NISTIR 4618

Standards for the Physical Protection of National Resources and Facilities

artment of Commerce
Institute of Standards and Technology
and Fire Research Laboratory
burg, MD 20899

Prepared for:
Federal Emergency Management Agency
National Preparedness Directorate
Office of Mobilization Preparedness
Washington, DC 20472

NISTIR 4618

Standards for the Physical Protection of National Resources and Facilities

Robert D. Dikkers

July 1991

U.S. Department of Commerce
Robert A. Mosbacher, *Secretary*
National Institute of Standards and Technology
John W. Lyons, *Director*
Building and Fire Research Laboratory
Gaithersburg, MD 20899

Prepared for:
Federal Emergency Management Agency
National Preparedness Directorate
Office of Mobilization Preparedness
Washington, DC 20472

Table of Contents

Table of Contents (continued)

Abstract

In regard to a Federal Emergency Management Agency (FEMA) responsibility for the protection of essential resources and facilities, NIST conducted a study whose objectives are: (1) to identify and compile existing standards and guidelines pertaining to the protection of facilities and resources; and (2) to prepare a plan and strategies for developing national standards which may be needed to assist Federal departments and agencies in the protection of their facilities and resources.

A review of factors and considerations involved in the planning and design of physical protection for facilities and resources is discussed along with a description of physical security activities of selected Federal departments and agencies, and non-government organizations. General information on standards and brief descriptions of 110 standards pertaining to physical security and protection are included in Appendices.

Recommendations are made for: (1) the conduct of a comprehensive study to identify and describe Federal agency physical security activities and resource information; and (2) the development of national voluntary standards which would cover the planning and design phases of the security engineering design process as well as various physical security equipment and systems.

Key words:

Assets; emergency preparedness; essential resources and facilities; Federal government; physical security; security engineering; standards; threats.

Acknowledgements

The excellent cooperation and useful information provided by various Federal agencies, especially the U.S. Army Corps of Engineers Protective Design Center, Omaha, Nebraska, for this study is greatly appreciated. As mentioned in the text, Section II (pages 6 - 15) is entirely based on a security engineering design process developed by the Protective Design Center.

The helpful assistance of James H. Pielert, Building and Fire Research Laboratory, NIST, in the preparation of Appendices A and B is also gratefully acknowledged.

Executive Summary

Objectives. In regard to a proposed rulemaking (44 CFR Part 335, August 7, 1989) on the protection of essential resources and facilities, the Federal Emergency Management Agency (FEMA) funded a study at the National Institute of Standards and Technology (NIST). The specific objectives of this study are: (1) to identify and compile existing standards and guidelines pertaining to the physical protection of facilities and resources; and (2) to prepare a plan and strategies for developing national standards which may be needed to assist Federal departments and agencies in the protection of their facilities and resources.

Background. Since the proposed rulemaking pertains to many different types of resources (natural resources, economic resources, infrastructure systems, etc.) and facilities (factories, plants, and buildings used for manufacturing, production, processing, etc.), it is desirable that the design process used for developing physical protection plans and strategies be applicable to a variety of assets and threats (terrorists, criminals, protestors, etc). The security engineering design process used by the U.S. Army Corps of Engineers' Protective Design Center is considered to be a process which could be adapted and used by Federal departments and agencies and the private sector (Section II).

Federal Government and Private Sector Activities. The activities of a limited number of Federal departments and agencies pertaining to physical security or protection were reviewed (Section III). Although it was not possible to review all the pertinent activities of these departments and agencies, there is a substantial amount of Federal government activity being directed toward the planning, design, and research of physical security and protection systems. These activities include the preparation of design criteria and manuals; the development of standards; and the testing of security materials, components, and equipment. A number of the activities involve or impact the private sector, as well as State and local governments (i.e., DOD Key Asset Protection Program; DOE Vulnerability Program, DOJ Technology Assessment Program, FAA Security program).

In regard to the selected private sector organizations (Section IV), there is also considerable interest and involvement in physical security and protection activities, including the development of standards.

Standards. One hundred and ten standards pertaining to physical security and protection were identified and briefly described (Appendix B). Of the 110 standards, 42 are Federal department or agency standards and 68 are private sector standards. Standards were grouped into seventeen subject categories: general planning and design; fencing and gates; intrusion detection and alarms; vehicle barriers; walls and floors; doors; windows and glazing; ballistic resistance; access control; locks; vaults and storage systems; surveillance systems; screening devices; security seals; electrical; data transmission; and economics.

Recommendations. Although there is some dialogue and sharing of information between various Federal departments and agencies regarding their particular physical security programs, there remains, based on this study, an important need to develop a coordinated program for identifying and physical protecting national resources and facilities. Such a program should establish a clear and working relationship between the DOD Key Asset Protection Program and the physical protection programs being conducted by all other Federal Departments and agencies. In addition, this coordinated program can also be used to help establish priorities and resources for the collection and dissemination of physical security data and information and the development of national voluntary standards.

