the Departments of Transportation, Justice and Treasury, the General Services Administration, and the Nuclear Regulatory Commission. In addition, we visited research, development, and test and evaluation divisions of the Departments of Defense and Energy to obtain information on security technologies and practices. Finally, we convened an advisory panel to extend our knowledge of terrorist threats, antiterrorism issues, protection strategies, law enforcement and physical security system technologies and practices, and civil liberty and constitutional rights issues. We also worked with the Committee on the Protection of Federal Facilities Against Terrorism of the Building Research Board of the National Research Council who were developing guidance for federal agencies to improve the security of persons, buildings, and information against terrorist attacks. Their report, entitled

Protection of Federal Office Buildings Against Terrorism, was published in April 1988.⁷

To answer the evaluation questions related to elements of an antiterrorism program, we chose a case study approach. Our case study method was designed to collect descriptive information illustrative of the antiterrorism practices being used in a judgmentally selected sample of federal court facilities and urban rapid-rail mass-transit systems. In addition to examining specific policies or programs addressing terrorism, we also focused our study on a broad range of activities related to security, safety, and emergency preparedness that might have some application to the prevention of or response to terrorism. Strategies to address situations such as bomb threats or hostage taking by criminal elements are examples of activities that might be applicable to antiterrorism efforts.

Our data came from semistructured interviews that included the use of open-ended interview guides, available documents, and on-site observations. We did not conduct a sample survey or employ other means of structured data collection. We gathered information from appropriate federal executive-agency officials and experts on terrorism issues and related security practices. Our principal data-collection effort, however, focused on gathering extensive information from representatives of our two infrastructure components: federal court facilities and urban rapid-rail mass-transit systems. To obtain information about these components, we visited seven cities in the spring of 1987. The federal court facilities and mass transit systems in these cities provided variation across a number of factors, including geographic location, workload of the court and size of transit system, age of court facilities and transit systems, experience with and awareness of terrorism-related issues, special characteristics of protection practices, and organizations with responsibility for the security of federal court facilities and transit systems.

For help in answering the evaluation questions, we developed interview guides for collecting information from federal judicial and mass transit officials. The guides were used to obtain information about perceptions of terrorist threats, efforts taken to identify risks, strategies either considered or considered and implemented to reduce risks, evaluations of these strategies in response to complaints from the public and employees regarding the alleged intrusiveness of security technologies and

⁷Washington, D.C.: National Academy Press, 1988).

practices, and overall roles in and responsibilities for antiterrorism plans and programs.

At the federal court facilities, we interviewed the chief judge for the district court, judges for other courts (such as appeals and bankruptcy), the United States marshal and his staff, the United States attorney, and other members of the court family such as the clerk of the courts and the circuit executive. In addition, we interviewed the GSA regional representatives, local law-enforcement officials, and the FBI whenever possible. At the mass transit systems, we primarily interviewed either the executive director or representatives from management (or both), and those individuals responsible for security, safety, and operations. If appropriate, we also talked with staff from legal counsel, public relations, and county or regional transit-authority offices.

In addition to our interviews, we requested and reviewed available documentation of annual reports; plans, policies and procedures; and risk assessments, security surveys, drills and evaluations. At the federal court facilities, we visited such areas as courtrooms and judicial chambers, the U.S. marshals' command center, prisoner transportation and holding areas, and other buildings that housed court facilities. We also toured the mass transit systems' operations, including such areas as the control center and selected stations and rail lines.

We analyzed the data for the federal court facilities and mass transit systems separately, using the summaries of interviews, documents, and observations aggregated for each site. We also used information obtained from interviews with appropriate federal agency officials and experts as well as from our literature review.

Our findings regarding antiterrorism practices in federal court facilities and mass transit systems are presented in chapters 2 and 3 respectively, and similarities and differences between the two case studies are discussed in chapter 4. For security reasons, we do not identify particular facilities or systems.

Strengths and Limitations of Our Review

Growing concern about the threat of terrorism has led to a proliferation of written material on various aspects of terrorism, but relatively little has been written specifically about domestic antiterrorism practices. Our collection of information about such practices in two diverse components of our nation's infrastructure should be useful to those involved in developing programs to deal with terrorist threats. In areas where little

has been done to plan for terrorism, our information may be helpful in raising levels of awareness of and consideration given to the possibility of terrorist threats. The identification of existing practices may also provide other institutions with strategies for improving their antiterrorism efforts. In addition, the identification of existing gaps in antiterrorist programs can indicate where government efforts may be needed.

Our data collection about specific antiterrorism practices, however, was limited to the federal courts and rapid rail systems in the seven cities that we visited. These sites were judgmentally selected and are not representative of all federal courts or rapid rail systems. Federal courts differ according to their number of judges, the number and types of cases tried, and the types of buildings they occupy. Transit systems vary in regard to their size, organization, operations, and public use. In view of differences like these, it would be improper to generalize on the basis of our sample of sites about current practices at other federal courts or transit systems. Furthermore, due to our focus on protective measures within these two components, it would also be improper to generalize to the totality of U.S. antiterrorism activities.

We collected most of our information through interviews with various federal court and transit system officials. Our study's accuracy and the completeness of its data, therefore, depended largely upon the availability, cooperation, and recall of those key officials. Furthermore, an assessment of the quality of the antiterrorism efforts described by these officials was not within the scope of this study. Our objective was to document the types of measures, if any, undertaken in selected federal court facilities and mass transit systems to cope with the threat of terrorism, and to provide this information to the Subcommittee in the form of a report.

Antiterrorism Practices in the Federal Courts

Terrorist incidents involving the courts have occurred in several foreign countries and have had an influence on their judicial processes. However, although the court system in the United States has been the target of a small number of terrorist incidents, terrorism has not yet had a major impact on our judicial process. We visited a sample of seven federal court districts to discover what steps were being taken to protect judicial officials, facilities, and operations against possible terrorist attack. This chapter presents our findings as they relate to the six evaluation questions contained in table 1.2. In addition to the information gathered at our sample sites, we include information obtained from experts on either the federal courts or antiterrorism strategies (or both) and from available literature.

Roles and Responsibilities

Evaluation question 1 was who is responsible for antiterrorism policies and for their implementation? Responsibility for protecting the federal courts, which includes securing them against terrorist attack, involves a number of federal judicial and executive agencies. The agency with principal responsibility for the protection and security of federal judicial facilities is the U.S. Marshals Service (USMS) of the Department of Justice (DOJ). Other departments, agencies, and individuals that assist the USMS in fulfilling this protective function are shown in table 2.1. Generally, these agencies set policies at a national level that subsequently are implemented within judicial districts that experience differing threats and security problems.

Table 2.1: Principal Departments, Agencies, and Individuals Involved in Federal Court Security^a

Branch of government	Department, agency, or individual
Federal executive branch	Department of Justice U.S. attorney general U.S. Marshals Service Court Security Division ^b Threat Analysis Division U.S. Attorneys Office Justice Management Division General Services Administration Federal Bureau of Investigation
Federal judicial branch	Judicial Conference Administrative Office of the U.S. Courts Federal district judges
Executive and judicial branches combined	U.S. district marshals Court-district security committees

^aEntities such as local law enforcement agencies and other tenants in multiuse buildings where courts are located also have a role in court security.

^bThis division has primary responsibility for the protection and security of federal courts.

Federal Roles and Responsibilities

The USMS security role for the federal judiciary dates back to the Judiciary Act of September 24, 1789 (1 Stat. 73), which established both a decentralized judicial system and the position of U.S. marshal to serve this system. Under the act, U.S. marshals were appointed by the President to attend sessions of the federal courts and execute all processes and orders directed to them. Marshals were authorized to command all assistance necessary to execute their duties.

In 1861, Congress enacted legislation which placed marshals under the "general superintendence and direction" of the attorney general, also a presidential appointee, and left unchanged the original requirement that marshals attend sessions of court when so directed by the judiciary. In 1870, Congress established the Department of Justice, designating the attorney general as its head. In 1969, the attorney general established the Marshals Service as a bureau within the Department of Justice.

Under the current structure, the President appoints, subject to Senate confirmation, one marshal for each of the 91 judicial districts and 3 territorial district courts, except in the territorial district court of the Virgin Islands where the marshal is appointed by the attorney general. The attorney general appoints the director of the Marshals Service, who has the authority to allocate resources for and set the priorities of the Marshals Service. Marshals, however, are still required to carry out the orders of the judiciary, including attending court sessions when so directed.

Within the USMS, the Court Security Division is responsible for developing security programs. Judicial security is managed through four security program elements:

- Judicial Facility Security Program, which provides security systems and equipment and court security officers;
- Courtroom Security Program, which provides deputy marshals for security in court proceedings and for other duties such as handling juries;
- Personal Security Program, which provides personal security for members of the federal judiciary, trial participants, and other officials whose welfare and safety are threatened during the course of performing their official duties; and
- Technical Assistance Program, which provides assistance to court districts in conducting security surveys and determining security requirements. A physical security inspection program is also included in this function.

A separate unit, the Threat Analysis Division, maintains a threat data base and conducts threat assessments for the various divisions and offices of the Marshals Service.

Providing judicial security is one of the responsibilities assigned to the Marshals Service. Other major program responsibilities include witness security, investigation and apprehension of fugitives, and the handling of federal prisoners. To reduce the competition for available funds, appropriations for the Judicial Facility Security Program are made through the Judicial Branch and the Administrative Office of the United States Courts (AOUSC). Since fiscal year 1984, these funds have been transferred to the USMS Court Security Division for allocation to the court districts. AOUSC has oversight responsibility for monitoring the program's effectiveness and use of appropriated court security funds.

The USMS has responsibility for the protection of court proceedings, court officials, and court areas occupied by the judiciary, such as courtrooms, judges' chambers, and other office areas used by members of the judiciary. This could include areas such as adjacent corridors, lobbies, and even parking areas. The General Services Administration (GSA) is responsible for providing general building and perimeter security. The level and type of protection to be provided is determined by GSA. During unusual situations, such as sensitive trials, GSA will provide additional security, on a reimbursable basis, to the USMS.

The U.S. attorneys, as part of the Department of Justice, are responsible for the protection of their offices. The Executive Office for U.S. Attorneys and the Justice Management Division, in conjunction with GSA who owns or leases their space, assist the U.S. attorneys in providing adequate security for their facilities.

The FBI has no direct role in court security but supports the USMS by investigating threats against court officials and providing intelligence information. The FBI is also the lead federal law enforcement agency for response to non-aviation-related domestic terrorist incidents. As such, it is responsible for preventing, interdicting, and investigating the criminal activities of domestic and international terrorist groups and individuals.

Judicial District Initiatives

Coordination between those agencies responsible for providing security and the members of the court being protected is accomplished through court-security committees in each judicial district. The membership on

the court security committees differed in the districts we visited; however, it usually included the U.S. marshal, the U.S. district court chief judge, the U.S. attorney, the clerk of the court, and a GSA representative. Some committees also included other judges from U.S. district, appeals and bankruptcy courts, and circuit-court executives. Court security committees were chaired by either the district court chief judge or his designee, or the U.S. marshal. All these committees met on an as-needed basis, which in most districts averaged about once or twice a year.

According to the USMS and confirmed by our interviews with court personnel in seven districts, the purpose of the court-security committee is to provide a forum for members of the court to identify and discuss security needs and also to provide some input into the development of ways to respond to problem areas. The range of items generally discussed by the court-security committees included proposals for security resources, plans for security improvements, and security problems brought to the committee's attention either by its members or by other court employees. Annually, the district marshal prepares and submits a security budget plan to the committee for approval before forwarding it to USMS headquarters for review and to AOUSC and the Judicial Conference for budget considerations.

In addition to the roles and responsibilities of the USMS, GSA and AOUSC, individual district judges may, and on occasion do, dictate changes in security arrangements through the use of court orders. We found, for example, that in one district we visited, responsibility for perimeter security had been transferred from GSA to the USMS by a court order signed by all the federal judges in that district. The reason for this action was concern by the district judges that security was insufficient to address the threat related to an upcoming high-risk trial. In other districts, court orders had been issued requiring the presence of marshals in the courtroom or dictating the use of specific security technology.

Concerns About Roles and Responsibilities

The designated judicial branch funding and the establishment of most of the district-court security committees cited in our review were based on recommendations contained in a 1982 report by the Attorney General's Task Force on Court Security. The Task Force was appointed in 1981 by the attorney general because budget reductions, funding uncertainties and reductions-in-force, as well as an existing fragmentation of responsibility for court security between the USMS and GSA, had caused concerns about the provision of security for the judiciary. At the time, these concerns were associated with a court environment in which the number of

judges and the number of complex and sensitive cases had grown. These factors contributed to a heightened concern about the adequacy of existing security arrangements.

Based on their examination of the court security requirements, the Task Force developed a number of recommendations for protecting the federal judiciary and maintaining the integrity of the federal judicial process. Their 1982 report provided basic policy guidance, endorsed by the attorney general and the Chief Justice, for the implementation of current security plans and procedures. This guidance was formally reiterated in 1984 in memorandums of understanding between the USMS and AOUSC, and again in 1987 between the USMS, AOUSC, and GSA.

Although these memorandums of understanding established guidelines and procedures to implement security recommendations, the court officials we interviewed indicated that many of the same issues addressed in 1982 exist today, even though improvements had occurred. Responsibility and resources for, and the adequacy of, perimeter security were still at issue. Court officials in most of the districts we visited expressed concern over the level of perimeter security that GSA had provided. As a result of this situation, the USMS had assumed a greater role in the provision of perimeter security in some court facilities. In two of the district court facilities we visited, for example, GSA had almost totally relinquished its responsibility for building security. In several of the court districts we visited, GSA officials expressed concerns about the negative perceptions of court officials regarding the security GSA provided. In one district, a GSA official emphasized that he perceived his agency's role as one of performing management functions rather than providing direct services. In another district, GSA officials indicated that, according to their assessments, the existing levels of security appeared to be adequate but that security could be enhanced if tenant agencies would cover the cost increases.

Many of the court officials we interviewed emphasized that they relied on the experience and expertise of their district's U.S. marshal for security matters. These officials supported the efforts of the Marshals Service and felt that the marshals were doing a good job. In a few districts, however, officials expressed some concern about the adequacy of existing antiterrorism security arrangements. These officials suggested the need for other sources of information and expertise on terrorism prevention measures. In one district, court officials expressed concern about the ability of government agencies, which lack experience and expertise

with terrorism, to develop adequate plans and programs to prevent terrorism.

Another area of concern involved the role of the FBI as the lead federal agency for responding to domestic terrorist incidents. In one court district, federal and local agencies, including the FBI, participated in a command-post exercise, which simulated a court-related terrorist incident, in order to identify coordination issues. At the conclusion of this exercise, officials from both court security and other federal and local law enforcement agencies challenged the FBI's lead agency role. A court security official in the district involved stated that the U.S. marshal has statutory authority over other law enforcement officials for the protection of the judiciary. According to this official, this authority would extend to any terrorist incident involving a threat against a court facility or member of the judiciary. Officials from the federal legislative branch who participated in the security exercise also questioned the FBI claim to lead-agency status in the case of an incident that occurs in a legislative office building, stating that the FBI's lead-agency designation only applied to executive-branch agencies. (Local law enforcement officials asserted that the FBI lead-agency role only applied to federal agencies.)

Summary

Federal court security involves several executive and judicial branch agencies at the federal level and court participants and U.S. marshals at the district level. The principal policies and programs to protect the courts are provided by the USMS. Other agencies and participants have responsibilities for the security of particular court components, program oversight, and the implementation of security measures. The ability of all of the participants to provide the necessary resources and to coordinate efforts in planning for and responding to a terrorist incident was a concern raised by several court officials we interviewed, and this same concern surfaced during a major antiterrorist exercise conducted in one district. While improvements in coordination have been made, problems remain—in particular those involving GSA's role in providing perimeter security.

Perceptions of the Threat of Domestic Terrorism

Evaluation question 2 was what is the current perception of the nature and level of the threat of domestic terrorism among those responsible for countering this threat? While court officials in our study indicated an awareness of the general threat of terrorism in this country, they showed greater concern about threats more directly related to their

court districts. Their awareness of the general threat of domestic terrorism had been heightened by recent terrorist incidents directed against American interests overseas and courts in other countries. Court officials expressed concern about the possibility of these incidents occurring in the United States but characterized the threat as moderate. If international terrorism were to invade this country, the courts would be a likely target according to the court officials we interviewed. The symbolic nature of the courts was mentioned frequently as a reason for this likelihood. In several districts, other facilities were also suggested as likely targets. These included government buildings, corporate headquarters, and other visible infrastructure facilities (such as bridges, monuments, and transportation facilities). Courts, however, were most often viewed as the potential primary target of domestic terrorism.

Perceptions of Potential Threat Sources

The threat of terrorism was viewed by court officials in our study as part of their overall concern with the high-risk trials that are conducted periodically in many court districts. Trials involving groups such as terrorists, crime syndicates, motorcycle gangs, and drug distribution organizations were often considered likely targets of terrorist threats by the officials we interviewed. These groups pose a threat to the courts for a number of reasons: They are generally charged with serious and often violent crimes, they have considerable resources at their disposal that could be used to obtain their release through nonlegal means, and they have a history of making threats against the court system. In addition, trials involving these groups are often highly visible and generate a good deal of attention in the media. These factors contributed to a heightened level of awareness on the part of court officials of the possibility of terrorist threats.

The court-district officials at our study sites varied in their responses according to their differing perceptions of the seriousness of the threats against their courts. These responses were associated with the number of high-risk trials held in the court districts and with threats emanating from the local community. (See table 2.2.) Five of the seven court districts in our review had completed high-risk trials in recent years or were in the process of conducting such trials. In these districts, concerns about the threat of terrorism were heightened by specific cases, many of which involved terrorist groups. Officials in one district were particularly concerned about the possibility of having to try extradited, state-supported terrorists. In a sixth court district, officials described a threat

climate that was broader in context and more constant than a case-specific threat. In this district, there was a perception of a long-term terrorist threat directed against the entire court district, rather than a short-term one related to a specific case. Here, officials indicated that, because of the large number of high-risk trials being conducted in the district, there had been a continuous threat in effect for the last few years. The seventh court district in our study had a very limited history of high-risk trials. Officials from this district perceived the threat of terrorism to be minimal.

Table 2.2: Characteristics of District Court Threats

Site	Experience with high-risk trials	Local community environment
1	Terrorism trial in progress, generating a high level of concern	Some remnants of support for leftist terrorist organizations
2	A moderate number of important terrorist trials held in recent years	Concern about activity of gangs with linkages to terrorist organizations
3	Several drug-trafficking trials, creating a threat of terrorism against the entire court	Immigrant population, opposed to certain foreign governments, that has resorted to violent acts in the past
4	Several lengthy, multiple-defendant trials involving organized crime, terrorists, and drug traffickers	Concentration of terrorist groups known to be active in the area
5	Very limited number of high-risk trials in past	Family and church-oriented community, not supportive of terrorism
6	Periodic high-risk trials held in past	Community tolerance of dissenting political views, reducing potential for terrorism
7	Periodic high-risk trials and concern about possible terrorist extradition trials in the future	Threat of protests against government

Several interviewees in the court districts we visited described the terrorism threat more broadly in terms of the local community environment. Officials in one district noted their community's history of gangs that have participated in terrorist related activities, such as maintaining bomb factories and safehouses. In recent years, at least one of these groups had attempted to align itself with an international terrorist organization. Officials in this district thought that their experience with terrorist trials would probably continue, given the continued existence of gangs supportive of terrorism. In another district, officials described their family and church oriented community as less supportive of terrorists, in their view perhaps one reason why they had not yet experienced terrorist trials.

In addition to their concerns about high-risk trials, officials that we talked with expressed a general concern about other threats which could lead to disruptions or violence in the courts. Of particular concern

to them was the potential threat posed by disgruntled litigants in various civil or criminal cases. The 1979 assassination of a federal judge in Texas highlights the threat posed by such litigants, especially those involved in drug-related cases. Several examples were provided by court officials of alleged assassination contracts directed against members of the court or litigants appearing in court and aimed at harming witnesses or court officials. Court officials also suggested that a threat was posed by unbalanced individuals who are not involved in any court case but who might have some grudge against government institutions or the court system. In one district, for example, officials described an incident in which an individual who was dissatisfied with the ability of a federal program office to resolve a benefit dispute broke windows and threatened to start a fire in the courthouse. Several officials also mentioned public demonstrations as a potential threat to the courts. Protesters have demonstrated at government buildings against controversial court decisions and various federal government policies. These demonstrations were viewed as having the potential to become disruptive and thus destructive of building activities and facilities.