Since limitations of this study did not permit a complete review of all pertinent Federal government activities relating to the physical protection of facilities and resources, it is recommended that such a comprehensive study be conducted. This study should identify and briefly describe various physical security activities and resource information (manuals, research data, standards) as well as list individual contacts (names, addresses, and telephone numbers) within the various Federal agencies. Information and data collected in the study would be a very useful resource for all Federal agencies having a responsibility for protecting essential resources and facilities. Such information would also be a useful resource in the coordination of Federal department and agency activities as discussed above. It is estimated the initial cost of this comprehensive study would be about $200,000. To keep the information relatively up to date and useful, it is also recommended that the report be revised on annual basis. As appropriate, available and non-classified information on Federal physical security activities, such as a list of technical manuals or standards, etc., should also be made available to private sector organizations.

Proposed 44 CFR Part 335.7 indicates that "plans and strategies will be coordinated with FEMA by the Federal departments and agencies ... to assist them in developing Federal Standards ..." Although many Federal Departments and agencies may have a need to develop their own standards, such departments and agencies should also be encouraged to participate in voluntary standards bodies as outlined in OMB Circular No. A-119 (see Appendix A). Such participation can help reduce duplication of standards development efforts in the government sector and can greatly assist in developing high priority voluntary standards which could be used by both government and the private sector.

Among high priority national voluntary standards which should be developed are standard guides which would cover the planning and design phases of the security engineering design process described in Section II. Such standards should be flexible enough to deal with the many different types of essential resources and facilities. As necessary, and to avoid duplication or conflicts, it is recommended that the development of criteria and standards be closely coordinated with the DOD Key Asset Protection Program and the Key Asset Protection Program Construction Option. To expedite the development of such standards, it is recommended that funding be made available to agencies that have developed pertinent background information and data such as U.S. Army Corps of Engineers Protective Design Center in order to develop draft standards and to assist in processing such draft standards into national voluntary standards for use by government and the private sector.

In regard to physical security equipment and systems, additional national voluntary standards need to be developed. Among high priority standards are specifications and test methods for intrusion detection systems, access control systems, and screening devices. Similarly, as mentioned above, to expedite the development of such standards, it is recommended that funding be made available to agencies that have developed pertinent background information and research data (see Section III).

The annual funding required for the development of the standards described above will depend on the total number of standards needed as well as the desired time table for completing all the desired standards. Initially, it is recommended that a minimum of $200,000 per year be made available to assist in the preparation of high priority standards.

STANDARDS FOR THE PHYSICAL PROTECTION OF NATIONAL RESOURCES AND FACILITIES

I. Introduction

A. National Security Emergency Preparedness

It is the policy of the United States "to have sufficient capabilities at all levels of government to meet essential defense and civilian needs during any national security emergency. A national security emergency is any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States.[1]" The President establishes policy for national security emergency preparedness, and the National Security Council (NSC) is the principal forum for consideration of this policy.

Executive Order (E.O.) 12656, which was signed by President Ronald Reagan on November 18, 1988, assigned national security emergency preparedness responsibilities to Federal departments and agencies. The Director of the Federal Emergency Management Agency (FEMA) serves "as an advisor to the NSC on issues of national security emergency preparedness, including mobilization preparedness, civil defense, continuity of government, technological disasters, and other issues, as appropriate.[2]" As the President may establish, the Director of FEMA also assists "in the implementation of national security emergency preparedness policy by coordinating with the other Federal departments and agencies and with State and local governments..." Part 2, of E.O. 12656 contains general provisions pertaining to national security emergency preparedness for each Federal department and agency. Part 3 through Part 28 describes specific lead and support responsibilities for the various Federal departments and agencies.

In regard to the **protection of essential resources and facilities**, Section 204 of E.O. 12656, includes the following:

> "The head of each Federal department and agency, within assigned areas of responsibility, shall:
>
> "(1) Identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency;
>
> "(2) Participate in interagency activities to assess the relative importance of various facilities and resources to essential military

---

[1] Section 101 (a), Executive Order 12656.

[2] Section 104 (c), Executive Order 12656.

and civilian needs and to integrate preparedness and response strategies and procedures;

"(3) Maintain a capability to assess promptly the effect of attack and other disruptions during national security emergencies."

B. Protection of Essential Resources and Facilities

In response to E.O. 12656, FEMA proposed a new Part 335 in Title 44 Code of Federal Regulations entitled "Protection of Essential Resources and Facilities" (Federal Register, Vol. 54, No. 150, August 7, 1989, pp. 32359-32361). The purpose of this proposed rulemaking is to provide: (1) policy guidance in the identification of facilities and resources, both government and private, essential to the national defense and national welfare; (2) criteria guidance for the Federal departments and agencies to assess on a priority basis the vulnerabilities of essential facilities and resources that would impact on the needs of national defense; and (3) planning guidance for Federal departments and agencies to develop strategies, plans, and programs to provide for the security of essential facilities and resources on a priority basis, and to avoid or minimize disruptions of essential services during any national security emergency.

Definitions. Among definitions included in proposed Part 335.3 are the following:

"***Essential facilities***. Any factory, plant, building, structure used for manufacturing, production, processing, repairing, assembling, storing or distributing a product or components deemed essential to national security and a Federal agency mission, including any industrial asset nominated for inclusion in the Department of Defense Key Assets List in accordance with the selection criteria set forth in DOD Directive 5160.54 of June 26 June 1989; any communication or computer facility or system; any energy source or distribution system; any air, rail, road or water transportation asset; any other infrastructure facility that is required to support an industrial asset listed in the DOD Key Assets list or a military facility; or to otherwise support DOD mobilization, deployment or sustainment.

"***Essential resources*** are natural resources, construction, industrial production, human resources (including health resources, housing, public information, training and education), economic resources (fiscal and monetary systems) and infrastructure systems (transportation, energy, communications, data processing, water and agricultural production).

"***Essential facilities and resources protection*** is the process used for the protection of essential resources and facilities from disruption by an event in a full spectrum of threats ranging from natural disasters to sabotage by groups or individuals whose actions are hostile to national security.

"***Facilities/Structures*** means those Government-owned and/or privately-owned plants, mines, buildings (including buildings occupied in whole or part by any Federal agency), materials, products, and processes, and those Government-provided and privately provided services, which are of importance to defense mobilization, defense production, or the civilian economy and are located in the United States or in the territories or possessions of the United States. This definition shall not extend to federally owned military posts, camps, stations, arsenals or other comparable facilities under the military command of the Department of Defense.

"***Mobilization*** is the process of marshalling resources, both civil and military, to respond to and manage a national security emergency.

"***Physical security*** means security against sabotage, espionage, and other hostile activity and other destructive acts and omissions, but excludes security attributable to operations of military defense or combat and excludes activities with respect to the dispersal and post-attack rehabilitation of facilities."

Criteria. The significance of essential facilities and resources to Federal departments and agencies or to the owners of such facilities or resources is determined by applying the following criteria contained in proposed Part 335.6:

"(1) An asset whose loss would halt or unacceptably delay mobilization deployment and sustainability efforts; and

"(2) An asset that produces critical items whose loss would halt or delay unacceptably, mobilization, deployment or sustainment efforts.

"(b) These criteria in turn depend upon the following factors:

"(1) The importance of the service or product it provides or produces;

"(2) The dependence of the population or industry on the product;

"(3) The cost of replacement;

"(4) The replacement time; and

"(5) The availability of substitutes.

"(c) Priority selection categories. An essential facility or resource shall be assigned to one of the following categories:

"(1) Category one. An essential facility or resource which has no replacement, substitute, or alternative. The partial or complete loss of such facility would have an immediate and adverse effect on the national defense.

"(2) Category two. An essential facility or resource for which alternatives are available, but such alternatives are required to meet other needs of a national security emergency."

Implementation. Proposed Part 335.7 describes responsibilities of Federal departments and agencies for implementing steps for the protection of essential resources and facilities. Section (c) of this part indicates that "plans and strategies will be coordinated with FEMA by the Federal departments and agencies under the aegis of the National Security Council, to assist them in developing Federal Standards for categorizing their essential facilities and resources; prioritizing their protection; and in understanding the need to assure the availability of essential facilities and resources in a national security emergency."

C. Objectives and Scope of NIST Study

As one of its activities to implement E.O. 12656 and the proposed rulemaking discussed previously, FEMA funded a study (March 1990) to be conducted at the Center for Building Technology[3], National Institute of Standards and Technology (NIST). The specific objectives of the NIST study are: (1) to identify and compile existing standards and guidelines pertaining to the physical protection[4] of facilities and resources; and (2) to prepare a plan and strategies for developing national standards which may be needed to assist Federal departments and agencies in the protection of their facilities and resources. The long range objective of this study is to develop national standards which would provide guidance and assistance to owners and managers of essential facilities and resources in categorizing their facilities and resources; prioritizing their protection; and in applying physical security and emergency preparedness measures.

As background information for this study, Section II of this report presents a review of factors and considerations involved in the planning and design of physical protection for facilities and resources. Section III reviews physical security activities of selected Federal department and agencies, and Section IV describes similar activities of several non-government organizations.

Based on information presented in Sections II through IV, Section V contains discussions and recommendations concerning the development of standards for the physical protection of facilities and resources. General information on standards (types of standards, standards development organizations, benefits of standardization) is contained in Appendix A. Brief descriptions of existing standards for materials, equipment and systems pertinent to physical protection and security are included in Appendix B.

---

[3] In January, 1991, programs of the Center for Building Technology were merged into the Building and Fire Research Laboratory at NIST.

[4] In this study, "physical protection" does not include protection of facilities and resources against natural disasters.

II. Physical Protection of Facilities and Resources

A. Security Engineering Design Process

To develop physical protection plans and strategies for different kinds of government and private-sector facilities and resources, it is desirable to utilize a design approach which is applicable to: (1) various types of critical assets (equipment, people, information, infrastructure systems, etc.) and (2) a variety of potential threats (terrorists, criminals, vandals, disgruntled employees, etc.). One such approach is the security engineering design process. This process was developed by the U.S. Army Corps of Engineers' Protective Design Center (USCOE/PDC), Omaha, Nebraska [1][5].