Summary

Court officials expressed concern about a broad range of threats to the courts. Some officials felt that courts, due to their symbolic nature, would be likely targets if terrorism were to increase in this country, but they characterized such a threat as moderately low. Actual threats directed against members of the judiciary by disgruntled trial litigants or convicted felons and anticipated threats related to high-risk trials involving organized crime, drug traffickers, and terrorist groups were highlighted by interviewees. Concerns about such threats varied across the districts we reviewed and were associated with the incidence of high-risk trials and other threat experience. One district that had conducted a series of high-risk trials characterized the threat as constant, serious, and directed toward the whole court district rather than toward a specific case. In the other districts, there was a heightened awareness associated with periodic high-risk situations.

Risk Assessments

Evaluation question 3 was what processes, methods, or procedures are used to assess the risk of terrorism, including assessments of the threat, the criticality of facilities and operations, and their overall vulnerabilities? Of the multiple organizations involved in providing court security, only the USMS and the GSA regularly conducted formal risk assessments. The USMS had undertaken efforts to implement the recommendations made by the 1982 U.S. Attorney General's Task Force on Court Security.

The Task Force encouraged a comprehensive and systematic approach to court security based upon a systems approach and risk-management principles. They recommended institutionalizing security-risk management, which was defined as

“the anticipation, recognition and appraisal of a security risk, and the initiation of appropriate action to remove or reduce that security risk. It assumes that various levels of anticipated risk and actual threat environments can be measured and defined. Risk management also provides for resource justification and allocation on the basis of an assessment of the projected or actual need for court security services.”¹

The following sections describe the USMS risk-assessment initiatives and those of other agencies.

Security Assessments

USMS

Based on the recommendations of the 1982 Attorney General's Task Force, the U.S. marshals were to conduct uniform, comprehensive security surveys of all federal judicial facilities in their districts and develop written security plans, including detailed instructions and procedures for meeting court security needs at various levels of anticipated risks and actual threats of terrorism. The Task Force said that these plans should attempt to balance the public's right of access to a public building—in this case a judicial facility—with the need to protect all participants involved in the judicial process and to maintain the integrity of that process.

The USMS had developed procedures for conducting court security surveys. Standard forms were provided to U.S. marshals that addressed a number of topics for inclusion in a survey. General information on characteristics of the building, occupants, and the immediate neighborhood was required. In addition, specific information on court facilities—such as a description of building access points, size and type of security-guard force, and inventory of existing security equipment—was solicited. A determination of areas vulnerable to intrusion or disruption was also to be made, for itemization in a survey. The survey also was to look at selected court facility components, such as courtrooms and judges’

¹Department of Justice, Report of the Attorney General's Task Force on Court Security (Washington, D.C.: March 1982), p. 2.

chambers, to identify whether security systems were in use and operating properly and to determine vulnerabilities, such as access points.

We found that security surveys were conducted by district deputy marshals or by USMS Court Security Division inspectors, who spend most of their time in the field providing technical assistance to the districts. The USMS was unable to provide security surveys for all of the seven court districts in our survey. However, based on the four surveys that we reviewed, the surveys appeared to have similar features, although there was some difference in the amount of detail provided on building characteristics and vulnerabilities. This was due in part to the differing security considerations and physical configurations of the various court facilities.

Special surveys were conducted in several of the districts we visited in response to scheduled high-risk trials or other increased-threat situations. These special surveys, in contrast to the regular court security surveys, focused on the identification of vulnerabilities and the adequacy of existing security measures against specific kinds of threats that varied across studies. These surveys variously addressed strategies for countering prison escapes, armed assaults, and vehicle-bomb attacks. In two of the court districts we reviewed, outside consultants and federal-agency security personnel assisted in conducting these assessments.

GSA

GSA had developed a process to assess risks using three interrelated components. The first component involved the assignment of levels of criticality, ranging from one to three, based on the sensitivity of the tenant agency's function (such as importance to national security), degree of public contact, and value of the property. Second, GSA regional staff were required to conduct security surveys to identify physical security hazards or deficiencies in a facility. The survey included an inventory of building and tenant characteristics. This information was also used to help determine the criticality levels previously noted as well as to complete the third component, a computer-generated "risk-assessment matrix." This latter assessment included additional threat information, such as the incidence of crime in the building and immediate neighborhood, bomb threats that had occurred, demonstrations conducted, and specifically terrorist incidents that had taken place. The matrix was developed with an algorithm which assigned various weights to the different categories of information. These weightings were then calculated, and an overall risk level was produced. GSA used this risk matrix as a tool to determine adequate levels of security and physical protection for

each building and leased space, including both a standard protection level and special protection measures that could be provided on a reimbursable basis.

We found that while these methods had been established by GSA headquarters, their use by regional officials varied. GSA security surveys were readily available for our review in three of the seven federal court facilities we visited. The three surveys included the general types of information outlined in GSA guidelines and also appeared to take account of the sorts of threat specifically associated with the courts. Two of the surveys concluded that existing court-facility security systems were inadequate in view of the criticality of the tenant agencies' activities. The third survey stated that the present court security system would suffice but that improvements should be implemented when funding became available.

According to the GSA officials we interviewed, the risk-matrix system had only been implemented within the last year and therefore had been applied to only a limited number of federal court buildings. GSA officials in one district indicated that the risk matrix should not be viewed as a comprehensive method of determining risk because the risk levels provided by the matrix were directly related to the quality and quantity of information used as input. The threat information that was used in this district, for example, was limited exclusively to incidents that had occurred. They did not include any consideration of potential future threats.

Emergency preparedness plans for responding to emergencies such as bomb threats, fires, or natural disasters were also available in the court districts we reviewed. These plans were developed through GSA-organized building-occupant committees. The largest tenant agency in a building usually was designated as lead agency for organizing and implementing an emergency plan. Plans included procedures for notifying authorities in case of emergencies, conducting building searches, and evacuating personnel.

Prior to the mid-1980s, a security-compliance form was used regularly to review the adequacies and deficiencies of security programs in U.S. attorneys' offices as well as other Department of Justice facilities. This lengthy form required data on perimeter, building and internal security, and on safeguards for information (for example, tax, grand jury, and personal records), automated data processing, and safety and health.

Executive Office of U.S.
Attorneys, Justice Management
Division

Lacking the resources to continue this regular assessment, the Justice Management Division presently conducts security surveys only when requested. We reviewed reports on facilities in three districts that we visited. The studies had been requested because of concerns about the adequacy of security in relation to perceived threats to personnel and to information related to organized crime, international drug trafficking, and terrorism cases. The studies focused on and made recommendations for changes in physical security systems, the guard services, and office operations, as well as procedures for monitoring building access and safeguarding information.

Threat Information

The USMS and court officials we interviewed distinguished between an "actual threat environment" that was quite specific and an "anticipated security risk environment" that was more general. An actual threat existed when a bona fide written or verbal threat had been made whose aim was either to cause injury to a federal judge, a U.S. magistrate, or other trial participant; or to lessen the integrity of the judicial process in a particular trial or judicial proceeding through intimidation of the threatened party. Anticipated security risks included the potential for violence, an estimate based mainly on factors specific to cases being tried.

Actual Threats

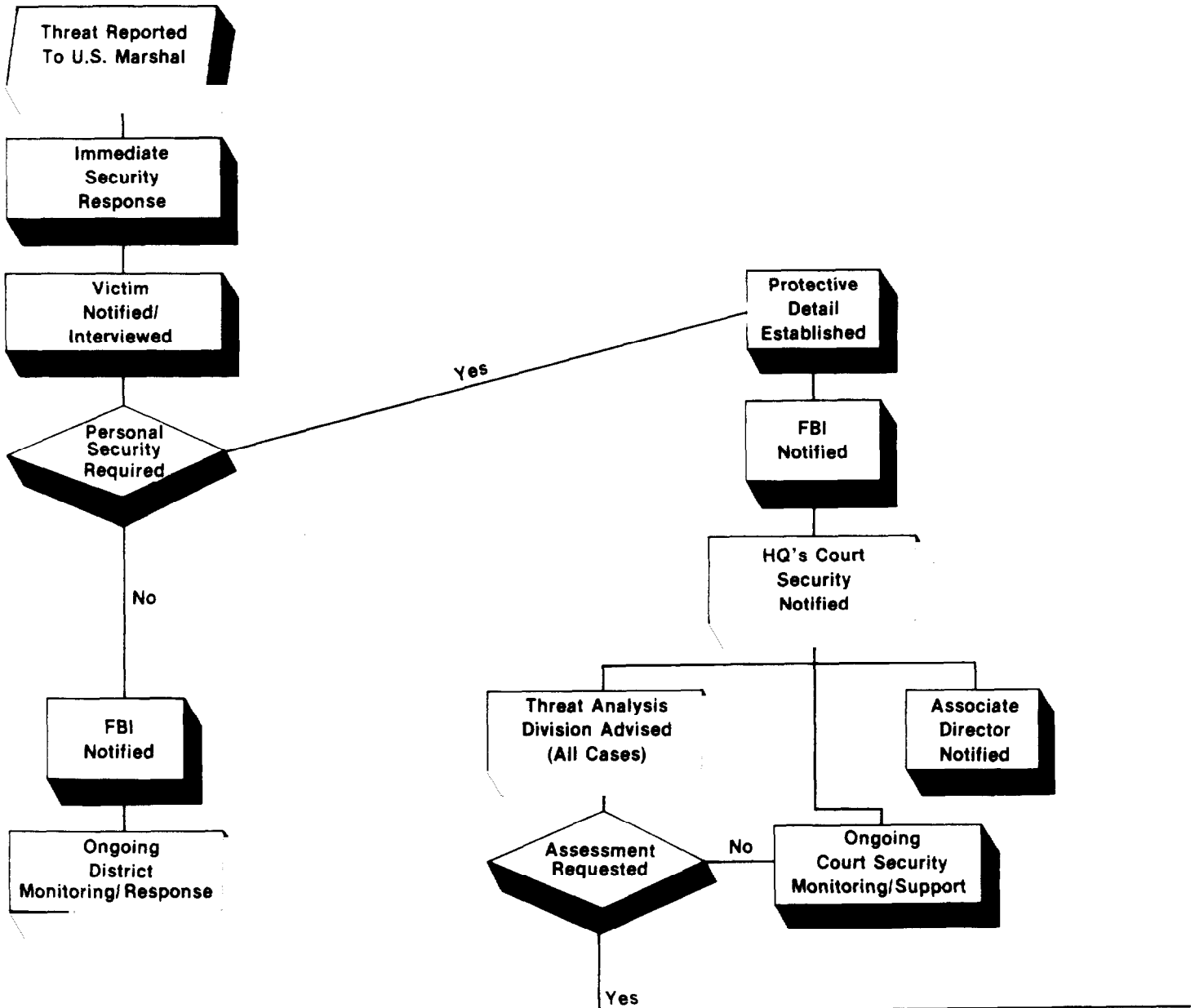
The main activities and decisions to be undertaken in response to an actual threat to a judicial official are diagrammed in figure 2.1 on pages 38 and 39. Generally, threats were initially investigated by the U.S. marshal in the court district of the target. The U.S. marshal could authorize a 72-hour protective detail and forward the information to the USMS headquarters' Court Security Division and Threat Analysis Division (TAD), which was established in 1983 to conduct assessments of the validity of threats received against members of the federal courts. The TAD assessed the intent of the individuals who made the threat, and what their capabilities were, and then produced some estimate of the danger posed to those who were the target of the threat. This assessment was based on information collected from the district that was the source of the threat, background information on the past history of the individual or group responsible for the threat, and current threat information supplied by other federal investigative agencies, such as the FBI, Central Intelligence Agency, and Bureau of Alcohol, Tobacco and Firearms. Because the threat could change over time, subsequent reassessments were made, depending on the nature and seriousness of the threat.

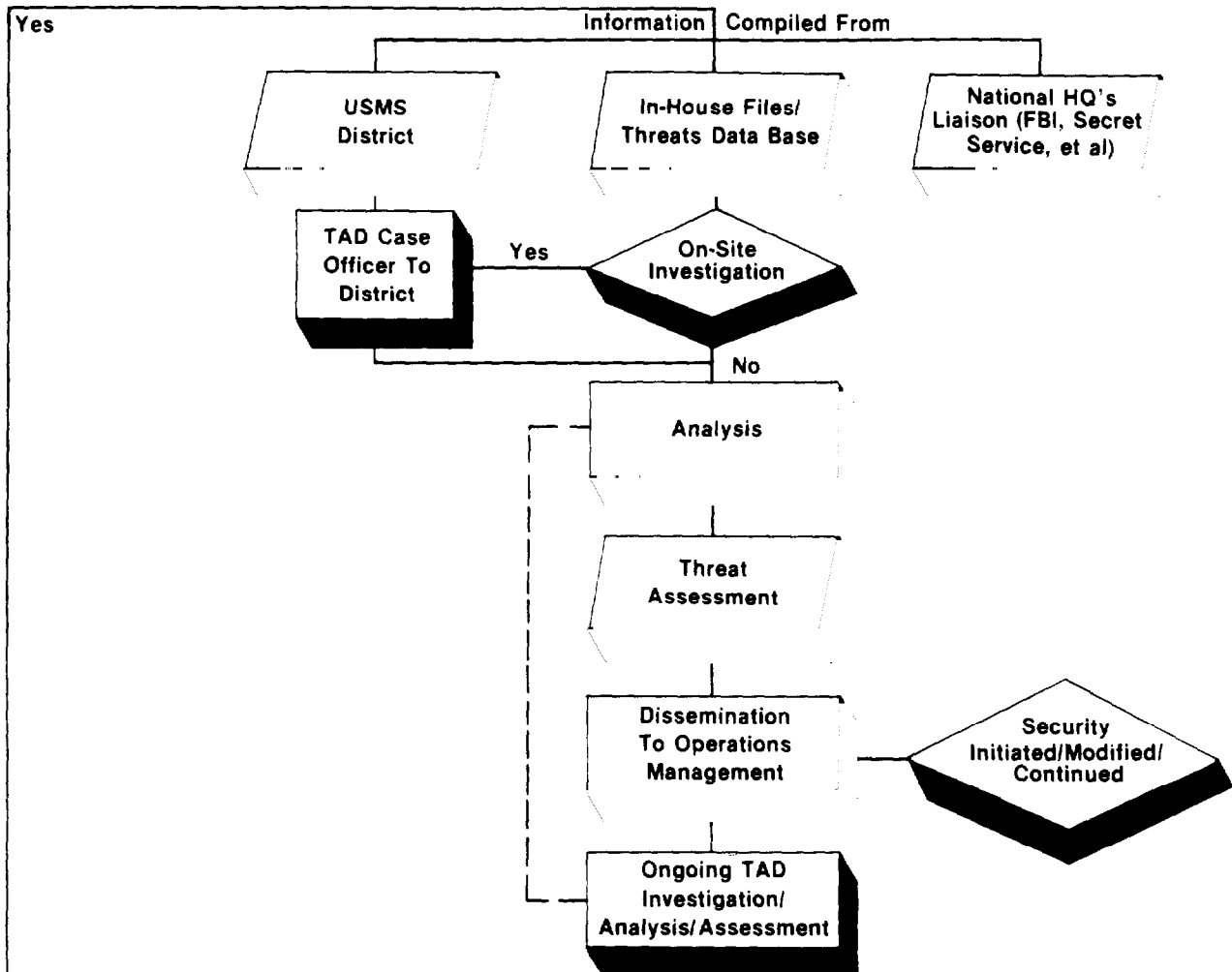
TAD categorized threats as low, medium, or high but did not make recommendations on how the USMS should respond to the threat. (The USMS has attempted to provide TAD with independence from USMS divisions in order to limit the influence of resource allocation issues on threat analysis.) Based on the information provided by the U.S. marshal and TAD, the Court Security Division then decided whether to continue a protective detail or provide other security protection. They also determined when the threat had been reduced to the point that the protective detail should be removed. Our court district interviewees indicated that while this process worked fairly well, there were disagreements at times about the seriousness of the threat and the necessity for protective details.

Having been supplied information obtained from a number of law enforcement investigative agencies, TAD officials then distinguished between intelligence for threat analysis and intelligence for investigations for prosecution. While the latter was useful for threat analysis, it typically had not been shared by investigative agencies because such disclosure might interfere with the development of a case. With increasing experience, TAD had planned to develop its own data base of threat information to expedite its analyses.

According to data provided by the Marshals Service, actual threats against members of the federal judiciary have increased in recent years. During fiscal years 1983 and 1984, there were 271 recorded threats, while in 1985 and 1986 there were 447 identified threats. Of the threats received in fiscal year 1986, about 75 percent were directed against district judges, and the remainder were against U.S. attorneys, magistrates, and other members of the judiciary. The majority of these threats in 1986 originated with individuals. (About 30 percent of the authors of these threats were serving time in prison, while another 40 percent were classified as nonprisoners.) Terrorist-related threats accounted for 2 percent of the total, while organized crime and drug cartels were responsible for 4 percent.

Figure 2.1: USMS Threat Response





Source: U.S. Marshals Service

Anticipated Threats

The 1982 Attorney General's Task Force on Court Security recommended that the determination of an "anticipated security risk environment" (threat) include the consideration of case-specific factors, such as type of trial, subject matter of the case, stage of proceeding, and identity and number of participants. Using these factors, the Task Force further defined an indicator system for identifying four levels of an anticipated-risk environment to guide the court districts in determining appropriate security measures. The lowest level pertained to civil proceedings or criminal pre-trial proceedings where there are no indications of potential disruption or violence (or both); the highest risk level included criminal trials and other proceedings where it is determined that a high potential for disruption or violence (or both) exists.

In the court districts we visited, interviewees described threats using the case-specific factors outlined by the task force. We did not find, however, a formalized process for the gathering and analysis of this threat information. Most court districts relied on informal, ad hoc communication on the assumption that high-risk cases had such visibility that they would be well-known. In addition to sharing information during the district's court security committee meetings, the U.S. marshal and his staff also maintained liaison relationships with local law enforcement organizations. In some cities, terrorism task forces had been established in response to the need for joint investigative activities among the FBI, state police, and local law enforcement organizations. While their focus was on investigation for prosecution, these task forces were also a source of threat information.

One court district in our review had initiated special procedures for sharing threat information. In this district, the marshal had developed a form which was circulated between the clerk of courts, U.S. attorney and chief judge to assist in the flow of information about serious-threat cases and enable the USMS to better meet the demands for security personnel. This district had also recently developed a computerized prisoner-management system so that information was available to those transporting prisoners about a prisoner's potential for violence and the likelihood of an escape attempt.

Identification of Critical and Vulnerable Elements

The court officials in our study sites identified the critical elements in the federal court environment as the individuals, facilities, and information or materials used in carrying out the judicial process. Officials considered these categories of elements to be interrelated rather than mutually exclusive. In terms of personnel, critical elements included the

judges, prosecuting attorneys, witnesses, and juries. The loss of any of these individuals, all of whom are directly involved in the judicial process, could lead to a disruption of ongoing trials. The assassination of a judge, for example, could result in a mistrial or, at the least, a delay in concluding a trial. If, as suggested by officials in one district, a judge was presiding over a lengthy trial and it appeared that a guilty verdict was imminent, a defendant could gain additional time and freedom if the judge were removed from the case.

The facilities in the court environment that were considered critical included those areas where the judicial process formally operated (courtrooms), where critical individuals worked (judges' chambers, U.S. attorney offices, and jury rooms), and where prisoners were held and transported. Similarly, critical information or material included evidence and records that might be essential for developing or presenting a case. In addition, information pertaining to the identification of informants was also viewed as sensitive. (See table 2.3 for a list of court elements.)

Table 2.3: Elements of the Court Environment That Are Either Critical or Vulnerable, or Both

Element	Type
Personnel	Judges, U.S. attorneys, clerks, court executives, probation staff, juries, witnesses, public
Facilities	Judges' chambers, courtrooms, U.S. attorney offices, prisoner holding areas, garage area, clerks' offices, court executive offices, probation offices, other judicial offices, Marshals Service offices
Information	Evidence, dispositions, records, court fees

The vulnerabilities in the court environment were discussed by court officials in relation to protecting the critical entities discussed above. Vulnerabilities associated with various access points to the court facilities were of concern to most of the officials in the districts we visited. Public entrances as well as restricted ones for deliveries or parking were viewed as vulnerable points. This was of particular concern in buildings that housed multiple agencies. Some officials identified the lack of procedures to monitor custodial and maintenance staff within court buildings as another vulnerability. In addition, the failure to adhere to security precautions on the part of some court personnel was a concern to members of the Marshals Service. Examples of this failure included distributing keys to nonauthorized personnel, leaving doors unlocked, and failing to use CCTV monitors.

Summary

In response to the relatively high level of concern on the part of federal court officials over threats, including terrorist ones, the USMS had developed a planning process for assessing various threats, identifying vulnerabilities, and determining security needs. Security surveys that inventoried building characteristics and existing security measures and identified court areas vulnerable to intrusion or disruption, were conducted at the district level. In addition, special surveys which focused on the potentially more serious threat posed by high-risk trial situations were completed in several of the districts in our review. GSA also had developed a facility risk-assessment process which included assigning levels of criticality to federal buildings, conducting security surveys, and utilizing a computer-based risk matrix to determine security requirements. We found, however, that there was variation in the implementation of this process among the districts we visited.

Actual and anticipated threats against the courts were assessed by the USMS Threat Analysis Division when requested. The Threat Analysis Division assessed the individuals or groups who initiated threats in terms of their capabilities and motivations and then provided an estimate of the danger posed to those who were the target of the threat. The elements of the court environment that were considered critical by the court officials we interviewed included the individuals, facilities, and information directly involved in carrying out the judicial process.

Selection Factors

Evaluation question 4 was what factors—such as costs, safety, impacts on civil liberties, or on the environment—are considered when selecting antiterrorism strategies? Headquarters staff of the Marshals Service, Court Security Division, played a central role in the selection of the types of security devices and technologies used and the number of security personnel allocated to the various court districts. The district court officials in our review provided some input into the selection process as well as retained decision-making authority regarding the security measures actually used in their districts. The building entry-control screening systems that were used at many of the court facilities in our review, were selected by the Marshals Service. However, the district court, through either the marshal or the court-security committee, configured the systems to address site-related security concerns.

We found that recommendations or proposals for security measures were part of the Marshals Service risk-assessment process. When security surveys of court facilities were conducted, strategies for reducing risks were often included. Court Security Division officials and district

court officials considered a number of factors in selecting risk-reduction strategies. These factors were not necessarily developed systematically into a formal assessment, but the court officials we interviewed indicated that they were taken into consideration and sometimes discussed in security survey documents or during court security committee meetings. The key factors discussed by these officials included civil liberties, practicality, costs, and technical quality. Officials pointed out that these factors are interrelated, and they did not ascribe any rank order to them.

Civil Liberties

A number of court officials in the districts we visited emphasized that difficulties existed in providing security to federal judicial facilities. Of major concern was how to provide security to safeguard the functional integrity of the judicial process while preserving the open nature of our court system. The interviewed court officials pointed out that security systems must provide protection without affecting too significantly the conduct of the courts. Too much security could disrupt trial proceedings or possibly influence juries who are deliberating a case. Too little security could place court members, jurors, witnesses, court employees, or the public at risk.

The need to preserve the court system as an open, democratic institution was strongly advocated, even if this meant that security risks were increased. Security measures that might create the appearance of an "armed camp" or that could possibly have a negative impact on judicial proceedings, were of concern to court officials. The added security, for example, that surrounds a high-risk trial could give juries a biased impression that might influence their deliberations and possibly even result in a mistrial. Security measures could also damage the defendants' right to be presumed innocent until proven guilty and perhaps even impede the defendants' right to prepare their own defense.

Court officials, sensitive to these concerns, had attempted to provide security measures that were low-key and unobtrusive while, at the same time, equal to any perceived threat. Keeping security low-key involved such things as requiring court security officers and deputy marshals to wear business garb rather than law enforcement uniforms, limiting the use of CCTV monitoring systems in areas where lawyer-defendant discussions might take place, and taking steps to ensure that prisoners are segregated from other trial participants and spectators. This latter point has involved clearing corridors before escorting prisoners into a courtroom and removing prisoners' handcuffs before seating them in front of

juries. Court officials in one district indicated that the effort to keep juries and the public from any contact with prisoners had at times led to delays in conducting court trials because of the time and trouble involved in escorting prisoners to courtrooms, restrooms, and areas where lawyer-client meetings were held.

Court officials in some districts in our study indicated a reluctance to implement a high level of security which might give the impression that the court has "given in" to a threat situation. This view was particularly important in relation to terrorism because one major objective of terrorism is to expose weaknesses in a governmental system and, through intimidation, cause changes in existing policies. One example of this concern that we encountered in two of the court districts included in our review, was the idea of conducting high-risk terrorism trials in a highly secure location, such as a military base. Court officials in these districts were opposed to the use of a military base for holding trials largely because of the negative effect maximum security might have on the trials. These officials felt that the presence of military personnel and other security measures associated with a military base might compromise a juror's objective view of a trial defendant.

Practicality

Practical issues were mentioned by court officials we interviewed concerning both the selection and the implementation of security strategies. Many problems in providing adequate security for the courts we visited stemmed from the fact that a majority of these facilities were not initially designed to meet the threats currently facing the courts. At the time these facilities were constructed, security threats against the courts were not perceived to be an important issue. These court facilities were therefore designed to provide a functional space for carrying out the activities of the judiciary, including an emphasis on providing access to the public. Current efforts to retrofit buildings with security devices often has been made difficult by architectural impediments and resource constraints.

The location of many court functions in multi-tenant buildings containing other federal government agencies or, in some cases, nongovernment offices also had posed some difficulties concerning the provision of security in the court districts we visited. The presence of other federal agencies increased the public traffic in these buildings and thus made it more difficult to implement access-control measures to protect court activities. In some buildings, access control was particularly problematic because court facilities were scattered throughout the building rather

than concentrated in a particular section. In one district building in our study, for example, court facilities were located on ten different levels between the second and twentieth floors. Interviewees pointed out that even when it was feasible to integrate security measures into such buildings, there was still the possibility that such measures might adversely affect the operations of other building tenants. In three of the court districts we visited, some of the court functions were located in facilities which contained only court-related activities. Interviewees indicated that these buildings were often easier to secure, but in some cases there were security constraints due to the historical significance of a building or its neighborhood location. In addition, structural problems, such as the presence of asbestos, were found to be a limiting factor in the implementation of security measures.

We noted other instances of space-use and structural problems in the districts we reviewed. We found, for example, that some court districts' proposals to reconfigure existing court facilities or to install screening systems to improve access-control capabilities were considered from the perspective of their potential effect on building operations or other building-tenant activities. In at least two court districts in our study, major plans to redesign court facilities were proposed as a means to improve security. These plans involved the reconfiguration of various court facilities, including offices, courtrooms, and prisoner holding areas. These plans were judged impractical from the perspectives of cost and level of impact on building activities. In another proposal for security upgrading of a court building, consideration was given to the installation of a screening system on the upper floors of a building where court facilities were located. This proposal was determined to be impractical by the court-security inspectors who conducted the survey due to a lack of space for the screening equipment, an anticipated disruption of the offices near the screening system, a need to reprogram existing elevator service in the building, and the inability of the screening system to limit access to lower floors of the building.

In view of these problems, court officials in several districts and headquarters offices advocated better security planning in the selection, siting and construction or renovation of court buildings. In court districts where there is a greater threat to security, officials suggested that, where possible, buildings be used that are dedicated entirely to judicial activities and are designed with a focus on security. Where multi-tenant buildings are used, these officials suggested that greater attention, especially on the part of GSA, should be given to space-use policies and to the

coordination of court security needs with the needs of other building occupants.

Costs

The level of security in the various district courts is constrained by budget resources according to court security officials in the Marshals Service and in the court districts we visited. These officials felt that the number of court security officers and deputy marshals available was inadequate to counter the level of threat that was perceived to exist. Also, the standard package of security devices recommended by the Attorney General's Task Force for use in the courtrooms and judges' chambers (duress alarms, entry control, bullet-resistant benches) has not been allocated to all court districts. As a result of their limited security resources, officials considered cost an important factor in the selection of security strategies. Officials of the Marshals Service, Court Security Division, for example, indicated that one strategy being considered in the procurement of security devices is the development of inter-agency procurement agreements. Such agreements, involving the procurement of larger amounts of security equipment through inter-agency contracts, could be more cost effective according to officials at the Marshals Service.

At the court-district level, court officials stated that they had little control over budget resources. Their requests for security personnel and devices were submitted to the Marshals Service to be reviewed and integrated with other court-district requests into a national budget request forwarded to the Congress for appropriation through the Administrative Office of the U.S. Courts (AOUSC). Officials in many of the court districts in our study indicated that cost was often the reason given by the Marshals Service when certain requests for security were denied.

Technical Quality

The Marshals Service reported that their physical security specialists reviewed the technical aspects of various security devices and equipment under consideration for use in court protection. These staff did not have a formal testing program but conducted informal assessments of existing commercial security products and relied to some degree on the experience of other agencies with the security products under review. The Department of State, Department of Defense, and other federal law enforcement agencies were mentioned as agencies where useful security-equipment test and evaluation information had been obtained. The Marshals Service did not conduct formal testing of security equipment, but in some cases equipment had been distributed to selected court districts

for a trial run. A new type of magnetometer, for example, was informally tested by three court districts in this way.

Summary

While we found no systematic process in place for the selection of security risk-reduction strategies, USMS and district court officials noted that they did consider such factors as civil liberties and intrusiveness, practicality, costs, and technical quality. We further found that the USMS had chief responsibility for selecting security equipment and allocating resources to the court districts, where court members and the district marshal implemented security measures to meet district needs. Of major concern to court officials we interviewed was the maintenance of a balance between the provision of security and the open nature of the court system. These court officials advocated the use of security measures that would provide adequate protection without negatively affecting the conduct of the courts. However, when the risks appeared great, enhanced security measures were chosen to protect the participants in judicial activities. The issue of practicality was raised with regard to the possible effect of security measures on building operations and activities. The provision of security in buildings not originally designed with today's security issues in mind and where multi-tenant agencies resided was problematic according to interviewees. Court officials at the USMS noted that costs were an important factor in determining the amount and type of security equipment to be purchased. They also pointed out that information on the technical quality of security equipment was often obtained from other federal agencies or through assessments by the USMS.

Risk-Reduction Strategies

Evaluation question 5 was what risk-reduction strategies are being used? (Strategies include structural, design and space use aspects of facilities; policies and procedures; and security measures involving personnel, systems, and equipment.)² Different levels of security were implemented in the district courts we reviewed to address threats whose sources ranged from infrequent high-risk or politically sensitive trials to the more common cases involving litigants in civil proceedings. Officials described certain standard security measures used in court facilities for low to moderate level threats and enhanced measures for high-level threat situations like terrorism trials. Security measures used in the

²The personal protection of key court officials (such as judges and US attorneys) outside of the federal court facilities is important. However, this section concentrates on strategies to safeguard people, information, and physical structures within the court facilities.

courts included a combination of physical security devices and technologies, personnel, procedures and operations, and design-related features. We found some variation in the level and application of security at the court facilities in our review. This variation reflected differences in actual and anticipated threats and site characteristics such as the location and configuration of court facilities. In some cases, variation may also have reflected differences in district needs or requests for security measures, resource availability, and implementation efforts. In addition, in some districts enhanced security measures originally installed for high-risk trials had been retained because of concerns about other threats.

Standard Security Measures

The following are examples of standard security measures utilized in many of the court districts included in our review:

- security personnel stationed at entrances or at various other locations in the court building;
- x-ray machines and magnetometers for screening building visitors;
- CCTV systems to monitor building entrances, corridors, and prisoner cell-block areas;
- duress alarms and CCTV entry-control packages for judges' chambers;
- duress alarms in courtrooms, clerks' offices, and other court locations;
- locks and alarms on building perimeter doors, windows, and gates;
- bullet-resistant material applied to court benches;
- emergency lighting in courtrooms and light switches protected from public access;
- vaults for safeguarding sensitive trial information;
- card entry-control devices for garage entrances and access control systems for cell-block areas; and
- elevators and entrances dedicated to the exclusive use of judges or for prisoner transport.

The following are examples of enhanced security measures being used for high-risk situations in some of the court districts under review:

- screening at building entrances, with secondary screening set up at courtroom entrances;
- an increased presence of security personnel in the court building and courtroom, including arrangements for support from outside law enforcement agencies;

- personal protection provided to key court members in response to specific threats;
- physical searches of courtrooms or other critical areas for weapons or explosive devices;
- use of special high-security courtrooms;
- restrictions on courtroom seating through the use of “small” courtrooms or by requiring visitors to show identification and sign in; and
- the use of sequestered or anonymous juries.

In addition, the officials we interviewed mentioned the following as examples of security measures that had been considered for high-risk situations:

- barriers, including concrete planters and hydraulic vehicle ramps;
- armor coating on building windows;
- moving trials to high-security facilities, such as military bases; and
- closing the courthouse to all but those who are directly involved in a high-risk trial.

Security Personnel

Deputy marshals and court security officers provided a security presence in federal court facilities. Their role was to protect against possible threats and to respond if incidents occurred. Court security officers were deputized with law enforcement authority within the court facilities. Their duties included operating and monitoring entry-control screening systems, patrolling building areas, and guarding various court activities. Court security officers were hired through competitive contract and were required to have graduated from an accredited police academy and to have prior law enforcement experience. They also received additional training at federal law enforcement training centers. Deputy marshals had a broader range of responsibilities related to court security and other federal law enforcement activities. In regard to court security, marshals had been used to perform the duties prescribed for court security officers in addition to providing personal protection for court members, transportation of prisoners, and security assessments of court facilities. Deputy marshals had received formal law enforcement training at federal centers.

The court districts in our review relied on security support from local as well as federal law enforcement agencies. This support had been used for perimeter protection at court facilities during high-risk trials, prisoner transport, and to provide personal protection for court members under threat. Deputy marshals from other districts around the country

had also been temporarily reassigned to high-risk trials. Court officials indicated that tactical-response teams from local or other federal law enforcement agencies would be used for bomb disposal and possibly hostage situations. Most of the districts in our review had experienced intermittent bomb threats, and on at least one occasion a hostage situation involving a disgruntled litigant had taken place.

In each of the district court facilities we visited, the Marshals Service maintained an operations center for administrative work, prisoner holding, and for monitoring security activities throughout the court facilities. CCTV, alarm, and communication systems were typically monitored and controlled from these centers, and any necessary security response efforts were coordinated from here. In three of the court districts in our sample, USMS security personnel were on duty in the court facility at all times. In other districts, security personnel were active only during the normal working hours. If there was a security incident during evening or weekend hours, law enforcement personnel from GSA, if available, or local law enforcement agencies were called upon for assistance.

GSA provided a small number of contract guards and maintained building perimeter alarms that were linked to local or regional GSA control centers or to the Marshals Service operations center in five of the court facilities in our review. In one of the other two court facilities that we visited, the Marshals Service had taken over full security monitoring and guard responsibilities. In the seventh court facility, GSA did not provide an operational perimeter alarm system or guard services because of a perception that the existing threat was minimal.

GSA officials that we interviewed pointed out that their budgets had been so reduced in recent years that they did not now possess the law enforcement resources to provide a timely response to incidents at the federal buildings within their jurisdiction. At the time when we visited the seven court districts, GSA maintained only a small security-response force to cover federal buildings in areas often of several hundred square miles. GSA officials noted that they had developed a greater reliance on local municipal law enforcement agencies in responding to incidents in federal buildings. GSA officials indicated that the perimeter building alarms that are located in many federal buildings annunciate to GSA control centers that are sometimes located far away in other cities or even other states. Where such great distances were involved, GSA officials stated that after an alarm signal was received they would contact the municipal law enforcement agencies with whom they have cooperative agreements and request a response.

Access Control

Screening systems were used as a basic strategy by the USMS to control access to the court facilities we reviewed. We found that six of the seven court facilities had installed magnetometers and x-ray devices either at main building entrances or within buildings at main entry points to the court itself. In the seventh district, the Marshals Service had recommended using a screening system, but court officials had opposed its regular use because of their recollection of disruptions to building activities when a similar screening system had been used in the mid 1970's. Of the six district courts that used screening systems, five screened only building visitors and the other one screened all persons entering the building, both visitors and court employees. In the latter district, court officials perceived a relatively high level of threat associated with various drug-trafficking trials. Concern over this threat led to security efforts aimed at addressing a possible "insider" threat as well as any threat from outside sources. Court security officers in this district set the screening equipment to higher levels of sensitivity and also used informal threat profiles as guides in screening for individuals who might pose a threat to the court. In the other courts that employed screening systems, court employees and government workers with official identification were exempted from screening.

In some cases, access control measures in the court facilities we reviewed also were integrated with building design features and operational procedures. Where screening systems were in place, for example, other building entrances were often closed in order to limit the number of access points. In two of the court facilities, we found that court offices had been moved to different locations within the building to reduce the amount of public traffic around critical areas. For instance, clerks' offices, which receive a high volume of traffic, were relocated to lower floors within the court buildings, and judges' chambers were moved to upper floors where traffic was typically lighter. Similarly, hours of operation were limited in a few of the court buildings in our review to those times when entry-control screening systems were in operation.

Card-entry systems were used to limit access to underground garage areas and to restrict building use during off hours. District-court officials pointed out that the magnetometer and X-ray screening systems did not cover those personnel who entered the building through the garage entrances. Other perimeter access points, such as delivery entrances, were protected by guard stations or CCTV monitoring (or both). CCTV monitoring was also employed around the main entrances of most of the facilities we visited.

Within the court buildings, separate elevators for prisoner transport and for judges were features of the more recently constructed court facilities we visited. These elevators usually operated by key control and were equipped with duress alarms. In the older court facilities, public elevators were used to transport prisoners and judicial officials, except in high-risk situations when elevator use was temporarily limited to prisoner-transport purposes. In one court district, a proximity-access card system was being installed to control access to selected areas within the building, such as the prisoner elevator, cell block area, and the Marshals Service operations control center.

Summary

Different levels of security were implemented in the courts to deal with situations that ranged from high-risk trials to more common civil and criminal proceedings. We encountered both standard and enhanced security measures in these court districts. Although we noted some variation in the use of security strategies, security personnel played a major role in guarding court facilities and their employees and in the management and operation of security systems. Access-control screening systems, alarms and CCTV monitoring were used extensively in the court facilities we visited. Design elements and operational procedures also contributed to overall security programs.

Evaluations

Evaluation question 6 was how are the implemented risk-reduction strategies evaluated concerning their technical performance, operational effectiveness, and possible intrusiveness on civil liberties?

Formal Evaluation

Formal evaluations, to determine if overall court-security systems were effective against the threats they were designed to protect against, were not conducted in the court districts we visited. We found some fragmentary examples of evaluations of existing security measures that were integrated into some of the court-security survey assessments and the court-security inspections conducted by the Marshals Service. These efforts mainly addressed issues related to assessing the performance of security equipment and personnel. In addition, we found that some court districts in our review also conducted periodic technical performance tests of security equipment to determine whether equipment was operational or in need of repair or replacement.

As part of its technical assistance program, the Marshals Service recently established a court-security inspection program in order to conduct physical inspections of court facilities. The intent was to conduct these inspections on a regular basis. However, because of a lack of available resources to carry them out, only a limited number of court-security inspections had been conducted and subsequently documented as written reports. There were no inspection reports available for review in the districts we visited.

One of the intended purposes of court-security surveys—particularly those surveys conducted for high-risk situations—was to determine the effectiveness of existing security measures. In some of the special high-risk security assessments, testing of existing measures was undertaken. This included checking various locations to see if there were areas that CCTV systems did not cover or measuring the time needed to gain access through locked doors. For example, we found one security survey in which a number of cipher locks were tested to see if access could be gained within a set time.

Informal Evaluation

Officials from a majority of the court districts included in our review indicated that security personnel did conduct testing of certain security equipment and measures. In three districts, regular weekly or biweekly testing of alarms, locks, CCTV cameras, and screening system equipment was conducted, according to the officials we interviewed. In the other districts, similar testing was conducted but on an irregular basis. The testing that was conducted at these court facilities consisted of security staff checking to see whether doors were properly locked and setting off alarms to determine whether security equipment was functioning and, in some cases, testing the sensitivity of screening equipment to see whether certain objects could be detected. In one court facility, security personnel had used concealed weapons to test the detection capabilities of a screening system and the alertness of those monitoring the machines. Several court officials also indicated that an additional informal testing situation that had occurred from time to time in many court facilities was the accidental activation of duress alarms by individuals who were unfamiliar with their use. Since all activated alarms must be responded to, court officials viewed these incidents as one way of testing emergency-response procedures.