The USCOE/PDC security engineering design process consists of two phases -- the planning phase and the design phase. The objective of the planning phase is to define protective system design criteria for the physical protection of the facility. The design criteria describes assets within a facility, the threat to the assets, the level to which assets are to be protected, and constraints to the protective system design. This approach is illustrated in Figure 1. The design criteria relates primarily to assets within facilities since protecting individual assets is generally more cost-effective than protecting an entire facility. Buildings would be considered assets if they would be the actual target of an aggressor.

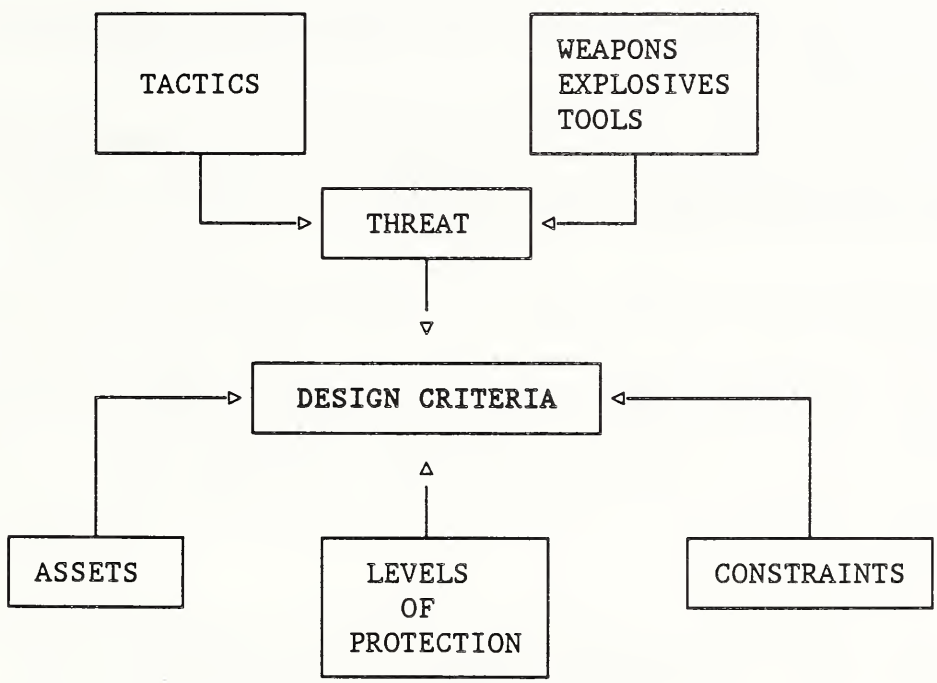

Figure 1.

---

[5] Numbers in brackets pertain to references listed in Section VI of this report.

In the design phase, the objective is the actual design of a protective system for a facility. The process by which this is accomplished is to: select design strategies which will achieve the appropriate level of protection; assess existing conditions to determine design opportunities and constraints, determine the measures needed to protect the asset against the threat, and integrate these measures into a protective system; and estimate the protective system's cost and assess the system's acceptability to the user.

1. **Planning Phase**

The development of design criteria for the physical protection of a facility involves the following steps:

Step 1. Identify and categorize assets.

Step 2. Assess asset value.

Step 3. For each asset, determine the likely aggressors and the likelihood of their attacking the asset.

Step 4. For each asset and aggressor, identify likely tactics and severity levels.

Step 5. Consolidate tactics from all aggressors into a design basis threat.

Step 6. Determine a level of protection for each asset based on the asset value.

Step 7. Identify constraints to the protective system design.

Step 1 - Identify Assets and Asset Categories

Resources or facilities can be considered assets based on one or more of the following value factors:

- Criticality to the organization's, company's or agency's mission;
- Criticality to the asset's immediate user's mission;
- Monetary value;
- Human value; and
- Organization's, company's or agency's directives.

An asset can be a primary or a secondary asset. Primary assets have a value to their owner and are generally the ultimate target of an attack. In order to function properly, a primary asset may depend on other facilities or equipment. These other facilities or equipment are considered to be secondary assets. Damaging the secondary asset may result in the compromise of the primary asset. An example of a primary asset which depends on a secondary asset is a mainframe

computer (primary asset) which depends on an uninterrupted electrical power supply (secondary asset).

Asset categories can be defined to address a wide range of items. Categories identified by the USCOE/PDC [1] include: Pilferables; Money; Drugs; Vehicles; Arms, Ammunition, and Explosives; Information; Mission-Critical Personnel/VIP's; Military/Civilian Personnel; and Equipment/Machinery/Buildings.

Step 2 - Assess Asset Value

The value of primary assets measures their value to their user and can be determined by evaluating the four value factors described below. The factors may apply differently to various asset categories with some factors not applying to some asset categories at all. The overall value is based on a combination of the applicable factors.

- **Organization Criticality**. This factor measures the impact of the asset's compromise on the organization's, company's or agency's mission. It applies to assets which directly affect the capability of the organization to carry out its mission.