As previously mentioned, court officials at one of our study sites had recently participated in a terrorism-related command post exercise. This exercise involved several different federal and local law enforcement

agencies and was intended to focus on certain issues of coordination that would be involved in responding to a terrorist incident. The scenario was directly related to a current court concern, the extradition of international terrorists to the United States to stand trial. The exercise involved several concurrent terrorist incidents instigated in an attempt to influence trial proceedings.

As discussed earlier in this chapter, civil liberties were viewed by court officials as an important consideration in the selection of risk-reduction strategies. Civil liberties, however, were not addressed in the evaluation efforts we reviewed. For example, the Marshals Service had made no effort to record instances of intrusiveness caused by security strategies. Court officials that we interviewed indicated that they were aware of only a few incidents that involved concerns about civil liberties on the part of the public or court employees. They recalled a few complaints about the intrusiveness of security measures that were generally related to the installation of screening systems in court-occupied buildings. These complaints tended to originate with defense attorneys who viewed such systems either as an inconvenience or as a threat to lawyer-client confidentiality. The majority of court officials interviewed in our review felt that security measures, such as screening systems, had been generally accepted by the public and by court employees.

Summary

Formal evaluations of overall court-security effectiveness were not conducted in the court districts in our survey. Some assessment was included in the court security-survey process and arrived at through informal tests by district security personnel. These efforts focused on whether security equipment was working and, in the special surveys for high-risk situations, on the effectiveness of security measures to protect against identified threats. While we found intrusiveness and civil liberties to be concerns in the selection of risk-reduction strategies, we did not find these factors included in any evaluation efforts. The court officials we talked with felt that, although some complaints had been made early on, the public had generally come to accept the use of security measures in the court environment.

Mass Transit Antiterrorism Practices

While rapid rail systems in this country have not thus far experienced terrorist incidents, they could become targets like their counterparts in other countries. To answer our six evaluation questions about practices implemented to prevent terrorism (listed in table 1.2), we collected information from eight large domestic urban-rail systems located in the seven cities we visited. As we did in the previous chapter on federal court antiterrorism practices, we present our information together with information supplied by experts knowledgeable in the area and that found in the available literature.

Roles and Responsibilities

Evaluation question 1 was who is responsible for antiterrorism policies and for their implementation? The answer to this question is that roles and responsibilities for the regulation, oversight, and management of mass transit systems are shared by federal and local public and private agencies.

Federal Roles and Responsibilities

Federal government involvement in mass transportation is formally structured by the Urban Mass Transportation Act of 1964. The purpose of the act is to provide assistance to communities for the development of improved mass transportation capabilities. Through a series of programs operated by the Urban Mass Transportation Administration (UMTA), financial aid is allocated to communities for the purchase of transit equipment, and for operating expenses, planning, engineering, and designing of transit systems. In addition, the agency sponsors research and development, demonstration projects, and technical studies that assist in the development and operation of mass transportation systems.

UMTA functions principally as a "grants" agency and not as a regulatory agency dictating how local mass transit systems must operate. The agency has no direct federal government responsibility for operating mass transit systems—which are typically owned by local intergovernmental agencies, quasi-governmental transportation authorities, or private companies. Through its role as manager of federal-assistance grant programs, UMTA has some discretionary authority in awarding grants and thus can indirectly influence how funds are used by transit recipients.

The Office of Safety (OS), recently established as an independently functioning unit of UMTA, provides guidance, research support, and training

assistance on transit safety and security matters.¹ This office reports directly to the administrator of UMTA. Officials in this office, having no direct responsibility for the safety and security of transit systems, view their role as largely one of promoting safety and security awareness within the transit industry. In the past, they prepared guidelines and sponsored research studies on various aspects of transit safety, security, and emergency preparedness. OS has used research centers, such as the Transportation Systems Center in Cambridge, Massachusetts, to develop emergency preparedness guidelines for rail transit systems, to evaluate transit fire-safety measures, and to survey transit security problems and countermeasures. In addition, training programs in rail and bus safety and security are supported by OS through the Transportation Safety Institute in Oklahoma City. One of the security training programs includes a four-hour segment on terrorism prevention-and-response strategies and another half-day segment on explosives-incident management.

There are no policies or programs at UMTA with the specific objective of preventing or responding to terrorism. In 1986, however, OSS began a project through the Transportation Systems Center to assess the threat of domestic terrorism and how it might affect mass transit systems. The purpose of this effort, which is currently in progress, is to learn more about terrorism prevention-and-response capabilities and to disseminate this information to transit system officials in order to raise their level of awareness concerning terrorism. One component of the project involves the collection of information on past terrorist incidents, the characteristics and motives of terrorist groups, and the strategies used by other government agencies for the prevention of and response to terrorism. Civil liberties issues, however, have not been included. A second planned component of the project is a series of regional workshops to disseminate this information to local transit authorities.²

In addition to the mass transit terrorism study, the Transportation Systems Center recently conducted security-related studies and projects for other federal agencies, such as the Department of Defense and Department of State. These activities included the management of a physical

¹Prior to December 1987, this office was known as the Office of Safety and Security (OSS) and was part of the technical assistance function at UMTA.

²Another component initially proposed but subsequently cancelled involved either one or a series of terrorist-related demonstrations. These demonstrations, as proposed, would have involved various terrorist-incident scenarios (such as a bombing, hostage-taking, or hijacking) enacted on different urban mass-transit systems (such as bus, heavy rail, or light rail).

security test and evaluation program, analysis and design of access-control security systems, and the evaluation of telecommunications security measures. Officials at the Transportation Systems Center indicated that an important reason for conducting this work was to develop a core of expertise in security systems work that would be available, should the need arise, for transportation agencies as well as other government agencies concerned about terrorism or other security matters. To date, however, the center has not had a formal role as a clearinghouse for disseminating technical information on security systems to local mass-transit systems or to other government agencies.

Local Transit System Initiatives

At the local transit-system level, we found that response to the threat of terrorism was not identified as a separate initiative by transit officials.³ As a result, specific roles and responsibilities in addressing terrorism were not delineated within these transit organizations. However, roles and responsibilities for security, safety, and emergency preparedness activities were assigned to various organizational units within the systems. All of the transit systems we reviewed relied on municipal fire departments for emergency services and local law-enforcement agencies for backup assistance or tactical-response support.

The transit industry, through the American Public Transit Association, has developed its own system to monitor the safety and security of transit systems. Review boards composed of transit system officials have met on a regular basis to discuss transit safety and security issues and to share information on existing prevention and response practices. In addition, peer reviews of selected transit systems have been conducted periodically either to provide input for the planning of a new system or to assess a transit system's response to an emergency incident. Terrorism itself has not been a specific focus of this organization's effort. APTA officials have been more concerned with basic security issues related to transit crime.

³An office of special planning that addresses terrorism issues has been functioning for several years at one study site. This office was established in response to concerns regarding terrorist incidents at, and threats to the numerous facilities (including major airports, port terminals, bus facilities, heliports, tunnels, a bridge, and a large building, in addition to the rapid rail system that was the focus of our study) operated by the parent organization. The rapid rail component was included in risk assessments conducted by the office of special planning.

Concerns About Roles and Responsibilities

Transit officials interviewed in our study did not perceive a need for greater UMTA involvement in antiterrorism efforts. They indicated that they would rather see an increase in federal support for conventional safety and security problem-solving efforts. According to these officials, UMTA's oversight of safety and security and its technical and training assistance to transit systems have been reduced in recent years due to federal budget reductions. A restoration of federal support for these traditional activities was advocated by these interviewees.

Transit officials at two sites in our review expressed an interest in the establishment of some focal point that could provide expertise on terrorism prevention-and-response planning. They felt that there would be a need for information about the implementation of effective measures against terrorism if the threat of terrorism increased, but they did not specify where such a focal point should be located in order to be most helpful to them.

Summary

Although UMTA does not currently have policies and programs to address terrorism, UMTA officials have recently shown an awareness of the terrorist threat and have initiated a project to learn more about the subject. In addition, some technical expertise on security systems has been developed through federal-agency contracts with the Transportation Systems Center. Local transit-system officials that we interviewed had not previously shown much concern about terrorism and therefore had not identified roles and responsibilities for addressing terrorism planning. Although the transit system authorities were officially responsible for the safety and security of transit patrons, employees, property, and operations, they coordinated with municipal agencies for emergency-response assistance. Some transit officials believed that it would be useful to establish a focal point from which they could obtain expertise and technical assistance on antiterrorism planning and responses.

Perceptions of Terrorist and Other Threats

Evaluation question 2 was what is the current perception of the nature and level of the threat of domestic terrorism among those responsible for countering this threat? The transit officials at our study sites perceived the current threat of terrorism against U.S. mass transit systems to be minimal, due largely to the lack of incidents or threats against domestic transit systems in the past. Transit officials from several of the systems we visited viewed their transit systems as possible secondary targets of terrorism, and certain government buildings, corporate headquarters, monuments, electric power plants, airports, bridges, or tunnels

as primary targets. This view was based on the perception of the officials that their transit systems had less visibility and recognition than these other facilities. At one transit system, however, officials viewed their system as a possible target if terrorism were to increase because other primary targets in the area had recently added protective security, thus making a facility without much security, such as a transit system, a more attractive "soft" target. Transit officials from two of the systems in our review also felt that their transit systems would not be a likely target because the systems had such a low ridership that any disruption to service would produce only a small effect on transportation in the community.

Perception of Terrorist
Threat

The transit officials we talked with tended to view terrorism as similar to other types of rare emergency events, such as a natural disaster, over which they have little or no control but for which they must be prepared because the consequences could be so great. They also viewed terrorism as a lower priority than other basic safety and security issues, such as the protection of transit riders from criminal acts and the avoidance of transit accidents. The types of threats of common concern to the transit officials we interviewed are listed in table 3.1. Except for bomb threats or bombings, terrorist acts per se were not mentioned as common concerns. Transit officials, however, at times described some of these common threats as similar to those that might be instigated by terrorists (as noted in the table footnote). These officials indicated that their crime-prevention plans and their response, safety, and emergency preparedness procedures for other threats would probably also be used for terrorist incidents because no plans and procedures had been developed specifically for the latter.

Table 3.1: Types of Threats of Concern to Transit Officials

Threat categories	Particular threats
Transit crimes	Vandalism, graffiti Fare evasion Theft from system Vagrancy, trespassing
General crimes	Pickpocketing Robbery of patrons Assault ^a Rape Homicide ^a Arson ^a Kidnapping ^a Bomb threats or bombings ^a Auto theft
Natural disasters	Floods Earthquakes High-velocity winds Snow and ice Lightning
Accidents ^a	Fire Derailment Train collision Death or injury on right-of-way Gas leak or toxic spill Explosion Power failure Structural collapse

^aThe transit officials we interviewed described these events as being similar in terms of strategies and consequences—although not in terms of motives—to terrorist incidents such as assassinations, indiscriminate shootings, hostage and barricade situations, hijackings, chemical or biological poisonings, and sabotage.

Perception of Crime and Accident Threats

Criminal acts were considered a major priority by officials at all the transit systems we visited. Officials were concerned not only with the incidence of crime but also with how the public's perception of transit crime affected transit ridership. The type and level of crime that concerned officials varied across the transit systems in our study. In three of the transit systems, for example, officials described numerous types of crimes as problematic. Grouped together by these officials were crimes against transit property (such as graffiti, vandalism, and fare evasion) and crimes against transit riders (such as pickpocketing, robbery, assault, and homicide). Officials from two of these transit systems indicated that the incidence of these crimes on their systems reflected the generally high crime rates in the urban areas where their transit systems operated. Officials from the third system maintained that the incidence of crime was lower on their system than in the local urban area, but that the public perceived that crime was a problem on the system. In the other five transit systems in our study, transit officials were

concerned about a narrower range of crimes. In these systems—that were largely commuter-oriented in their service—crimes such as pickpocketing, fare evasion, and thefts at transit station parking lots were considered problems.

Accidents such as fires, train derailments, or injuries on the right-of-way, and natural disasters such as floods, were identified by the transit officials in our study as being serious threats that could have a major impact on transit riders, property, and operations. Several of the transit system officials pointed out that train fires or accidents occurring in difficult to reach locations, such as in a tunnel or on a bridge, were threats of particular concern.

Summary

We found that the transit officials in our study perceived the threat of terrorism directed against their systems to be minimal, primarily because there had been no history of such events. These officials felt that if terrorism were to increase in the United States, transit systems for the most part would be viewed as secondary targets in comparison to more visible government buildings and other infrastructure facilities. Officials were concerned largely with problems of transit crime and tended to equate terrorism with rare emergency incidents such as accidents and natural disasters.

Risk Assessments

Evaluation question 3 was what processes, methods, or procedures are used to assess the risk of terrorism, including assessments of the threat, the criticality of facilities and operations, and their overall vulnerabilities?

Formal Risk Assessments

Seven transit systems in our review did not conduct risk assessments with regard to terrorism. Only one transit system had conducted a formal assessment that looked at the threat of terrorism, determined what components within the system it was most important to protect, identified various vulnerabilities of the system, and recommended measures for guarding against possible incidents. The approach used in conducting this assessment was to study the characteristics of past terrorist incidents against nontransit targets and then apply this knowledge to the development of different attack scenarios against the transit system. As part of the assessment, the system facilities were also surveyed in order to identify existing security measures and their adequacy against

a terrorist attack. This survey involved a review of equipment and of system-design characteristics.

While they did not have a formal risk-assessment process for terrorism, we found there was evidence of some risk-assessment activities among the other transit systems we reviewed that focused on crime-related safety and security concerns. In five of these transit systems, security surveys of selected facilities—such as rail stations, rail maintenance yards, and revenue-collection operations—were conducted. The purpose of these surveys, according to transit officials we interviewed, was to inventory existing safety and security measures and to determine where maintenance and replacement of equipment might be needed or possible improvements made. Transit officials indicated that these surveys were completed intermittently as time and resources permitted.

Security assessments were also conducted as part of the overall design-planning process which preceded the construction of four of the newer transit systems in our study. Assessments focused on strategies for deterring crime, detecting criminal activity, and avoiding injuries or losses in the transit system through the integration of architectural features, security devices and technologies, and operational procedures. In the other, older transit systems in our review, officials indicated that security was not a consideration at the time these systems were built, but that security considerations were included in the design of recent rehabilitation and system-expansion projects.

All the transit systems included in our study had formal plans and procedures for responding to emergency situations. Emergency response plans were tailored to individual systems and to the personnel responsible for carrying out the plans, but all tended to address situations that posed a major risk to the safety of one or more of the following: persons, property, and system operations. These plans, for the most part, included the types of response activities listed in the UMTA emergency preparedness guidelines for rail transit systems. The UMTA guidelines recommend that transit systems prepare procedures for

- “• reporting the emergency;
- “• evaluating and establishing the parameters of the emergency;
- “• notifying emergency response organization personnel;
- “• dispatching emergency response personnel and equipment to the emergency site;
- “• coordinating the activities of all emergency response personnel;

- “• protecting passengers, personnel, and equipment at the emergency site;
- “• evacuating passengers;
- “• keeping passengers, employees, emergency response personnel, and other agencies informed; and
- “• restoring the normal operations of the transit system.”¹⁴

Some transit systems had developed special equipment or technical aids for emergency response efforts. A few of the transit systems, for example, had designed emergency response vehicles that could be utilized in fighting fires, evacuating transit riders, or transporting rescue teams. In addition, a couple of systems had created computer-based emergency-response information systems to provide transit managers with information that might be needed in responding to an emergency situation.

Threat Information

Local transit system officials indicated that they have not received information concerning terrorist threats on a formal or regular basis. This lack of information can largely be attributed to the relatively low incidence of domestic terrorism and the lack of threats against transit systems. Officials at only one transit system said that they had received information regarding a specific potential terrorist threat. According to these transit officials, federal intelligence sources had obtained information about an international terrorist threat against a U.S. transit system called “metro.” Since this “metro” system was not specifically identified, a number of transit systems around the country were informed of the potential threat.

The transit police officials we interviewed stressed that they had maintained contact with other municipal and federal law enforcement agencies in the course of regular crime prevention activities. This interaction had occurred through work on joint investigations and joint planning efforts for special events, and through interagency groups such as professional law enforcement associations that met to discuss crime-related issues. Transit officials felt that if an actual threat were identified by another law enforcement agency, the intelligence information would be shared in a timely manner with officials at the transit systems. Officials at one transit system, however, expressed some concern over the fact

¹⁴W.T. Hathaway, S.H. Markos, and R.J. Pawlak, Recommended Emergency Preparedness Guidelines for Rail Transit Systems, UMTA-MA06-0152-85-1 (Washington, D.C.: U.S. Department of Transportation, July 1986), pp. 2-1 and 2-2.

that federal law enforcement agencies such as the FBI have not traditionally been very cooperative with local agencies concerning the sharing of intelligence information. These officials felt that information would probably be shared, but only at the discretion of the federal agency and based on its judgment of the requesting official's need to know.

Identification of Vulnerabilities

The critical and vulnerable components of transit systems as described by officials in our study are summarized in table 3.2. Officials identified these components on the basis of familiarity with their transit systems rather than as a result of any structured assessment. There was little differentiation by transit officials concerning what was viewed as critical or vulnerable, or both. Criticality was discussed in terms of two elements: the level of impact on people (either the public or employees) and on the system itself.

Table 3.2: Risk Assessment of Transit System Components^a

Transit components	Criticality or level of impact		Vulnerability
	People	System	
Stations	High ^b		High
Rail			
Track	Low		High
Cars	High ^c	Low	High
Maintenance yards	Low	Medium	Medium
Switching stations	Low	Medium	Medium
Electric power			
Source for system	Medium	High	Medium
Substations	Low	Medium	Medium
Command control center	Low ^d	High	Low
Revenue collection facilities	Low ^d	Medium	Low
Bridges, tunnels	Medium	Medium	Medium
Fans, vents, and emergency hatches	Low	Medium	Medium

^aThese ratings are based on our assessment of the information collected from interviews with transit officials, available literature, and observations during site visits.

^bDepends on what time of day incident occurs. Greater impact would be experienced during rush hour than non-rush hours.

^cDepends on the location in the system where an incident occurs. An incident at a crossover or main junction would have greater impact than one at an outlying station or track segment. Also depends on the alternatives available, such as redundancies, rerouting capabilities, and other factors.

^dAffects employees only.

Transit officials identified rail stations and rail cars as the areas where transit patrons are concentrated within the system and therefore where the greatest potential for personal injury would exist if an incident such as a bombing took place. Depending on the timing and location of an incident, the level of effect could also be high if certain other components were the target. A bombing of a tunnel or bridge, for example, could cause a high level impact if a train full of riders happened to be caught in that section of the system when the incident occurred.

When disruption to the system was considered by the transit officials we interviewed, they identified the primary sources of electric power to the system and the central command control center as critical elements. The electric power source was considered critical because of the transit systems' dependence on electricity for operating the trains. The central control facility was considered critical by transit officials we interviewed because that is where train traffic is controlled, track power is monitored, communications to train and station operators and to the public are carried out, and where any response to emergency problems typically would be coordinated. Various backup capabilities were designed into the systems, but they are not usually automated or centrally located. Track switching, for example, could be carried out on the system, but in order to do so it would be necessary to manually activate the switches at various track locations. Another critical component mentioned by transit officials was those centrally located stations or track segments that, if damaged, would limit traffic on other sections of the system. However, the degree to which such a component was considered critical depended on the particular transit system's ability to reroute traffic.

With respect to vulnerabilities, officials considered factors such as access to and the lack of protection for various transit elements. Officials at our study sites considered transit systems to be highly vulnerable to damage or disruption from a terrorist attack. This view was based on the fact that transit systems are extensive networks that cover large geographic areas, transport large volumes of people within concentrated timeframes and, for the most part, have not been designed to protect against terrorist threats. Transit systems are closed in the sense that access to them is gained by purchasing a ticket; however, they are also designed to allow for easy access and use by the public. Thus, if a terrorist wanted to attack a transit system, it would not be difficult to gain access to the system and select a target from among numerous alternatives. Particular components identified by transit officials as vulnerable

were rail stations, track areas, and rail cars. The fare collection and central control facilities were considered less vulnerable targets because they had been secured. Some transit components were also considered to have differing criticality and vulnerability factors. Rail tracks, for example, had a high vulnerability rating but low criticality with respect to the potential for impact on the public.