- **User Criticality**. This factor measures the impact of the asset's compromise on the user's mission. An asset can be critical to it's user's mission but may not have significant impact on the overall organization's mission. It can also be critical to both the user's and the organization's mission.

- **Replaceability**. This factor measures the ease with which an asset can be replaced either in kind or with a reasonable substitute (temporary or permanent). Replaceability measures the impact of delays in replacing assets on the organization's or user's mission.

- **Value**. This factor measures the relative value of an asset. For assets which have a monetary value, this factor considers the dollar cost of the asset and any other costs related to its loss. When people are the asset, monetary value does not apply. People value is based on the number of people in a facility, including the likely number of visitors. Value for information assets is based on the sensitivity of the information.

Persons in charge of security planning can override the resultant asset value if it is considered too high or too low. The planners must consider any agency or organization directives or other requirements which may affect decisions on the asset's value.

The asset value helps the security planning team determine how much money should be spent to protect the asset. Considering the high cost of protecting assets and the limited resources which may be available, the planning team must select a level of protection appropriate to the value of the asset. The asset value

helps the planning team make this selection and becomes a part of the protective design criteria.

Step 3 - Determine Aggressors and Likelihood of Attack

The threat to an asset depends on the type of aggressors who have an interest in attacking the asset and their objectives in attacking it. With this information, the most likely threat against the asset can be determined in terms of specific tactics and sizes and types of weapons, tools, and explosives.

According to the USCOE/PDC [1], historical patterns and trends in aggressor activity indicate general categories of aggressors and the common tactics which they can be predicted to use against various assets. These tactics and their associated weapons and tools are the basis for the threat to the assets. Understanding the basis for the threat and the aggressors' objectives is essential to effective protective design. Four possible aggressor objectives are: (1) Inflict injury or death on people; (2) Destroy or damage facilities, property, equipment, or resources; (3) Steal equipment, material, or information; and (4) Create adverse publicity[6]. The four types of aggressors who share common objectives and tactics are criminals, protesters, terrorists, and subversives.

Criminals fall into one of three possible groups based on their degree of skill. These three groups are defined as unsophisticated criminals, sophisticated criminals, and organized criminal groups. The objective for all three criminal groups is theft of assets. Unsophisticated criminals are unskilled in the use of weapons and tools and have no formal organization. Their targets are those which meet their immediate needs such as drugs, money, and pilferable items. Unsophisticated criminals are interested in "opportune" targets which present little or no risk. Breaking and entering and "smash and grab" techniques are common. Sophisticated criminals are skilled in the use of certain weapons and tools, efficient, and organized. They plan their attacks and have sophisticated equipment and technical training to use it. Sophisticated criminals often employ insiders for assistance. They target high value assets, frequently steal in large quantities, and target assets with relatively low risk in handling and disposal. Organized criminal groups are sophisticated and are able to draw on specialists and to obtain the equipment needed to achieve their goals effectively. These groups form efficient, hierarchical organizations which can employ highly paid insiders. Targets of organized criminal groups may involve a high degree of risk in handling and disposal such as large quantities of money; equipment; and arms, ammunition, and explosives.

Protesters include the two general groups of vandals/activists and extremist protesters. Both groups are politically or issue oriented and act out of frustration, discontent, or anger against the actions of other social or political groups. The primary objectives of both groups include destruction and publicity. Vandals/activists are unsophisticated and superficially destructive.

---

[6] Publicity is generally not treated as a separate objective because one of the other objectives is usually linked to it.

They generally do not intend to injure people or cause extensive damage to their targets. Their actions may be covert or overt. Typically, they choose symbolic targets which pose little risk to the aggressor.

Extremist protest groups are moderately sophisticated and are more destructive than vandals. Their actions are frequently overt and may involve the additional objective or consequence of injuring people. They attack symbolic targets, including authority figures such as high-ranking officials or police and weapon systems.

Terrorists are ideologically, politically, or issue oriented. They commonly work in small, well-organized groups or cells. They are sophisticated, skilled with weapons and tools, and possess an efficient planning capability. Terrorist objectives include death, destruction, theft and publicity. The USCOE/PDC identifies three types of terrorists based on their areas of operation -- those operating within the United States; those operating in the Middle East and Northern Ireland; and others operating outside the continental United States (not included in the second type) [1].

Subversives include aggressors from foreign governments or from groups trying to overthrow the government by force. They include saboteurs and spies (hostile intelligence agents). Saboteurs include guerrillas and unconventional warfare forces (commandos). They are paramilitary or actual military personnel who are sophisticated, highly skilled, and employ meticulous planning. The objectives of saboteurs include death and destruction of property and their targets include mission-critical personnel, equipment, or operations. Spies are also highly skilled and very sophisticated. They are generally foreign agents, but frequently employ insiders for assistance.

To determine the likelihood that a particular aggressor will attack a given asset, the USCOE/PDC evaluates the factors described below. These factors address the value of the asset to aggressors, the history of and potential for attacks on similar assets, and the vulnerability of the asset.

- o Profile. This factor assesses the visibility of an asset and the public's perception of its value. Highly visible assets and those which are perceived to be highly valuable to their user may attract aggressors such as terrorists and protesters seeking visibility.