Summary

Transit officials at all but one of the transit systems in our study had not conducted formal risk assessments that addressed the terrorism threat. Some examples of risk-assessment efforts that focused on other criminal threats were evident, however. These included various security surveys of selected transit facilities and security assessments of newer transit systems to integrate crime prevention considerations into design plans. In addition, plans for responding to emergency incidents were available at all the systems we visited.

For the most part, local transit officials had not established a structured process for identifying components of their transit systems that would be considered critical or vulnerable, or both, in relation to terrorist attack. However, these officials did provide information on those components of their systems that they considered critical and particularly vulnerable. Officials characterized transit systems in general as highly vulnerable to terrorist attack. This view was based on the fact that transit systems are extensive, unprotected networks within which large numbers of people are concentrated.

Selection Factors

Evaluation question 4 was what factors—such as costs, safety, impacts on civil liberties or on the environment—are considered when selecting antiterrorism strategies? Transit officials at the systems we reviewed noted that strategies specifically designed to prevent terrorism have not received much consideration in security planning due to the fact that transit officials have felt relatively little concern about the threat of terrorism. These officials pointed out, however, that even if the threat of terrorism were to increase, it would still be difficult, costly, and perhaps impractical to implement certain preventive measures. Any attempt to screen transit passengers to detect explosive devices or weapons, for example, would very likely be too disruptive of normal operations. Similarly, the level of security that would be needed to protect against an armed terrorist assault probably would exceed the resources or capabilities of transit systems, according to the officials we interviewed. One official described the problem in this way: The purpose of a terrorist

attack might be to strangle the transit system, but it is possible that the security measures implemented to prevent such attacks would achieve the same purpose.

Cost and Applicability

We did not find evidence of a structured selection process at transit systems for choosing among alternate risk-reduction strategies for security against crime. The costs of risk-reduction measures, their possible impact on safety, and their practicality in relation to system operations were factors most often mentioned as considerations in the selection of security measures. Requests for security equipment or resources usually competed with the requests of other transit system components in the budget process. Several transit officials we talked with thought that security was viewed as less important than other activities more directly involved in transit operations. The cost and effectiveness of any proposed activity were important, according to officials we interviewed, because reductions in federal mass transit grants, along with rising operating expenses, had imposed general restrictions on spending for transit systems.

Transit officials identified different sources from which they had obtained information on security measures and technologies. In many cases, they relied on the experience of other transit systems and the expertise of professional security contractors. Officials provided examples of instances when they had contacted other transit systems to learn about a particular security technology, such as CCTV, or had requested information on strategies for dealing with particular criminal threats. Transit officials pointed out that security information was often shared through contacts made at meetings of the American Public Transit Association, other professional associations (such as the American Society for Industrial Security), and through informal contacts among transit officials. In addition, at four of the transit systems we visited, officials stated that they had some staff who were specifically knowledgeable about various security technologies.

Concern for Civil Liberties

The use of CCTV provides an example of a technology—either in use or considered for use in all of the transit systems we visited—that potentially intrudes on civil liberties. Factors mentioned by transit officials as contributing to their decisions to use CCTV systems for security included practicality, cost, and maintenance considerations; consideration of the effects of CCTV use on civil liberties played a minor role in their decisions.

In five of the transit systems where CCTV was used, officials advocated its use because they felt CCTV increased monitoring capabilities and provided some deterrence against crime by its very presence. In three other transit systems, CCTV was considered for security but was either not used or only used on a limited basis due to a lack of clear lines of sight and problems in integrating CCTV equipment into the existing transit-station setup. At one of the transit systems, officials were also concerned about vandalism and the adequacy of response capabilities as they were associated with the use of a CCTV system.

We found that the possible impact of security measures on the civil and constitutional rights of transit patrons or employees was not a major factor in the selection of risk-reduction strategies. At two transit systems in our study, there was mention of concerns on the part of transit employee unions over the use of security technologies that were considered intrusive. In these cases, the unions had objected to the use of CCTV to monitor transit workers on the job. According to transit officials, these concerns had some influence on the placement of CCTV cameras in transit stations. This attention to union concerns, however, was distinct from any awareness regarding the civil liberties of the public. We did not find this latter concern to be an important selection consideration for any of the transit systems in our study.

Summary

The officials in the mass transit systems we examined had not implemented any specific antiterrorism strategies and also had not developed a structured process for selecting risk-reduction strategies applicable to terrorism or crime threats. But factors such as cost, safety, and practicality of proposed security measures received some consideration by decision makers. However, the civil and constitutional rights of transit patrons and employees received only minor attention from those involved in the selection of security measures.

Risk-Reduction Strategies

Evaluation question 5 was what risk-reduction strategies are being used? (Strategies include structural, design and space use aspects of facilities; policies and procedures; and security measures involving personnel, systems, and equipment.) In the transit systems we reviewed, risk-reduction strategies consisted of law enforcement activities, physical security devices and technologies, and system-design-related components. We found little variation in the general strategies being used across the sites in our study. Some variation, however, was evident in the extent of use of security measures and the placement of security

devices in the different transit systems. The transit officials we talked to indicated that it was not practical to provide a high level of security protection for all elements of their transit systems. Implemented security measures focused on components viewed as critical and those where security problems may have been identified during risk assessment or planning.

Law Enforcement

Law enforcement services at our study sites were provided through different organizational arrangements. Five of the transit systems had their own in-house transit police force, two had a designated transit police unit provided by the municipal police department, and one system had both. Six transit systems also used contract guards to supplement transit police units. Guards were used at one system to monitor rail stations and at the other systems for property protection and revenue-collection purposes.

The transit police forces we observed operated in a fashion similar to that of regular municipal police forces. Officers received both basic law enforcement training and special transit police training to familiarize them with the transit environment and transit security problems. Transit officials believed that a uniformed police presence in stations and on trains was very important and acted to some degree as a deterrent to crime. Regular patrols by police officers were carried out in all the systems we visited and often were supplemented by plainclothes details.

The transit police officials we talked with had established plans and procedures for several types of incidents, including serious situations like bomb threats or hostage takings. These officials indicated that if serious incidents occurred, they would generally depend on support from tactical-response units (bomb disposal squads and "SWAT" teams) called in from local law enforcement agencies or, in some cases, from nearby military bases. One of the transit systems in our study had its own "SWAT" team. Officials at this system thought that it was important to have such a team available because its members were more highly trained than a normal "SWAT" unit in tactical-response measures designed for use on a transit system. This training included techniques for approaching trains undetected, gaining access to barricaded trains, and using weapons effectively in a transit environment.

All of the transit systems we reviewed had been targets of bomb threats. According to officials we talked to, the number of bomb threats that had

occurred in the past ranged from a few per year at three of the systems, to a dozen or more per year in the other systems. Transit officials indicated that all threats were taken seriously but that response actions were generally undertaken only when there was sufficiently detailed information about the bomb threat. This detail tended to include information on the time and location of the intended bombing. Transit officials emphasized that there were no absolute rules to follow in formulating response decisions; rather, it was often a matter of judging whether to take no action or to respond by conducting searches, closing stations, rerouting trains, or evacuating trains and stations.

Physical Security Measures

Some examples of the security equipment and technologies in use on the various transit systems we visited are provided in table 3.3. Several of these devices (such as fences, gates, lighting, and locks) are fairly standard in the security and safety field and were used extensively in the transit systems in our study. Other devices (such as CCTV, intrusion-detection alarms, and access-control measures) were not in widespread use in the transit systems we reviewed.

Table 3.3: Examples of Security Measures Used at Transit Systems in Our Review

General category	Type of measure	Particular measure
Law enforcement activities	Police patrols (Routine and special)	Uniformed Plainclothes Canine units
Physical security equipment	Closed circuit television	Constant monitoring; video recording capability; alarm-activated; monitored safety zones
	Intrusion-detection alarms	Electro-mechanical Microwave Ultrasonic
	Access control for non-public areas	Employee ID badges; magnetic-card key; employee sign-in procedures; fences and gates; locks; vaults
	Communications	Radio; public address system; emergency station and rail car phones; train-approach annunciator system; silent alarms
System and design-related components	Design	Open-site stations; unobstructed views; barriers; elevated guideways; lighting
	Redundancy	Excess train capacity; spare parts
	Materials	Vandal-resistant stations and rail cars; bullet-resistant station booths

Transit officials emphasized that there traditionally has been a strong overlap between the areas of safety and security on transit systems. A key distinction between the two areas is that security relates to intentional threats or acts while safety relates to accidental events. One illustration of the overlap between safety and security functions is the use of CCTV transit station monitoring in the transit systems we visited. CCTV provided station operators or viewers in a command control center with the capability to monitor potential criminal acts against transit patrons or property. At the same time, CCTV also enhanced safety by providing a better means for assessing crowd size and activity and for monitoring safety violations.

We found that transit systems used CCTV within transit stations to monitor platform areas, fare collection machines or ticket booths, and station access points. Transit officials in these systems considered CCTV to be an important means of preventing station-related crimes such as fare evasion, vandalism, robbery, and assault. Officials emphasized, however, that CCTV systems must always be linked with an adequate response-force capability in order to be effective in crime prevention. In one transit system, CCTV was relied upon almost exclusively in selected stations where there were no transit employees assigned to operate the stations. At these stations, transit police officials had established "safety zones," monitored by CCTV cameras, where patrons could stand while waiting for a train.

Other examples of security measures used in the transit stations in our study were enhanced lighting, gates to block off closed station entrances and to keep unauthorized persons from entering track right-of-ways, fences or barriers around station perimeters, and alarms on fare card machines, ticket booths, and emergency exits. In some stations, operator ticket booths were hardened with bullet-proof material and equipped with silent alarms for use in emergencies. Public address systems were standard equipment in most transit system stations as were radiotelephones for use by transit employees.

Enhanced security measures were evident at the fare collection facilities and the command control centers of the transit systems we reviewed. In both transit components, entry-control measures were used to confine access to authorized personnel. In several transit systems, these measures included formal sign-in procedures and the use of card key or combination access locks. In the fare-collection facilities, measures to protect against theft included CCTV to monitor access points and employees handling revenues, vaults to store collected revenue, and alarms on access

points to detect attempted break-ins. In several systems, fare-collection employees were also required to wear pocketless uniforms or work with a partner to discourage misappropriation of revenue.

System-Design-Related Components

A number of the transit systems we reviewed had examples of design-related elements that helped to reduce the vulnerability of the system to damage or disruptions. (See table 3.3.) Redundancy and excess capacity were built into most of the systems in our study to allow for the continuation of train service if some segment of a system network was disrupted. Types of redundancy included train rerouting capabilities and the use of bus “bridges” to bypass breakdowns that might occur on the system due to train malfunctions, power outages, or maintenance work on a rail line. The ability of a system to overcome such problems depended in part on the size of the system and the linkages among existing rail lines. In fact, officials at one transit system believed that their system was so extensive that it would be very difficult to shut down completely. The ready availability of a supply of spare parts also contributed to a transit system’s ability to more rapidly restore disrupted service.

The use of damage-resistant materials in the construction of transit facilities was also considered an important risk-reduction element. Transit officials that we talked with pointed out that transit stations and other system components were not initially designed to protect against bombing incidents. In most transit systems, however, certain components (such as underground stations and tunnels) were designed with a high degree of structural support. In some systems, these components were designed to withstand natural disasters such as earthquakes and floods. Concern about crime prevention also has influenced the design of several newer transit stations and train cars that feature unobstructed views and uncluttered spaces. Transit officials felt that these design features eliminated many locations where bombs could be hidden.

Summary

A combination of security personnel, equipment and technologies, and design features were used by the transit systems we reviewed to address criminal threats and emergency situations. Law enforcement services were provided by in-house transit police forces or by municipal transit police units. Standard security devices such as fences, gates, and lighting were found on all systems; the use of alarms, CCTV, and entry-control measures was less widespread. Transit officials also noted that it was

not practical to attempt to protect all elements of a transit system. In critical areas of the system and in areas where particular security problems had been identified, enhanced security measures were used.

Evaluations

Evaluation question 6 was how are the implemented risk-reduction strategies evaluated concerning their technical performance, operational effectiveness, and possible intrusiveness on civil liberties? The transit systems that we reviewed did not have structured evaluation plans or programs to test existing risk reduction strategies. Technical performance tests were rarely conducted to determine if security devices were working properly, and operational effectiveness tests were not routinely completed to determine if existing security measures provided the protection that they were designed to provide. Some examples of evaluation studies and exercises were described by the transit officials we interviewed, but these either addressed particular security areas that were identified as problematic or were conducted in response to some major incident on the system, such as an accident. In one transit system, for example, a consultant team with experience in corporate security was brought in to review the fare-collection process. At another transit system, a study was conducted to assess the effectiveness of existing law enforcement protection on the system and to determine whether alternate strategies were needed. A major tunnel fire on one system and a snow emergency on another were the subjects of studies to assess the adequacy of emergency-response efforts.

Emergency Response Testing

Transit officials at all the systems in our study indicated that they had conducted regular emergency preparedness drills and exercises for reacting to incidents such as fires and transit accidents. These exercises were viewed by transit officials as an important means of testing emergency preparedness plans and procedures, training employees and support agencies, and improving interagency coordination efforts. In several systems, "worst case" accident scenarios were included in these exercises. Exercises were usually conducted during off hours when transit system operations would not be adversely affected.

We found only a few examples of exercises involving terrorism related threats. The one transit system that had its own "SWAT" team conducted periodic exercises involving terrorism-type scenarios such as train hostage rescues. Another transit system had participated in a terrorism-response exercise involving several local and federal law enforcement

agencies. This "command post" exercise was organized to test coordination efforts among agency participants. While these exercises served as a means of evaluating emergency-response capabilities, they did not include an assessment of measures designed to prevent unwanted occurrences.

The related issues of the possible intrusiveness of risk-reduction strategies and their impact on civil liberties were not addressed by any transit system evaluation effort. Transit officials were not particularly concerned about intrusiveness, in part because they had not received any complaints from the public about this issue. Most of the complaints received, either through letters or phone calls, involved requests by patrons for more security on transit systems.

Summary

Evaluations of risk-reduction strategies were not performed in any routine fashion by the transit systems in our study. We found some examples of security studies that were conducted to address specific security problems (such as protection of fare-collection facilities) and a few studies that followed major incidents (such as accidents on the system). Emergency-response drills and exercises were conducted in all the transit systems we studied. These exercises were viewed by transit officials as an important means of testing existing plans and procedures for reacting to major incidents. However, we found no effort either to determine systematically the effectiveness of risk-reduction strategies or to explore the possible effect of those strategies on civil liberties.

Summary Observations and Matter for Congressional Consideration

In this chapter, we examine our two case studies in relation to each other in order to compare and synthesize our findings. These two case studies—federal courts and mass transit systems—were selected because of their differences with respect to operations, government involvement, security threats, and public use. In view of these differences, it is not surprising that we also found differences in the level and type of antiterrorism practices in place. In the courts we reviewed, officials had an awareness of terrorism and other high-risk threats. These concerns had led to the development of a process for assessing risks and planning risk-reduction strategies, and to the use of more stringent security measures in the court facilities we visited. In contrast, we found that transit system officials had minimal experience with terrorist-related incidents, had little sense of an imminent terrorist threat, and had not established a structured planning process nor implemented risk-reduction strategies that specifically addressed terrorism. The major similarities and differences that we identified in the antiterrorism practices at the federal court and mass transit facilities in our review are summarized in Table 4.1 and are highlighted in the following sections of this chapter.

Chapter 4
Summary Observations and Matter for
Congressional Consideration

Table 4.1: Antiterrorism Program Elements and Their Implementation

Program element	Implementation	
	Courts	Transit systems
Role and responsibilities		
Federal	USMS has major role but other federal agencies, from both the executive and judicial branches, share responsibility for security policy at the national level	No direct federal responsibility for security. UMTA provides oversight and technical assistance
Local	Implementation responsibility at district level involves several agencies and various court members	Local transit authorities have primary responsibility for safety, security, and emergency preparedness
General observations	Specific policies and programs exist to address security threats, including terrorism Some issues addressed but coordination, resources, and implementation problems remain, including conflicts between USMS and GSA over perimeter security	No major policies or programs to address terrorism but UMTA technical assistance project planned
Perceptions of terrorism threats		
Specific terrorism threats	Moderate awareness of threats based on history of actual threats against courts generally Experience with high-risk trials varied across districts	Little awareness of existing threats based on minimal experience with threats
Terrorism in relation to other security issues	Ongoing concerns with other threats, including high-risk trials, disgruntled litigants, and demonstrations	Treatment of terrorism as rare emergency event similar to accidents and disasters
Risk assessments		
Terrorism risk assessments	Threat validity assessed by TAD; special surveys performed for high-risk situations, including terrorist threats	Only one transit system had performed a terrorism assessment
Related assessments	Regular security surveys conducted by districts Emergency response plans developed	Other activities conducted to address crime, security surveys of selected transit facilities and security systems design planning Emergency response plans developed
General observations	Formal USMS and GSA processes for assessing threat and planning security measures, but implementation varied across districts	No structured process for assessment of threats, criticalities, or vulnerabilities; informal, ad hoc sharing of threat information and knowledge of critical and vulnerable elements
Selection factors	Centralized selection through USMS, some national guidance and standards but also some discretion in implementation at the district level	No federal guidance, no identified structured selection process at local transit authorities Security competes with other operational components in local budgetary process
Issues considered	Increasing threat level warranted standardized basic security and enhanced security for high-risk trials Civil liberties, practicality, costs, and technical quality considered important	Threats did not warrant additional measures Costs and safety considered in selection of crime reduction strategies
General observations	Concern with maintaining a secure environment without unduly affecting the operations, conduct, and integrity of the judicial process	Security secondary to main operations, recognition that antiterrorism measures difficult to implement in transit environment without major effect on operations

(continued)

Program element	Implementation	
	Courts	Transit systems
Risk-reduction strategies		
Standard basic measures	Standard security package for low to moderate level threat	Integration of security personnel, equipment, and design features for crime prevention
	Reliance on security personnel, equipment and technologies, and design features	Greater emphasis on emergency preparations to respond to and recover from incidents
Enhanced measures	Enhanced security for high-risk situations	Additional measures employed for special events
General observations	Protective measures stressed but security remains problematic due to lack of coordination among agencies and to open nature of the courts	Emergency preparedness stressed, protective measures difficult to implement in a network system
Evaluations		
Effectiveness	Security inspection program developed but not implemented on regular basis	Exercises and drills conducted to test emergency response plans but not preventive measures
Performance	Some testing of security equipment by district court personnel	No examples of security system tests identified, some examples of studies to address specific security problems
Civil liberties	No assessment of impact on civil liberties	No assessment of impact on civil liberties
General observations	Effectiveness of current security unknown due to lack of evaluation	Effectiveness of current security unknown due to lack of evaluation

Roles and Responsibilities

There is a direct federal responsibility for the safety and security of the federal judicial system. A history of various threats against the courts has raised levels of awareness towards security among agency administrators, resulting in the development of policies and programs to address a broad range of threats, including terrorism. Although the USMS has the principal responsibility for the protection of federal court facilities and their employees, other agencies of the executive and judicial branches of government assist in providing security. Due to the location of courts within federal buildings, GSA has responsibility for perimeter security and for the building in general. At the local district-court level, further responsibilities for implementing security provisions are delegated to the marshal and to various members of the court.

Since the transit systems that we visited are owned and operated by regional or local quasi-public agencies, roles and responsibilities for security, safety, and emergency preparedness reside chiefly with the transit systems themselves. We found that transit system officials generally had not defined any specific plans or programs for terrorism prevention or response within their organizations, but that they had done so for transit crime, accidents, and other emergency situations. At the federal level, UMTA has traditionally provided some financial and technical assistance to local transit authorities, but the agency has not established policies or programs to address terrorism. A growing awareness

of the threat of terrorism by officials in UMTA's Office of Safety, however, has led to a recently initiated transit terrorism planning project that may provide local transit system managers with basic information on strategies for the prevention of and response to terrorism.