- o Usefulness. This factor assesses the usefulness of the asset to aggressors. An aggressor is more likely to attack assets which satisfy immediate needs or goals or which would apply to future needs or goals.

- o Availability. This factor assesses the availability of the asset at other facilities than at the one being evaluated. If assets similar to the one being protected are widely available elsewhere, aggressors are more likely to seek them elsewhere.

- o Local Events. This factor assesses previous attacks on similar government or civilian assets at a particular facility location or in its immediate vicinity.

- o Events Elsewhere. This factor assesses previous attacks on similar assets at similar installations in the same geographical area.

- o Potential Events. Assessment of this factor is based on analysis of intelligence reports which indicate the likelihood of the assets under evaluation being attacked in the future.

- o Accessibility. This factor assesses the accessibility of the site or facility without any new security enhancements.

- o Law Enforcement. This factor assesses the general attitude of the local population toward law enforcement and the effectiveness of the local enforcement community.

- o Deterrence. This factor assesses aggressors' perception of their possibility of successfully achieving their goal towards the asset and escaping afterward.

Step 4 - Determine Likely Tactics and Severity Levels

Aggressor objectives of theft, destruction, and injury/death dictate which tactics the aggressor will use. An asset's category also suggests how it may be compromised; i.e., stolen, destroyed, injured, killed. Aggressors employ a wide range of offensive strategies reflecting their capabilities and objectives. The USCOE/PDC [1] categorizes these offensive strategies into 15 tactics or specific methods of achieving aggressor goals. These tactics are:

- o Moving Vehicle Bomb Tactic - An aggressor drives an explosives-laden car or truck into a facility and detonates the explosives.

- o Stationary Vehicle Bomb Tactic - An aggressor parks an explosives-laden car or truck near a facility and then detonates the explosives by time delay or remote control.

- o Exterior Attack - An aggressor attacks the exterior of a facility or an exposed asset at close range. Weapons may be rocks, clubs, improvised incendiary or explosive devices, or hand grenades.

- o Standoff Weapons Attack - Military weapons or improvised versions of military weapons are fired at a facility from a significant distance. Weapons include direct and indirect line of sight weapons such as anti-tank weapons and mortars, respectively.

- o Ballistics Attack - The aggressor fires various small arms, such as pistols, submachine guns, shotguns, and rifles, from a distance determined by the firearm's range.

- o Forced Entry Attack - The aggressor forcibly enters a facility using small arms or forced entry tools.

- o Covert Entry Tactic - The aggressor attempts to covertly enter a facility by using false credentials.

- o Insider Compromise - A person authorized access to a facility attempts to compromise assets by taking advantage of that accessibility.

- o Electronic Emanation Eavesdropping Tactic - The aggressor employs electronic emanation surveillance equipment from outside a facility or restricted area of a facility to monitor electronic emanations from computers, communications, and related equipment.

- o Acoustical Eavesdropping Tactic - The aggressor employs "listening devices" to monitor voice communication or other audible information.

- o Visual Surveillance Tactic - The aggressor employs ocular or photographic devices such as binoculars or cameras with telephoto lenses to monitor facility or installation operations.

- o Mail Bomb Tactic - Bombs or incendiary devices are delivered to the target in letters or packages.

- o Supplies Bomb Tactic - Bombs are concealed in various containers and delivered to supply and material handling points such as loading docks.

- o Airborne Contamination Tactic - An aggressor contaminates the air supply of a facility by introducing chemical or biological agents into it.

- o Waterborne Contamination Tactic - An aggressor contaminates the water supply to a facility by introducing chemical, biological, or radiological agents into it.

Associated with a majority of tactics are levels of severity. Selecting tactic severities considering the likelihood that an aggressor will attempt to compromise or attack an asset is based on "risk acceptance." If the likelihood that an aggressor will attack is low, the protective system can be designed for a severity level less than the maximum plausible threat for an aggressor.

Step 5 - Consolidate Tactic Severity Levels into the Design Basis Threat

When the all the aggressors and associated tactic severity levels have been evaluated, the information can be used to establish the design basis threat for a given asset or assets.

Step 6 - Determine the Appropriate Levels of Protection

Levels of protection refer to the degree to which an asset is protected based on its value to its user. The higher the level of protection, the lower the accepted risk will be that the asset will be compromised if attacked. For some tactics, levels of protection refer to the amount of damage a facility or asset would be allowed to sustain in the event of an attack. A low amount of allowed damage equates to a high level of protection. For other tactics, levels of protection refer to the probability that an aggressor will be defeated before the asset is compromised based on the sophistication of the protective system. A high probability of defeat equates to a high level of protection.

Step 7 - Identify Design Constraints

Design constraints include physical characteristics and qualities or operational considerations which restrict or dictate the design of a protective system. The following constraint categories are considered by the USCOE/PDC [1]: political; financial; regulations; procedural or operational; response force; response time; and manpower allocation.

2. Design Phase

The objective of the design phase of the security engineering design process [1] is the design of a protective system for a facility or asset. A protective system integrates all of the protective measures and procedures required to protect assets against the design basis threat. The ideal protective system deters, defends against, detects, and defeats aggressors. Protective system design is directed primarily toward defense and detection, because deterrence is unmeasurable and defeat is a function of the response force.

Deterrence. A potential aggressor who perceives an unacceptable risk may be deterred from attacking an asset. The effectiveness of deterrence varies with the sophistication of the aggressor, the attractiveness of the asset, and the aggressor's objective. Although deterrence is not considered a direct design objective, it may be the result of design.

Defense. Defensive measures protect an asset from aggression by delaying or preventing an aggressor's movement toward the asset or by shielding the asset from the aggressor's weapons and explosives.

Detection. Detection measures sense evidence of an act of aggression, assess it, and communicate the appropriate information to the response force.

Defeat. Some protective systems depend on response personnel to defeat an aggressor.

The design of a protective system involves the following steps [1]:

Step 1. Select Protective Strategies.

Step 2. Assess Design Opportunities and Constraints.

Step 3. Determine Required Protective Measures.

Step 4. Integrate Protective Measures Into Protective System.

Step 5. Estimate Protective System Cost.

Step 6. Assess Protective System Acceptability.

Step 7. Prepare Documentation.

Step 1. Select Protective Strategies

The design of protective systems to meet the levels of protection for individual tactics is based on specific strategies. These strategies help designers to determine appropriate and necessary protective measures. The USCOE/PDC Security Engineering Manual [1] details strategies for each tactic.

Step 2. Assess Design Opportunities and Constraints

In the planning phase, constraints include nontechnical considerations related to user requirements. For the design phase, both opportunities and constraints relate to technical design considerations (i.e., site-specific design elements, existing protective measures, environmental factors, or project criteria not related to security).

Step 3. Determine Required Protective Measures

Protective measures should be determined for each asset and each applicable tactic. Minimum defensive protective measures (Table 1) should be considered for all facilities regardless of the tactics identified in the design basis threat.

Step 4. Integrate Protective Measures Into Protective System

The aggregate of the selected protective measures represents a preliminary protective system for an individual asset. To ensure uniform, effective protection of all assets against all threats, protective measures must be integrated into a system. The following requirements should be considered to effectively integrate a protective system:

- Compatibility with installation elements;
- Compatibility with elements of the facility; and
- Compatibility with the individual assets being protected.

The remaining compatible protective measures form the protective system for the project.

Table 1 - Minimum Defensive Protective Measures [1]

Sitework Elements

- Eliminate potential hiding places near the facility.
- Provide unobstructed view around the facility.
- Site facility within view of other occupied facilities on installation.
- Locate assets stored on site but outside of the facility within view of occupied rooms of the facility.
- Minimize need for signage or other indications of asset locations.
- Minimize exterior signage which may indicate location of assets.
- Provide 170-foot minimum facility separation from installation boundary.
- Eliminate lines of approach perpendicular to the building.
- Minimize vehicle access points.
- Eliminate parking beneath facilities.
- Locate parking as far from facility as practical.
- Illuminate building exterior or exterior sites where assets are located.
- Secure access to power/heat plants, gas mains, water supplies, electrical service.
- Locate public parking areas within view of occupied rooms or facilities.
- Locate construction staging areas away from asset locations.
- Site facility away from vantage points.
- Locate the facility away from natural or manmade vantage points..

Building Elements

- Locate critical assets on interior of facility.
- Minimize window area.
- Glass doors in foyers backed by solid door or wall.
- Do not allow windows to be next to doors such that aggressors could unlock the doors through them.
- Secure exposed exterior ladders, fire escapes.
- Lay out buildings to conceal assets and make access difficult for intruders.
- Simplify building configuration to eliminate hiding places.
- Design circulation to provide unobstructed views from control points or occupied spaces.
- Arrange building interiors to eliminate hiding places around asset location.
- Locate assets in spaces occupied 24 hours/day where possible.
- Locate activities with large visitor populations away from protected assets where possible.
- Locate protected assets in common areas where they are visible to more than one person.
- Place mailroom on perimeter of facility.

Step 5. Estimate Protective System Cost

Cost estimates may be obtained from security equipment manufacturers, building contractors, etc. The USCOE/PDC Security Engineering Manual [1] provides cost data for various protective measures as well as names and addresses for various security equipment manufacturers.

Step 6. Assess Protective System Acceptability

Acceptability of the protective system to the user of the assets depends on the system's cost effectiveness, its impact on operations, and its compliance with the design criteria established in the planning phase.

Step 7. Prepare Documentation

Since security engineering is generally only one of the many disciplines involved in a project, the documentation for the protective system needs to be incorporated into the overall documentation package.

III. Selected Federal Government Activities

The purpose of this section is to present a brief review of various Federal government activities pertaining to physical security or protection, especially those activities which relate to the development of standards, guidelines, design manuals, etc. Because of limitations of this study, it was only possible to compile such information relating to a small number of Federal departments and agencies. In addition, for those departments and agencies discussed, no attempt has been made to include all pertinent activities which a particular department or agency may be engaged.