The numerous agencies and individuals involved in providing security to the federal courts have raised concerns about the coordination of roles and responsibilities and the allocation of resources. While interviewees noted that improvements have been made with respect to the coordination of the agencies involved, conflict still remains, particularly about the issue of perimeter-security responsibility. In the transit systems we reviewed, coordination appeared to be less of a problem, but this may be due to the fact that transit systems are largely autonomous organizations. Transit systems had developed agreements with municipal agencies for law enforcement and emergency-response assistance. Several transit systems relied on these outside agencies for day-to-day security, and all transit systems required their assistance in responding to fires and accidents when they occurred. As a result of frequent contact between transit systems and outside security agencies, certain coordination problems may have been overcome or minimized. However, the transit systems we visited had not been faced with the high-risk situations found in many of the court districts we visited, and therefore these systems had not needed to rely on outside agencies for special assistance, a relationship in which coordination problems can arise.

Threat Perceptions

The court officials that we interviewed in our study considered the threat of terrorism to be one of several serious threats against the courts. These officials expressed concerns about high-risk trials involving terrorist groups, organized crime figures, and drug traffickers. In addition, they also included threats from disgruntled litigants involved in civil or criminal trials, threats from individuals who might target courts because of some unrelated grudge against government institutions, and threats posed by public demonstrations in the category of serious threats. Neighborhood crime and emergency events such as natural disasters, although of some concern, were threats of less importance to most of the court officials we interviewed. Court officials' perceptions of threats were associated with the actual threat situations that had occurred in their districts. For example, one court district had a high number of ongoing high-risk trials and characterized the threat of terrorism as a continuous one against the entire district court, while other districts had occasional high-risk trials that posed only a periodic threat to certain court members.

We found that transit officials at the eight mass transit systems in our review had a general awareness of terrorism but that they viewed the threat of terrorism against transit systems as minimal. This perception was largely based on the relative lack of terrorist threats or incidents directed against transit systems in the past. Transit officials tended to lump terrorism together with other types of emergency situations and expressed a much higher level of concern about transit crime in their systems. Crimes against transit patrons (such as robberies or assaults) and crimes against transit property (such as fare evasion or vandalism) were generally considered serious problems by transit officials, along with emergency events such as fires, accidents, and natural disasters.

Risk Assessments

In the courts, we found a structured planning process, although one that was not uniformly implemented across the court districts we visited. The 1982 Attorney General's Task Force on Court Security identified a number of security problems, which led to the establishment of several USMS court-security planning activities. These included a special threat-assessment group to validate court district threats, a court security-survey program to inventory building features and identify court areas vulnerable to intrusion or disruption, and the development of written plans for meeting security needs. For high-risk situations, additional security surveys were conducted with greater attention focused on potential vulnerabilities and the adequacy of existing security measures. GSA also has a process in place for assessing risks to federal buildings. The components of this process include the assignment of criticality rankings to federal buildings based on occupant functions and property value, security surveys to identify vulnerabilities, and a computer-based risk-assessment matrix to determine security needs.

We found only one example of a transit system risk assessment that focused on terrorism. In the other transit systems in our review, we identified a limited number of examples of risk assessment activities related to other threats, such as crime. These included security surveys of various transit facilities and security-systems studies completed for the design of certain transit systems or system extensions. Transit officials indicated that threat information has typically been exchanged on an ad hoc basis through informal contacts with law enforcement agencies and that the identification of critical and vulnerable transit system components has been determined largely through transit officials' familiarity with their systems rather than by any formal assessment process.

Although transit system officials generally did not consider the threat of terrorism in their planning, certain of the planning activities we identified may have some application to antiterrorism strategies. The transit systems we reviewed, for example, have established a structure for responding to emergency incidents. Emergency-response plans have been developed, coordination with various municipal agencies has been set up, and drills are conducted regularly to practice existing plans and procedures. These activities are similar to the kinds of strategies that would be employed in responding to certain types of terrorist incidents. A train fire, for instance, that results from a mechanical failure, or one that results from a terrorist bomb explosion, and a bomb threat from a disgruntled employee versus one from someone claiming to represent a terrorist group, are types of emergencies that would require a similar kind of immediate response, regardless of the fact that the causes of the incidents are different. (However, those attempting to effectively resolve a terrorist incident may need to devote more attention to the question of motives.)

A focus on emergency-response planning may be a reasonable approach given the open nature of transit networks and transit officials' current perception of the terrorist threat as minimal. Further efforts to implement preventive security measures may be unwarranted unless the level of threat increases. However, the lack of risk assessments focused specifically on terrorism makes it difficult to know what different levels or types of security measures are needed for different threat levels. Once risk assessments are conducted, transit organizations may find that existing measures are enough or that only minor modifications are needed to enhance security. The ongoing effort by UMTA to provide information about terrorism prevention and response to local transit authorities may result in more risk assessments and further efforts to address identified risks.

In the district courts, we also found emergency response plans, but there appeared to be a greater emphasis by officials in this sector on the development of plans and measures to prevent incidents. While the district courts had not developed strategies specifically designed to prevent terrorist incidents, officials did recognize different levels of threat, including high-risk situations such as terrorism trials. The planning activities for these high-risk situations appeared to be similar to the planning that would be conducted in an antiterrorism program; what may perhaps be needed is additional consideration of terrorist motives and methods.

Selection Factors

In the courts, security was viewed as an important function by officials we interviewed. Of special concern to court officials was providing a secure court environment without affecting the operations, conduct, or integrity of the judicial process. Court officials pointed out that due to the open nature of the court system, where the right of public access must be maintained, it has been difficult to implement a high level of security protection. In addition, because court facilities were not originally designed to address current security threats and because many courts are located in multi-tenant buildings, there have been problems in achieving improvements in security.

The USMS has played a central role in the selection of security measures and technologies and in the allocation of security resources to the districts. At the district level, court members have some input in the selection process for security measures to address their site-specific security problems. As was true in the case of the transit systems, the court system's budget process was found to be an important factor in determining what level and type of security could be used, even though funds were specifically earmarked for court security by the judicial branch of the federal government. In addition to cost, the practicality and technical quality of security measures also were considered important by program managers. In order to make determinations about technical quality, USMS staff have conducted informal assessments of security equipment and have also relied on test and evaluation information supplied by other federal agencies.

Transit officials indicated that strategies to protect a transit network specifically against terrorism have not received much consideration because of the lack of a serious threat climate. Officials pointed out that even if the threat of terrorism were to increase, they did not know what kinds of preventive measures could be implemented without seriously affecting normal transit-system operations.

We also found that the transit systems in our review did not have a formal set of procedures for selecting preventive security strategies to address more common threats. Security-staff proposals for equipment or resources typically competed with other transit system functions in the budget process. Transit officials we interviewed frequently considered security secondary in importance to the activities that directly support transit operations. Trade-off factors considered when crime-reduction strategies were being selected most often included cost and safety. In several transit systems in our review, safety officials reviewed security

proposals to identify potential safety problems. In contrast to this concern for the physical safety of transit system riders, the civil and constitutional rights of the public received only limited consideration in the security-system selection process.

Risk-Reduction Strategies

In the courts, we found a standard set of security measures in use to address low to moderate level threats and various enhanced security measures for serious threat situations. As in the transit systems, security measures in the court facilities in our review included a combination of security personnel, equipment and technologies, and design-related features. In the court districts we visited, there appeared to be some differences in the level and use of security measures. These differences may have reflected variations in actual and anticipated threats, site configurations, resource availability, and willingness or method of implementation.

All the court districts in our review used deputy marshals and court security officers with special qualifications for guard and patrol duties and for general protective services. Some examples of security equipment we were shown were locks, alarms, CCTV, and card entry-control devices. In addition, access-control systems consisting of magnetometers and X-ray machines were used in six of the seven court facilities to screen building visitors. Examples of enhanced security measures for high-risk situations included the use of dual screening systems at both building and courtroom entrances, greater numbers of security personnel, personal protective details for members of the court, and physical searches of court facilities.

The transit systems in our review used a combination of law enforcement personnel, security equipment and technologies, and design-related features to respond to transit crime threats. The basic strategies in use were fairly similar across the systems we visited, but we found some variation in the application of security measures to different transit system elements. Where security problems were recognized as part of planning or transit components were viewed as critical to operations, enhanced security measures were used by transit officials. Law enforcement services were provided either by in-house transit police forces or, as we found in a few systems, transit units from municipal police forces. Municipal law enforcement agencies also provided backup assistance to transit systems for crime prevention and response as well as tactical-response support for high-risk incidents such as bomb threats. Security equipment such as fences, locks, and lighting was used extensively in

the transit systems we reviewed, and equipment such as CCTV, intrusion-detection alarms, and entry-control devices was found in most systems but was employed less extensively. A limited number of design-related elements (such as track redundancies, stocking of spare parts, and unobstructed transit station views) were also identified as being applicable to security issues.

Evaluations

We found that formal evaluations of performance and effectiveness were not routinely conducted in the court districts we reviewed. The USMS has established a court-facility security inspection program, but it had not been implemented in the districts we visited. Some security assessments were conducted as part of the security planning process, particularly for high-risk situations. In the special security surveys conducted for high-risk threats, we found a small number of cases where security measures had been tested to determine vulnerabilities. Court officials in several of the districts in our review also indicated that security personnel informally test security equipment to determine if equipment was functioning properly or in need of maintenance. We did not find the issues of intrusiveness in particular or civil liberties in general to be the focus of any evaluation efforts in the courts.

The transit systems that we reviewed also did not have plans or programs to routinely test the performance or effectiveness of existing preventive measures. We found some examples of studies conducted to assess selected security strategies, such as fare-collection protective measures. These studies were conducted on an as-needed basis in response to identified security problems. Transit systems did have programs of exercises and drills to test emergency preparedness plans and procedures. In a few cases, these exercises involved terrorism-related threat scenarios. We did not find any evidence of evaluations of the possible connection between security measures and intrusiveness or other infringements of civil liberties.

In both the courts and transit systems, the lack of evaluation of the performance and effectiveness of security measures makes it difficult to know how well certain measures work in deterring or protecting against identified threats. Where evaluation activities were conducted, they tended to be responses to identified security or emergency-response problems. A more systematic evaluation approach would provide empirical information that could in turn be used to strengthen the security planning process.

Conclusions

This exploratory study has provided descriptive information on the antiterrorism security practices found in two components of the nation's infrastructure. At the present time, very little is known about what antiterrorism efforts have been developed by other infrastructure organizations. Therefore, in this study, we have developed a framework for conducting an assessment that could be used to examine other infrastructure components.

Based on our review of two infrastructure components in seven cities, it is clear that antiterrorist security is still at a relatively low level of development, particularly in mass transit systems but to a lesser degree in court districts too. Although they expressed some concern about the current potential threat of domestic terrorism, transit officials have not undertaken a concerted effort to develop risk assessment and planning strategies that specifically address the prevention of or response to terrorist incidents. District-court officials have taken some actions in these areas. However, the paucity of studies and evaluations of existing antiterrorist security measures means that the effectiveness of the current systems and practices is virtually unknown. Overall, the lack of such evaluative information regarding transit systems and court districts makes it nearly impossible to determine what can and should be done to improve our current antiterrorism strategies and responses, and especially how to do so in the manner that is least intrusive on civil liberties.

Although not a major focus of this study, concerns about the availability of expertise and technical assistance for planning domestic antiterrorism strategies were sometimes raised by officials we interviewed. The responsibility for coping with the threat of domestic terrorism is shared not only by multiple federal agencies but also by numerous state, local, and private sector organizations. Several federal organizations have been established to coordinate policies and programs to combat terrorism, but their efforts have been focused mainly on international terrorism and response and investigative measures. Information regarding protective measures neither has been made available in a coordinated manner nor has been effectively dispersed among agencies that have responsibility for the safety and protection of people and facilities within the United States.

We did not find any one executive agency responsible for providing technical information and expertise to federal agencies regarding the

planning, coordination, and evaluation of domestic antiterrorism strategies. Consequently, we found neither uniform, systematic, and comprehensive planning efforts nor sufficient attention being given to evaluating the effectiveness of current activities. Furthermore, we found no thorough study of the impact on civil liberties of these antiterrorism strategies.

Matter for Congressional Consideration

Congressional committees that are concerned about the need for careful planning against the threat of domestic terrorism and about the preservation of civil liberties may want to request that agencies provide information on the strategies they have developed to prevent and respond to terrorist acts. Of special interest would be the extent to which agencies have evaluated the effectiveness and intrusiveness of existing preventive measures, not only for threats in general but also for terrorism threats in particular. Until such evaluations of the effectiveness of existing security strategies are conducted, it is difficult to know whether those strategies are more or less protective than necessary. As part of the evaluations, consideration should be given to different threat levels so that knowledge is gained about how protective strategies can be effective and flexible in addressing different terrorist threats, while at the same time adhering to a consistent standard of minimal intrusiveness on the civil liberties of the public and employees. Congressional committees might also want to ensure that the antiterrorism programs that are developed are compatible with the mission and operations of their institutions or facilities, are integrated with related functions such as safety and emergency preparedness, and are coordinated with appropriate law enforcement agencies.

Agency Comments and Our Response

DOT, AOUSC, GSA, and DOJ commented on a draft of this report; their comments appear in appendixes III, IV, V, and VI respectively. Overall, DOT, AOUSC, and GSA were in substantial agreement with our findings. DOT found the report accurate and the findings reasonable, and AOUSC remarked on its comprehensiveness and usefulness. DOT also highlighted the report's role in training and in disseminating information, which we agree is important in raising levels of awareness about antiterrorism measures among local transit agencies. DOJ made a number of comments that were helpful, and changes were made where appropriate.

Regarding coordination among the agencies involved in court security, AOUSC and GSA concurred with our observations that there are problems

in this area, primarily at the local and regional levels. However, GSA further noted that disagreements were rare and quickly resolved. DOJ stated: "There is no problem...." We found, however, examples of points of contention, some of which had been longstanding ones, in each of the seven court districts we visited. Problem areas included the responsibility for perimeter security, the type of security provided in parking areas, and the level of security available after normal work hours. Although these 7 districts were not a representative sample of the 94 federal districts, the fact that all 7 had problems suggests to us that coordination issues need reexamination.

AOUSC, GSA, and DOJ also commented on our findings concerning the lack of routine evaluation procedures. AOUSC agreed that more can be done in this area and indicated their intention to work with USMS to develop a realistic, formal evaluation process. GSA and DOJ, however, said that the lack of any serious or life-threatening breaches of security indicates that established procedures are working. Since the lack of security breaches might be due to any of a number of reasons—for example, the rarity of domestic terrorist incidents—we disagree that the lack of breaches is a proof of effectiveness. Instead, we believe that the systematic evaluation approach that we mention in our report is needed to determine effectiveness.

Congressional Request Letter

NINETY-NINTH CONGRESS

PETER W. RODINO, JR., NEW JERSEY, CHAIRMAN

JACK BROOKS, TEXAS
ROBERT W. KASTENMEIER, WISCONSIN
DON EDWARDS, CALIFORNIA
JOHN CONYERS, JR., MICHIGAN
JOHN F. SEIBERLING, OHIO
ROMANO L. MAZZOLI, KENTUCKY
WILLIAM J. HUGHES, NEW JERSEY
MIKE SYNAR, OKLAHOMA
PATRICIA SCHROEDER, COLORADO
DAN GLENN, KANSAS
BARNEY FRANK, MASSACHUSETTS
GEO. W. CROCKETT, JR., MICHIGAN
CHARLES E. SCHUMER, NEW YORK
BRUCE A. MORRISON, CONNECTICUT
EDWARD F. FEIGHAN, OHIO
LAWRENCE J. SMITH, FLORIDA
HOWARD L. BERNAN, CALIFORNIA
RICK BOUCHER, VIRGINIA
MARLEY O. STAGGERS, JR., WEST VIRGINIA
JOHN BRYANT, TEXAS

HAMILTON FISH, JR., NEW YORK
CARLOS J. MOONHEAD, CALIFORNIA
HENRY J. HYDE, ILLINOIS
THOMAS N. KIRNESS, OHIO
DAN LUNGREN, CALIFORNIA
F. JAMES SENSENBRENNER, JR., WISCONSIN
BILL MCCOLLUM, FLORIDA
E. CLAY SHAW, JR., FLORIDA
GEORGE W. GEEKS, PENNSYLVANIA
MICHAEL DOWNE, OHIO
WILLIAM E. DANNEMEYER, CALIFORNIA
HANK BROWN, COLORADO
PATRICK L. SWINDALL, GEORGIA
HOWARD COBLE, NORTH CAROLINA

GENERAL COUNSEL
M. ELAINE MIELKE
STAFF DIRECTOR
GARNER O. CLINE
ASSOCIATE COUNSEL
ALAN F. COFFEY, JR.

U.S. House of Representatives
Committee on the Judiciary
Washington, DC 20515-6216
Telephone: 202-225-3951

June 19, 1986

Charles A. Bowsher
Comptroller General of the
United States
General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Bowsher:

The Subcommittee on Civil and Constitutional Rights has conducted hearings in recent years on a number of aspects of federal counterterrorism measures. The Subcommittee has been concerned to ensure that responses to the threat of terrorist activities against targets within the United States are both adequate and consistent with constitutional principles. As terrorist incidents involving American interests in foreign countries have increased during the last several years, many experts have come to believe that it is only a matter of time before such incidents occur in this country as well. Potential targets include various components of the nation's infrastructure: electric power plants, roadways and bridges, ships and sea ports, federal buildings, airports, communication facilities, oil and gas pipelines, etc. Counterterrorism measures should appropriately safeguard these components and at the same time preserve individual civil and constitutional rights.

The Subcommittee is interested in information on how federal agencies have responded to the threat of domestic terrorist actions against the nation's infrastructure. A description of the security systems used and the level of intrusiveness they impose on federal employees and the public, as well as an assessment of the extent to which the effectiveness of such systems have been tested, would be most useful to the Subcommittee. Members of the Subcommittee staff have discussed our interests in this regard with staff from your Program Evaluation and Methodology Division, who indicated that the collection and analysis of the information about counterterrorism systems may be feasible. Given the numerous infrastructure

Appendix I
Congressional Request Letter

Charles A. Bowsher
June 19, 1986
Page 2

components and agencies involved, however, it will be necessary to limit the review to selected components.

This letter is to request that this work be done for the Subcommittee. By the Fall of this year, I hope that GAO staff will be able to brief us on characteristics of security systems used to protect selected infrastructure components and also their plans for the remaining work to be done on the evaluations of the security systems. At that time we could also decide on the type of report that would be most useful to the Congress. The Subcommittee staff will, of course, be available to assist in establishing criteria for selecting the infrastructure components to be reviewed and other assistance as appropriate.

Thank you for your cooperation in responding to this request.

Sincerely,



Don Edwards
Chairman
Subcommittee on Civil and
Constitutional Rights

DE:jdb

Antiterrorism Programs

This appendix describes the six issues that we consider to be most important in planning antiterrorism programs: (1) assigning roles and responsibilities; (2) perceiving and understanding terrorism threats; (3) assessing risks; (4) selecting alternative strategies for reducing risks; (5) implementing risk-reduction policies and protective measures; and (6) evaluating their performance, effectiveness and intrusiveness. Overall, the objective of an antiterrorism program (as outlined in table II.1) is to ensure the protection of people and facilities through the employment of security strategies that are appropriate, adequate, and as little intrusive as possible.

Table II.1: Components of an Antiterrorism Program

Program components	Implementation issues and actions
1. Roles and responsibilities	Internal planning, implementation, and evaluation External coordination
2. Perceptions of terrorism threats	General domestic terrorist threats Specific terrorist threats
3. Risk assessments	Sources of potential threats History and likely course of action Motivation, capabilities, and attributes Vulnerability of what is to be protected Attractiveness (criticality or value) Site characteristics (accessibility) Consequences to be avoided
4. Selection factors	Costs, practicality, and safety Technical and operational effectiveness Intrusiveness on civil liberties
5. Risk-reduction strategies	Intelligence monitoring Physical security protection Mitigation
6. Evaluations	Technical performance Operational effectiveness Assessment of intrusiveness

Roles and Responsibilities

Antiterrorism programs, like other programs designed to deal with risks, are considered in the context of the mission and operations of their particular institution or facility and are usually integrated with related functions, such as security against other threats, safety, and emergency preparedness. While each organization must deal specifically with its own risks, the responsibilities for coping with a domestic terrorist-threat environment generally are shared not only by multiple federal agencies but also numerous state, local, and private sector organizations. Assigning roles and responsibilities to officials within an organization

can facilitate not only the internal planning, implementation, and evaluation of protective strategies, but also the external coordination with other key organizations.

Perceptions of Terrorism Threats

How key agency officials view the threat of terrorism determines, in part, the efforts they will make to prevent such incidents or to respond should an incident occur. Their perceptions concerning domestic terrorism in general are usually based on general media accounts of international, national and local events, whereas their perceptions of their specific organizations are usually based on their own experiences and those of their counterparts in similar organizations.

Risk Assessments

A necessary starting point in antiterrorism planning is an assessment of risk specifically in regard to terrorist threats. Terms such as risk, vulnerability, criticality, and threat analyses or assessments, and site or security surveys, are sometimes used with different meanings and, at times, even interchangeably. We consider risk assessment to be a process for estimating the possibility of loss or injury from a dangerous element or factor, in this case a terrorist attack. It includes analyses of both threats and vulnerabilities, as shown in the third section of table II.1.

Threat Assessments

In considering the magnitude of the potential threat, the primary factors considered include (1) the historical pattern of terrorism against such institutions (including its facilities, activities, and people); and (2) the probability of occurrence based on the existence, activities, and capabilities of militant organizations with hostile intentions toward the government in general or toward identifiable institutions or officials. Even when no historical evidence exists that a given type of institution has been previously targeted, one cannot assume that a threat does not exist. A new or existing terrorist group that is opposed to a particular institution may choose to attack it, although they had not done so previously. Also, any institution can be a target of a terrorist group that has an undifferentiated hostility toward our government or society. A terrorist group may attack merely because a facility is conspicuous physically or symbolically, or is the most readily accessible target. In addition, a terrorist may attack one facility but have an equal spinoff effect on a neighboring facility. Furthermore, an institution may be involved in contemporary events or political incidents that could

increase the likelihood of its becoming a terrorist target literally overnight.

Threat assessments also typically include a study of the capabilities and intentions of potential adversaries. Knowledge of the operational methods and the technical skills and equipment used by potential adversaries is important. This knowledge is essential in order that an effective security strategy can be selected and designed. Terrorist tactics have been described in various ways. Generally, terrorists attempt to instill fear by killing or injuring personnel, damaging property or disrupting operations, and stealing or destroying information or materials. A terrorist group typically includes individuals who are highly dedicated and disciplined, and who are politically and ideologically motivated. Typical weapons used by terrorists include handguns, rifles, automatic weapons, and explosive devices. Tools and equipment for entry include simple tools for barrier penetration, false credentials and communication equipment. The terrorist is commonly trained in weapons tactics, explosives manufacture, forgery, codes, and security.

Pertinent information and intelligence for assessing a specific threat include factors unique to the institution or facility as well as generic information. Since possession of this information may be divided between the specific institution and various federal, state, or local law enforcement or intelligence agencies, information-sharing and coordination are important for timely and complete threat assessments.

Vulnerability Assessments

A vulnerability is any weakness that a terrorist could take advantage of in carrying out a threat. A terrorism vulnerability assessment, therefore, includes a review of the susceptibility of the facilities, operations, and people of an institution to possible damage, disruption, or theft resulting from terrorist activity. Assessments are conducted to identify the critical vulnerabilities that terrorists could easily exploit. In order to complete an assessment, information is needed on the physical characteristics of the facility, its environment, its operations, and its personnel. Analysis involves determining criticality; that is, those elements that have considerable importance based on monetary value, historical significance, operations, or public opinion. Analysis also focuses on accessibility, which includes an overview of existing security measures and their effectiveness and of deficiencies in the areas of access, detection, and response time.

Risk assessments bring this information about vulnerabilities together with data about the potential level of threat to be countered. Risk assessments can range from simple general descriptions of a facility to computer-generated models using path analysis. However, most attempts to determine risks include interviews with key personnel, inspections and field observations of the facility and its surrounding environment, review of documents, and field testing of hardware and electronic systems. More complex assessments may include such techniques as computer models that compare time from detection to adversary success along defined paths or logic trees, and security management questionnaires that focus on the ability of physical protection systems to deal with a range of adversary tactics.

The logical conclusions of risk analyses are recommendations (or matters for consideration) for corrective actions to eliminate or minimize systemic vulnerabilities. These actions can include both changing a facility or its components and the implementation of safeguards to provide a more secure operating environment. Recommendations may also be made for the development of plans and procedures for responding to emergency situations. In certain infrastructure components where corrective actions may not be a feasible or effective means of protecting against terrorism, greater emphasis may be placed on emergency preparedness plans.

Selection Factors

While the level of protection is primarily a function of what is to be protected from what kind of threat and the degree of security desired, there are several tradeoffs to consider in selecting among the different preventive measures. These factors include estimated costs, practicality, safety, technical performance, operational effectiveness, and the possible effect of a particular security system on civil liberties and on the surrounding environment.

Procurement in general usually involves considerations of cost and performance. However, as a result of the proliferation of the quantity and variety of technologies with potential application to physical security requirements, it is important to assess the effectiveness and suitability of the equipment and systems for specific applications.

It is also important that security measures do not present unnecessary risks to facility employees or to the public. Security measures to limit access, for example, could conflict with procedures for evacuation in the event of an emergency. Antiterrorism measures designed to delay or

incapacitate terrorist attackers may also have an impact on the safety of individuals. For example, aircraft cabins can be equipped to fill with instantaneously incapacitating gas that may have the side effect of causing injury or perhaps even death to elderly or sick people aboard.

An important concern evolving from the increased use of antiterrorism measures is their potential impact on the civil liberties of citizens. Democracies must maintain the delicate balance of protecting citizens from terrorist action while at the same time protecting both the collective and individual civil liberties that ensure the continuation of a democratic society. Such basic democratic rights as those to privacy, due process, free association, and freedom of movement can be compromised by steps taken against terrorist movements. Antiterrorism programs must be examined closely to see what their costs are in terms of possible infringements of civil and constitutional rights.

Risk-Reduction Strategies

Risk-reduction strategies against terrorism can be considered preventive measures and can be divided into the categories of intelligence monitoring, physical security protection, and mitigation efforts.

The purpose of the intelligence role is the gathering of information so that planned terrorist attacks can be identified and thwarted. Knowledge of terrorist intentions and capabilities, if obtained prior to a planned incident, provides the opportunity to protect the target itself against attack and perhaps to apprehend the terrorist attackers. Intelligence gathering in the United States has been the subject of some debate in recent years due to concerns over infringements of individuals' civil and constitutional rights. Guidelines have now been established to provide individuals with some level of protection against unwarranted governmental intelligence activities.

The objective of physical security as a risk-reduction strategy is to protect key personnel, sensitive information, and critical materials or facilities. A number of design features and a diverse set of security measures, relying on both technology and techniques, are available for protecting against a broad spectrum of potential threats.

There are a number of design considerations in facility planning and construction that can enhance security. Facility planning involves such concerns as the layout of public and restricted points of entry and access areas, communications and utility services, and illumination needs. Critical aspects of facility construction include natural terrain

features and adjacent environment, siting and setback distances, architectural and structural design features, and selection of building materials and construction options for walls, roof and ceilings, floors, doors, and windows.

In recent years, the use of physical security systems to protect against terrorism and other potential acts of violence has increased. Barriers, fences, metal detectors, and contract guard services are becoming common features around many government and industry facilities. A number of security technologies have been developed or are in the process of development to aid in the protection effort. These include explosives-detection devices for screening passengers, packages, and vehicles; entry-control devices using biometric identification characteristics; infrared and microwave intrusion-detection systems; and ballistic-resistant materials.

Most physical security experts emphasize the use of a systems approach to security that combines technological devices and human resources. People are ultimately responsible for security; mechanical and electronic devices can supplement but never replace security awareness and physical guarding. No matter how sophisticated, reliable, and sensitive electronic devices are; they are only as effective as the responding human being makes them.

As noted earlier, physical security may not always be a feasible or effective means of protecting against terrorism, especially for components that have large and diffuse distribution networks. For example, it might be too costly to provide physical security for all segments of an oil pipeline network. In such cases, mitigation strategies designed to make a facility or system more resilient to disruption could be appropriate risk-reduction strategies. Developing the capability to continue operation of the infrastructure or to restore the infrastructure to normal operation once a disruption has occurred are particularly applicable to network systems such as electric power, pipelines, and rail transportation. Some level of redundancy built into the electric power system, for example, could allow for the continued provision of power in the event that certain parts of the system were damaged. In addition, stockpiles of critical spare parts could be used to restore electric power service in the event of system disruption. Finally, emergency preparedness planning, training, and exercises to develop better capabilities for dealing with potential disruptions to infrastructure systems can augment these mitigation strategies.

Evaluations

Once decisions about the proper mix of intelligence, physical security, and mitigating strategies to be used have been made and the necessary resources have been allocated, equipment is installed and tested, and procedures are developed and implemented. When the equipment is tested after installation, performance assessments should include verification of measures of effectiveness (for example, probability of detection and false and nuisance alarm rates), operation, maintainability, and vulnerability to compromise, defeat or tampering. Once the security system is in operation, ongoing issues of technical performance, operational effectiveness, and intrusiveness need to be evaluated.

Questions typically addressed in assessing technical performance include:

- Does the equipment allow for proper operator (human factor) considerations?
- To what extent does the detection system reduce false and nuisance alarms?
- Are the integration of hardware elements and the integration of software with hardware feasible for entry-control-system equipment?
- Does the control and display equipment provide adequate back-up capability during maintenance downtime or repair?
- Does the backup-power subsystem meet the required quality, charging, and storage-life standards?

Evaluations of operational effectiveness include questions such as:

- Does the physical security system provide security personnel with adequate time to respond to intruder threats?
- Is the equipment designed to provide safe operation and ease of maintenance by agency technicians?
- Is the system segmented in such a way that equipment can undergo maintenance without deactivating the entire system?

Assessments of intrusiveness address such questions as:

- Does the physical security system unduly restrict or inconvenience public access? Are the security measures, especially those that involve searches and other invasions of privacy, reasonable given the current risk?
- Is the information gathered more personal or intimate than warranted? Is that information safeguarded and used only for official purposes?

Comments From the General Services Administration



General Services Administration
Public Buildings Service
Washington, DC 20405



Dear Mr. Fodel:

This letter is in response to your request of January 29, 1988, for comments on the Program Evaluation and Methodology Division, General Accounting Office (GAO) draft report entitled "Domestic Terrorism: Prevention Efforts in Selected Federal Courts and Mass Transit Systems."

The United States Marshals Service (USMS) security program for the Federal judiciary has always been of prime importance to the General Services Administration (GSA). We have endeavored to respond to the program in an effective and efficient manner within our statute responsibility and resources.

GSA's commitment to court security is well documented, as exemplified by the "Memorandum of Agreement" that GSA entered into in 1971 and renewed as recently as February 1987. The signatories to the agreement, the USMS, the Administrative Office of the U.S. Courts and GSA, have agreed to their responsibilities, both logistical and financial, and are carrying out their responsibilities in an effective and cooperative manner. There have been a few cases of disagreement at the local level, but, in those rare instances, the problems were quickly resolved.

GSA is constantly aware of the potential for terroristic threats or acts against the facilities that house the U.S. Courts, and works closely with the threat analysis group of the USMS in all potential threat matters involving those facilities. Recent examples of this cooperative effort is the allocation by GSA of increased security resources for trials in Hartford, Connecticut, and Fort Smith, Arkansas. In Hartford the trial involved a Puerto Rican nationalist group known as the "Macheteros," and in Fort Smith the trial involves a far right group known as the "Aryan Nations."

The draft report refers to the lack of evaluation procedures in determining the performance and effectiveness of court security. GSA and the USMS periodically conduct physical security surveys of the facilities housing courts and the procedure is repeated before trials involving unusual public interest. The evaluation procedure for the performance and effectiveness of court security lies in the fact that, for special trials and day-to-day operations, there has not been any serious or life threatening breaches of security since being established. This would indicate that the established procedures are working.

See comment 1

Now pages 24, 26, and 29

See comment 2

Now page 24

Appendix V
Comments From the General
Services Administration

-2-

As with any program, success can be measured by results. The results in the court security program have been very successful. This can be attributed to the cooperation of many Government agencies working together to ensure that the Federal Judiciary can perform its constitutional functions free from duress and intimidation.

Sincerely,



DUNCAN LENT HOWARD
Commissioner

Mr. Richard L. Fogel
Assistant Comptroller General
General Accounting Office
Washington, DC 20548

- Is information collection limited to “public” rather than “private” areas and to persons specifically under surveillance?
- Are individuals made aware of the surveillance of their movements, actions, and communications?
- Does the security system project an image that clashes with the democratic nature of our institutions?
- Are enhanced security measures reversible so that they can be removed or lessened if and when a particular threat diminishes?

These and other critical issues should be defined in advance, as should plans for regular evaluation. There are different assessment methods that can be used alone or in combination when assessing a specific facility-protection system. In some cases, these methods are used as part of risk assessments. However, regardless of when the assessments are done, their findings are important for making informed decisions about future security needs.

Assessing the technical performance of security equipment usually involves checking the security equipment to ensure that it is functioning properly. Operational effectiveness testing involves methods such as adversary simulation, also known as “black-hatting,” that uses a mock adversary team to attempt to defeat a physical protection system. This type of testing is often done by technical experts—either on paper or in the form of a physical exercise—and it helps to uncover unconventional scenarios and incorporate insights from a variety of backgrounds. However, this method of testing offers no assurance of comprehensiveness, and the results may be arguable because they depend on the individual skills of the team.

In field testing, another form of operational testing, the human element is brought directly into play, and the actual physical protection system is subjected to small-force engagements. This is a realistic evaluation technique, and the results are easily interpreted. However, system-level tests can become so complex that sound test-design controls are sometimes lacking.

Evaluation of intrusiveness involves a review of both how the security equipment is used and of the scope and use of the information collected. Procedural rules regarding the use of the equipment and information should be explicit, and adherence to these procedures should be assessed periodically. In addition, records of formal complaints and litigation by the public and employees concerning the intrusiveness of security measures should be maintained and reviewed.

Comments From the U.S. Department of Transportation



U.S. Department of
Transportation

Assistant Secretary
for Administration

400 Seventh St., S.W.
Washington, D.C. 20594

MAR 7 1988

Mr. J. Dexter Peach
Assistant Comptroller General
Resources, Community, and Economic
Development Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Peach:

The Department of Transportation has reviewed the U.S. General Accounting Office draft report entitled, "Domestic Terrorism: Prevention Efforts in Selected Federal Courts and Mass Transit Systems," dated January 25, 1988. The information presented appears to be accurate and the findings reasonable, therefore we find nothing objectionable in the draft report.

As the report states, we have begun a demonstration project to learn more about terrorism prevention and response strategies, in addition to providing training, through our Transportation Safety Institute, to transit personnel covering facilities protection, explosives incidents, and management. We are also proposing to conduct regional seminars on transit security that will focus on external security threats, surveillance techniques, and anti-terrorism tactics.

Thank you for the opportunity to review this report. If you have any questions concerning our reply, please call Bob Matthews on 366-5151.

Sincerely,

Maureen J. Allen for

Jon H. Seymour

Comments From the Administrative Office of the United States Courts

L. RALPH MECHAM
DIRECTOR

JAMES E. MACKLIN, JR.
DEPUTY DIRECTOR

ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS

WASHINGTON, D.C. 20544

February 23, 1988

Mr. Richard L. Fogel
Assistant Comptroller General
General Accounting Office
General Government Division
Washington, DC 20548

Dear Mr. Fogel:

I respond to your letter of January 29, 1988, requesting my comments on your draft proposed report, Domestic Terrorism: Prevention Efforts in Selected Federal Courts and Mass Transit Systems, to the Chairman, Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary of the House of Representatives.

Copies of the report have been distributed to the chief judges of the seven district courts included in your review, with the request that they provide me with any comments they want to have incorporated in my response. To date I have received none. When they are received I shall send them to you.

I am impressed by the comprehensiveness of the study and encouraged by the progress of the court security program since its inception in 1983. While we are still somewhat short of where we would like to be, I look upon your findings as a positive statement that the courts and the United States Marshals Service have carried out a national program of significant importance.

Your study focused on six issues: (1) the current roles and responsibilities for antiterrorism policies for the judiciary; (2) planners' and policy makers' perception of domestic terrorism threats; (3) existing risk assessment activities to identify the criticality and vulnerability of assets; (4) factors considered in selecting antiterrorism strategies; (5) strategies in use; and (6) evaluation of effectiveness.

The findings in the first five areas are generally positive. I shall comment on several reported shortcomings. I agree there may be a need for improved coordination between the

Appendix IV
Comments From the Administrative Office of
the United States Courts

Mr. Ricahrd Fogel
Page Two

agencies involved in the security program in some of the districts, particularly with respect to the role of the General Services Administration in perimeter security protection. Our experience indicates that the principal problem is regional interpretation of national policy within the General Services Administration. The Director of the Law Enforcement Division of that agency has been very cooperative and helpful in resolving those differences when called to his attention.

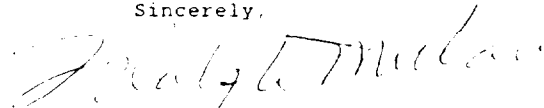
While your review found some variation in the use of security strategies, that is not perceived as a major problem. Some level of variation between districts is inherent in the security program. Each district court security committee has the responsibility to identify security problems, and the manner in which the resources will be deployed or utilized. Given the unique, independent nature of the judiciary I am encouraged that you found the level of uniformity you report.

With regard to the sixth issue addressed by the study, evaluations of effectiveness, you comment on the lack of any routine, formal evaluation process which tests the effectiveness or potential intrusiveness of existing security systems. While you make no recommendation in the report, I agree with the comment "a more systematic evaluation approach would provide empirical information which could in turn be used to strengthen the planning process." I shall instruct my Office of Court Security to work with the United States Marshals Service to develop a realistic, formal evaluation process.

Since the General Accounting Office undertook this review the Judicial Conference of the United States has established a Committee on Court Security consisting of nine federal judicial officers. The committee is responsible for overseeing all court security matters, including provision of security services, and for making recommendations for changes where deemed advisable. Your report will be a valuable resource to the committee members as they undertake their review of the security program and formulate strategies for the future.

I appreciate the opportunity to review and comment on your report.

Sincerely,



L. Ralph Mecham
Director

The following are GAO's comments on the General Services Administration's letter dated February 16, 1988.

GAO Comments

1. Although we visited only seven court districts—and thus not a representative sample of the 94 federal districts—we found examples of points of contention, some of which had been of longstanding duration, in each district visited. Since some of these coordination problems (such as the type of security provided in parking areas and the level of security and response to problems occurring after normal work hours) apparently were not “quickly resolved,” we believe that they need to be addressed.
2. We disagree with the conclusion that the lack of any serious or life-threatening breaches of security indicates that established procedures are working. Further evidence that other reasons or conditions did not contribute to the lack of security breaches is needed before such a cause-effect relationship can be established. We believe that the more systematic evaluation-approach we mention in the report is needed to draw conclusions about program effectiveness.

Comments From the U.S. Department of Justice



U.S. Department of Justice

MAR 25 1988

Washington, D.C. 20530

Mr. Richard L. Fogel
Assistant Comptroller General
General Government Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Fogel:

This letter responds to your request to the Attorney General for the comments of the Department of Justice on your draft report entitled "Domestic Terrorism: Prevention Efforts in Selected Federal Courts and Mass Transit Systems."

The report focuses its research on six elements that the General Accounting Office (GAO) considers most important in planning antiterrorism programs. They are: (1) assigning roles and responsibilities, (2) perceiving and understanding the threat, (3) assessing risks, (4) selecting alternative strategies for reducing risks, (5) implementing policies and protective measures, and (6) evaluating the performance, effectiveness, and intrusiveness of security systems. GAO decided that the overall objective was to ensure the protection of people and property with strategies that are adequate and least intrusive. Their case study design was to study two key facilities or infrastructures in our society--the Federal court system and the mass transit system.

The report determined that the Federal court system and the mass transit system differed in views about terrorism threats and the need for antiterrorism measures. The courts were more aware of possible threats of terrorism than the mass transit system and were concerned with high risk trials involving organized crime, drug, and terrorist groups. Mass transit was more concerned with natural disasters and emergency events. The courts were more concerned with civil liberties than were mass transit officials. GAO found that few studies had been done to evaluate existing antiterrorism measures and practices in either the courts or the transit systems.

The Department's comments to this report have been divided into the four major categories noted below.

Responsibility for Terrorist Matters in Federal Courthouses

Pages 2-1, 2-7, and 2-11 discuss the issue of the responsibility and authority of the United States Marshals Service (USMS) and the Federal Bureau of Investigation (FBI) for terrorist matters involving Federal courthouses. Some of the statements on these pages are incorrect or need clarification.

See comment 1

New pages 24, 26 and 29

Appendix VI
Comments From the U.S. Department
of Justice

- 2 -

Now page 24

The USMS is the agency vested with principal responsibility to provide protection and security for Federal courts. Other agencies assist the USMS in fulfilling this protective function. Thus, the first sentence of the last paragraph on page 2-1 is incorrect.

See comment 2

The FBI is the lead agency with respect to investigative activities and responses to terrorist activities generally. However, the USMS may, if required, take some initial actions prior to arrival of the FBI. Thus, the statement by an unidentified court officer in the last paragraph on page 2-11 that the USMS has authority over other Federal investigative agencies is wrong not only with respect to terrorism matters but also insofar as the statement implies that the USMS has this authority with respect to all law enforcement activities.

Now page 29

Within the context of the assignment of specific duties to the FBI and USMS, there may be some overlap when the security of a Federal courthouse is threatened by terrorist activity. The USMS will assume primary responsibility for maintaining the security of the courthouse and the FBI will assume primary responsibility for responding to the specific terrorist activity. However, this does not present any inherent conflict, and the appropriate course of action should be arrived at through consultation and coordination.

See comment 3

GAO's Case Study Design

This study, or any effort to undertake a similar study, has to be based on making some assumptions using a risk assessment process. This process was one of the six elements used in GAO's study. When there is no specific threat to a specific target, an effort to make an assessment can be made using general information concerning known terrorist groups. The results, coming from a hypothetical basis, do not have a solid, totally agreed-upon position to complete the other five elements of the six-element component model of such a study. The "quantitative assumptions" made during this study or any similar study may lead to circular, argumentative discussions about the intrusiveness of civil liberties, depending on the definition of terrorist being used by the participants.

For example, this report stated that a "typical" group of terrorists is from one to six people with handguns, shoulder weapons, and explosives. It is not known if all those contacted in the study agreed on this definition or used this definition in their planning.

The study concludes that no consistent plan has been developed by either the courts or mass transit to deal with a perceived terrorist threat, and the model used in this study could be a possible solution. However, the FBI's Counterterrorism Section

Appendix VI
Comments From the U.S. Department
of Justice

- 3 -

cautions that any over-simplification of the terrorism threat may also have a negative effect on the ability to respond to or interdict a terrorist event. It must be remembered that terrorists are criminals and should be treated as such. Any emergency response plan currently in existence on the local, State, or Federal level for use in a criminal act should also cover the actions of terrorists. To put special emphasis on counterterrorism planning and response plans, separate from any other anti-crime plans and responses because of fear of intrusive actions by law enforcement, may be adding an artificial framework that may not be justified.

See comment 4

Now page 12

Civil Liberties

On page 1-4 the report speculates on reasons for "the lack of a high level of terrorist activity" in the United States. It observes that "[t]he U.S. political system seems thus far to have been able to assimilate many different forms of dissension." We believe that this statement could be more explicit and note that the United States, having been founded by dissenters, gives explicit constitutional protection to freedom of speech and assembly and provides a mechanism for peaceful change. This constitutional protection may have reduced the need for terrorist acts as a means of communication.

Now pages 15-17

On pages 1-13 and 1-14, the discussion of civil liberties assumes that whether security methods are considered intrusive "depends on individuals' perception of the threat" at any given time. In fact, our system of civil rights is not based on such subjective individual judgments, but on a relatively objective system based on legal authority, such as the Fourth Amendment's protection against "unreasonable searches and seizures."

Moreover, the report states that "the use of security measures almost always imposes some level of intrusiveness or some reduction in individual liberties." This assertion is not documented. No methods are described which are alleged to violate civil liberties. We suggest it might be better to say that such measures must be examined to ensure that they do not violate individual liberties or to delete the sentence entirely.

Now pages 35-36

There are specific references to the Justice Management Division and court security on pages 2-24 and 2-25. These have been examined and found to be accurate.

We believe that the discussion of the civil liberties issue would be more valuable if expanded. This study was requested by the Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee. Understandably, GAO gave specific attention to the civil liberties issue. Thus, the study notes that "the civil and constitutional rights of transit patrons and employees

- 4 -

received only minor attention with regard to the selection of security measures." Similar statements are made concerning the courts. (p. 3-25; see also pages 3-36, 4-14, 4-16, and 4-17). It appears, however, that the measures discussed in the study did not, in fact, seriously raise civil liberties issues and that point should be made explicit. For example, no complaints about intrusiveness were received from transit patrons (p. 3-35). Without some expanded discussion of the civil liberties issue, this study may be interpreted as concluding that civil liberties have been ignored or violated, which is something the court system, in particular, is not likely to have done.

Specific Comments of the USMS on Federal Court Security

Page i-10, para 1. The USMS is in the final phase of developing procedures to test the overall effectiveness and potential intrusiveness of security systems installed to protect the Federal judiciary. Implementation of these testing procedures is expected to commence nationwide by the fourth quarter of FY 1988.

Page 2-1, para 2. There is only one agency with responsibility for protecting the Federal courts in general and specifically from attack. Whether such an attack would come from international or domestic terrorists, drug syndicates, or common criminals is irrelevant. While support may come at times from other agencies, just as with other criminal justice matters, it is incorrect to say that other agencies share responsibility in judicial security. The USMS has exclusive jurisdiction in protecting the Federal courts from intimidation, irrespective of its source.

The responsibility of the General Services Administration (GSA) for general building and perimeter security is coincidental to the judicial process taking place in a Federal building. However, due to budget constraints beyond its control, GSA has largely abdicated this responsibility. Consequently, where possible, the USMS has expanded its judicial security role to the perimeter of court facilities and beyond.

Page 2-7, para 1. The FBI has no direct role in judicial security. The FBI plays a support role in investigating threats against judicial officers and providing intelligence information.

Page 2-10, para 2. Developing effective anti-terrorism security plans is contingent upon developing an expertise in anti-terrorism and evaluating the responsiveness of the plans to potential terrorism threats. The Threat Analysis Division is currently undertaking a coordinated effort within the USMS to develop this expertise and improve terrorism prevention measures.

Appendix VI
Comments From the U.S. Department
of Justice

- 5 -

Now page 42

Page 2-36, para 1. The factors used by the USMS in determining risk reduction strategies are integrated systematically into a formal assessment process. However, implementation of security recommendations vary among court facilities. Security is custom tailored for each facility to meet its specific needs and assessed threat level.

See comment 8
Now pages 46-47

Page 2-43, para 2. In addition to using formal tests and evaluations performed by other agencies, the USMS contracts for its own testing of security items. Under an interagency agreement with the Department of Transportation's Research and Special Programs Administration, the USMS has contracted for the formal testing of x-ray machines and walk-through metal detectors. In addition, special evaluation teams have been dispatched to inspect installed items of security equipment in court facilities. Finally, under a national contract awarded in September 1987, the USMS has implemented a quality assurance program to ensure the adequacy and effectiveness of security systems in all Federal court facilities.

See comment 9
Now page 76

Page 4-7, para 1. There is no problem of coordination between the USMS, which is responsible for judicial security, and GSA, which is responsible for general building and perimeter security. Rather, the problem is one of inadequate resources for GSA to raise general building security to an adequate level. Nonetheless, the USMS recently reached an informal agreement with the Director of GSA's Federal Protective Service for additional perimeter security guards at selected high risk locations. Under this agreement, the additional cost will be shared equally between the two agencies.

See comment 10
Now page 83

Page 4-17, para 1. Evaluations of the effectiveness of security systems are being performed continuously. Effectiveness is measured on the one hand by the large numbers of illegal weapons, contraband, and other prohibited items detected upon entering a court facility, and on the other hand by the effectiveness of judicial security in terms of what has not happened. It is naturally difficult to quantify events that do not occur. But, if one perceives the terrorist threat as real and implements anti-terrorism measures, one has to assume the measures are effective when the threat does not materialize.

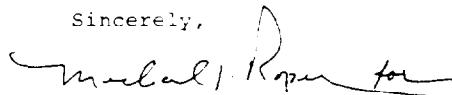
Also, the USMS is developing a formal assessment methodology for use at the Washington, D.C., Federal courthouse. This facility is likely to be the site for most trials involving terrorist activity committed outside the United States. As the result of upgrading the security for this facility, the USMS' assessment methodology is being tested and refined, and will serve as a model for formal security assessments at all Federal court facilities.

Appendix VI
Comments From the U.S. Department
of Justice

- 6 -

We appreciate the opportunity to comment on the report while in draft form. Overall, we believe our comments are constructive and will add to the value of the report. Should you have any questions concerning our response, please feel free to contact me.

Sincerely,



Harry H. Flickinger
Assistant Attorney General
for Administration

The following are GAO's comments on the Department of Justice's letter received March 25, 1988.

GAO Comments

1. The draft report stated that the USMS had the chief responsibility for federal court security, and we have clarified this point in the noted paragraph.
2. The statements about the role of the FBI were made by a court official and other governmental and local agency officials at a meeting concluding an exercise. We are simply reporting the different perceptions as they were presented by the participants. In view of the concerns raised, it appears that additional clarification, communication, and coordination are needed to resolve these differences. The Department of Justice's letter provides some clarification concerning the roles of the USMS and the FBI.
3. In conducting our study, we did not make assumptions about the domestic terrorist threat but rather recorded the perceptions of the federal court and transit officials we interviewed. We presented this information in chapters 2 and 3 of our report without making judgements as to the accuracy of these perceptions. However, in the appendix on antiterrorism programs, we did present a description of a "typical" terrorist that we compiled from information provided by terrorism experts. This general description was meant to be helpful to the general reader of the report and to organizations that have not yet considered terrorism threats. We did not intend that this description should substitute for the thorough threat analysis that is an important part of the risk-assessment process undertaken in any antiterrorism planning effort.

Furthermore, we did not mean to imply that antiterrorism planning should be separate from planning efforts addressing other security issues, but rather that terrorism-related risks be addressed explicitly and in a structured manner. In this way, plans to protect against and respond to terrorist acts can be efficiently integrated with other aspects of an organization's operations and, at the same time, such issues as intrusion on civil liberties can be considered.
4. We have revised and expanded our discussion of civil liberties in chapter 1, incorporating many of the constructive points made by the Department of Justice into this section.

5. We noted the lack of evaluation as a concern, and therefore are pleased that the USMS is finalizing a set of procedures to test the overall effectiveness and gauge the intrusiveness of security systems used in federal court facilities.

6. This information has been included in the expanded discussion of the FBI's roles and responsibilities in chapter 2.

7. In view of the concerns of several court officials about USMS knowledge of terrorism-prevention measures, we are pleased that the USMS is developing greater expertise in this area.

8. This information was not provided by the time our interviews were completed in the summer of 1987. These efforts should help to fill the gaps in evaluation that we noted in the report.

9. The inadequacy of the resources available to GSA for providing general and perimeter security may have been the basis for some of the coordination problems described by the court officials interviewed in this study. The informal agreement recently reached between the USMS and GSA headquarter's staff regarding additional perimeter security guards at selected high-risk locations should address some of the concerns raised by the court officials in several of the districts we visited.

10. The lack of incidents alone is not sufficient evidence to conclude that the antiterrorism measures are effective. Further evidence is needed before such a cause-effect relationship can be established. We hope that the formal assessment methodology described in the Department of Justice letter is designed to provide this evaluative data.

Selective Bibliography

Alexander, Yonah, and Charles Ebinger, eds. Political Terrorism and Energy: The Threat and Response. New York: Praeger Publishers, 1982.

American Defense Preparedness Association. Proceedings of the Joint Government-Industry Symposium on Physical Security, April 9-11, 1985. Eglin Air Force Base, Fort Walton Beach, Fla.: 1985.

Armed Forces Communications and Electronics Association. Proceedings of Second Annual Symposium on Physical/Electronic Security. Philadelphia: August 1986.

Barnard, Robert L. Intrusion Detection Systems: Principles of Operation and Applications. Boston: Butterworth Publishers, 1981.

Bloom, Richard. Closed Circuit Television in Transit Stations: Application Guidelines, UMTA-MA-06-0048-80-5. Washington, D.C.: U.S. Department of Transportation, August 1980.

Breemer, J. S. "Offshore Energy Terrorism: Perspectives on a Problem." Terrorism, 6:3 (1983), 455-68.

Broder, James F. Risk Analysis and the Security Survey. Boston: Butterworth Publishers, 1984.

Cavanagh, S. The Complexities of Developing a Federal Response to Domestic Terrorism: An Overview. Washington, D.C.: Congressional Research Service, 1982.

Center for Strategic and International Studies. Combating Terrorism: A Matter of Leverage. Washington, D.C.: June 1986.

Clement, R. E. Study on Transit Terrorism, DTR557-86-P-81186. Washington, D.C.: U.S. Department of Transportation, 1987.

Committee on the Protection of Federal Facilities Against Terrorism. Building Research Board. National Research Council. Protection of Federal Office Buildings Against Terrorism. Washington, D.C.: National Academy Press, 1988.

Cordes, Bonnie, Brian M. Jenkins, and Kinrad Kellen. A Conceptual Framework for Analysing Terrorist Groups. Santa Monica, Calif.: The Rand Corporation, June 1985.

Crenshaw, Martha, ed. Terrorism, Legitimacy, and Power: The Consequences of Political Violence. Middletown, Conn.: Wesleyan University Press, 1982.

Department of Justice. Report of the Attorney General's Task Force on Court Security. Washington, D.C.: March 1982.

Farrell, William R. The U.S. Government Response to Terrorism: In Search of an Effective Strategy. Boulder, Colo.: Westview Press, 1982.

Federal Bureau of Investigation, Terrorist Research and Analytical Center. FBI Analysis of Terrorist Incidents and Terrorist Related Activities in the United States 1984. Washington, D.C.: 1985.

———. FBI Analysis of Terrorist Incidents and Terrorist Related Activities in the United States 1985. Washington, D.C.: 1986.

Final Report of the Select Committee to Study Government Operations With Respect to Intelligence Activities, U.S. Senate. Intelligence Activities and The Rights of Americans. 94th Cong., 2nd sess. Washington, D.C.: U.S. Government Printing Office, April 26, 1976.

GAO (U.S. General Accounting Office). Employee Security: GSA Has No Criteria for Assessing Adequacy. GAO GGD-87-89. Washington, D.C.: June 1987.

———. Federal Electrical Emergency Preparedness Is Inadequate. EMD-81-50. Washington, D.C.: May 1981.

———. Key Crude Oil and Products Pipelines Are Vulnerable to Disruptions. EMD-79-63. Washington, D.C.: August 1979.

———. U.S. Marshals' Dilemma: Serving Two Branches of Government. GAO GGD-82-3. Washington, D.C.: April 1982.

GSA (General Services Administration). United States Courts Design Guide. Washington, D.C.: March 1984.

Guide to the Federal Courts. Washington, D.C.: WANT Publishing Company, 1982.

Hathaway, W. T., S. H. Markos, and R. J. Pawlak. Recommended Emergency Preparedness Guidelines for Rail Transit Systems. UMTA-MA-06-

0152-85-1. Washington, D.C.: U.S. Department of Transportation, July 1986.

Healy, Richard J., ed. Design for Security. New York: John Wiley and Sons, 1983.

Hoeber, F.P. "Terrorism, Sabotage, and Telecommunications." International Security Review, 7 (Fall 1982), 289-304.

Hoffman, Bruce. Terrorism in the United States and the Potential Threat to Nuclear Facilities. Santa Monica, Calif.: The Rand Corporation, January 1986.

Horowitz, I. L. "Can Democracy Cope With Terrorism?" Civil Liberties Review, 4 (May-June 1977), 29-37.

Jackson, John S., ed. Proceedings: 1985 Carnahan Conference on Security Technology, May 15-17. Lexington, Ky.: University of Kentucky, 1985.

Jenkins, Brian M. Future Trends in International Terrorism. Santa Monica, Calif.: The Rand Corporation, December 1985.

———. International Terrorism: The Other World War. Santa Monica, Calif.: The Rand Corporation, November 1985.

———. "International Terrorism: Trends and Potentialities." In U.S. Congress, Senate Committee on Governmental Affairs. An Act to Combat International Terrorism, Report to Accompany S. 2236, Senate Report No. 95-908. 95th Cong., 2nd sess. Washington, D.C.: U.S. Government Printing Office, 1978.

———. Terrorism: Between Prudence & Paranoia. Santa Monica, Calif.: The Rand Corporation, December 1983.

———. Testimony Before the Committee on the Judiciary. Santa Monica, Calif.: The Rand Corporation, February 1984.

Joyner, C. C. "Offshore Maritime Terrorism: International Implications and the Legal Response." Naval War College Review, 36 (July-August 1983), 16-31.

- Kerr, Donald M. "Coping with Terrorism." Terrorism: An International Journal, 8:2 (1985), 113-26.
- Kindel, S. "Catching Terrorists." Science Digest, September 1986, pp. 37-41 and 76-82.
- Kupperman, R. H. and D.M. Trent. Terrorism: Threat, Reality, Response. Stanford, Calif.: Hoover Institution Press, 1979.
- Laquer, Walter. Terrorism. Boston: Little, Brown, 1977.
- Lieberman, Jethro K. Privacy and the Law. New York: Lothrop, Lee and Shepard Co., 1978.
- Livingstone, N. C. "Vulnerability of Chemical Plants to Terrorism: An Examination." Chemical and Engineering News, 63 (Oct. 21, 1985), 7-13.
- . and T. E. Arnold. Fighting Back: Winning the War Against Terrorism. Lexington, Mass.: Lexington Books, 1985.
- Marx, G. T. and S. Sherizen. "Monitoring on the Job." Technology Review (November-December 1986), 64-72.
- Mauri, R.A., N. A. Cooney, and G. J. Prowe. Transit Security: A Description of Problems and Countermeasures, UMTA-MA-06-0152-85-1. Washington, D.C.: U.S. Department of Transportation, May 1986.
- Motley, James B. U.S. Strategy to Counter Domestic Political Terrorism. Monograph 83-2. Washington, D.C.: National Defense University Press, 1983.
- National Advisory Committee on Criminal Justice Standards and Goals. Disorders and Terrorism: Report of the Task Force on Disorders and Terrorism. Washington, D.C.: U.S. Department of Justice, December 1976.
- National Governors' Association. Domestic Terrorism. Washington, D.C.: Emergency Preparedness Project Center for Policy Research, May 1979.
- Report of the Subcommittee on Security and Terrorism, Committee on the Judiciary, U.S. Senate. State Sponsored Terrorism. Washington, D.C.: U.S. Government Printing Office, 1985.

Sessions, William S. Opening Statement of William S. Sessions, Director, Federal Bureau of Investigation, Before An Open Session of the Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, United States House of Representatives, 100th Cong., 2nd sess. Washington, D.C.: U.S. Department of Justice, March 1988.

Shultz, Richard H., Jr., ed. Responding to the Terrorist Threat: Security and Crisis Management. New York: Pergamon Press, 1980.

Stewart, B. L., ed. "State-Sponsored Terrorism: The Threat and Possible Countermeasures." Terrorism: An International Journal, 8:3 (1986), 253-313.

Trent, Darrell M. "A National Policy to Combat Terrorism." Policy Review, No. 9 (Summer 1979), 41-53.

U.S. Congress, House of Representatives. Domestic Security Measures Relating to Terrorism: Hearings Before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, 98th Cong., 2nd sess. Washington, D.C.: U.S. Government Printing Office, 1984.

———. Terrorism: Oversight Hearings Before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, 99th Cong., 1st and 2nd sess. Washington, D.C.: U.S. Government Printing Office, 1986.

Vice President's Task Force on Combatting Terrorism. Public Report of the Vice President's Task Force on Combatting Terrorism. Washington, D.C.: February 1986.

Wilcox, R. H., and P. J. Carrity, eds. America's Hidden Vulnerabilities: Crisis Management in a Society of Networks. Washington, D.C.: Center for Strategic International Studies, October 1984.

Wilkinson, Paul. Terrorism and the Liberal State. 2nd ed. London: Macmillan, 1986.

W. V. Rouse Associates. Predicting Automated Guideway Transit System Station Security Requirements, UMTA-MA-0048-80-4. Washington, D.C.: U.S. Department of Transportation, March 1980.