A. Department of Defense

1. General

Among lead responsibilities assigned to the Department of Defense (DOD) in Part 5 of E.O. 12656 are the following:

> "(1) Ensure military preparedness and readiness to respond to national security emergencies;
>
> "(3) Develop and maintain, in cooperation with the heads of other departments and agencies, national security emergency plans, programs, and mechanisms to ensure effective mutual support between and among the military, civil government, and the private sector;
>
> "(9) Develop, in coordination with the Secretary of Labor, the Directors of the Selective Service System, the Office of Personnel Management, and the Federal Emergency Management Agency, plans and systems to ensure that the Nation's human resources are available to meet essential military and civilian needs in national security emergencies;
>
> "(13) In cooperation with the Secretary of Commerce and other departments and agencies, identify those industrial products and facilities that are essential to mobilization readiness, national defense, or post-attack survival and recovery."

2. Key Asset Protection Program

DOD Directive 5160.54, June 26, 1989 [2], which is referenced in the definition of "essential facilities" on page 2, outlines DOD policy, responsibilities, and procedures for the DOD Key Asset Protection Program (KAPP). The Executive Agent for KAPP is the Commander in Chief, Forces Command (CINCFOR). As indicated in Section D of DOD Directive 5160.54, it is DOD policy to:

> "Develop and promote the security of Key Assets within the United States and in U.S. territories and possessions by providing to the owners or managers of such assets appropriate advice, guidance, and planning assistance on the application of physical security and emergency preparedness measures. Such assistance is designed to encourage owners and civil law enforcement agencies to protect Key Assets from sabotage,

espionage, and other hostile or destructive acts, and to minimize the effect of attack damage.

"Recognize that, in peacetime, responsibility for protecting Key Assets, and for structuring their physical security, rests primarily with their civil sector owners and with local, State, and Federal law enforcement agencies. However, the Department of Defense must participate with the civil sector and such law enforcement authorities in planning for the protection of Key Assets during a national security emergency, and must be prepared, in concert with the appropriate authorities and within defense priorities to assist in their protection."

As Executive Agent for KAPP, the CINCFOR is, among other responsibilities, required to:

- "Administer, publish, and distribute the Key Assets List (KAL);
- "Coordinate with FEMA and with other Departments and Agencies, as required, to solicit nominations of infrastructure assets (except telecommunications);
- "Coordinate with the Manager, National Communications System (NCS), to solicit nomination of telecommunication assets;
- "Coordinate with the Director, Defense Investigative Service (DIS), to facilitate training and information of DIS Industrial Security Representatives on threats to Key Assets and other planning matters, and provide guidance to the Director, DIS, for the conduct of Key Asset vulnerability surveys."

As stated in the DOD Key Asset Protection Program Regulation [3], the purpose of a DIS vulnerability survey is to determine the vulnerability of a key asset to sabotage and other hostile or destructive acts by assessing the adequacy and effectiveness of physical security systems and emergency preparedness measures, and to provide recommendations for their improvement.

Among definitions included in DOD Directive 5160.54 are the following:

"***Key Asset***. Any industrial asset and any infrastructure asset that is nominated for inclusion on the KAL in accordance with the criteria specified.[7] Key Assets are owned in all cases by civil agencies or the private sector, and do not include any military facility.

---

[7] "Any asset nominated for inclusion in the KAL must be either:
"1. An industrial asset that produces items on the Commander in Chief's Critical Items List or on a similar list of critical items prepared by a DOD Component, and whose loss would halt or unacceptably delay DOD mobilization, deployment, or sustainment efforts; or
"2. An infrastructure asset whose loss would halt or unacceptably delay DOD mobilization and deployment efforts."

"*Industrial Asset*. Any factory, plant, building, or structure used for manufacturing, production, processing, repairing, assembling, storing, or distributing a product or components deemed essential to a DOD Component.

"*Infrastructure Asset*. Any communication or computer facility or system; any energy source or distribution system; any air, rail, road, or water transportation asset; and any other facility that is required to support an industrial asset listed in KAL or a military facility, or to otherwise support DOD mobilization, deployment, or sustainment efforts."

Among major asset categories identified in the DOD Key Asset Protection Program Regulation [3] are: Utilities and Services; Chemicals, Drugs, and Plastics; Basic Industry Materials and Products (except chemicals); Ordnance; Transportation Equipment; Machinery (except electrical); Electronic and Electrical Equipment; Professional and Scientific Equipment and Instruments; and Miscellaneous Manufactured Products. A sample Key Asset Physical Security Plan is also included in the DOD Key Asset Protection Program Regulation [3].

3. U.S. Army Corps of Engineers

Protective Design Center. The U.S. Army Corps of Engineers established the Protective Design-Mandatory Center of Expertise in the Omaha District of the Missouri River Division in November 1985. Now known as the Protective Design Center (PDC), it coordinates the Corp's extensive protective design expertise and serves as the Army's single point of contact on protective design issues. Responsibilities of the PDC include all aspects of the following: nuclear weapons effects-resistant design; conventional explosives and weapons effects-resistant design; biological and chemical protective design; electro-magnetic compatibility design; physical security and anti-terrorism design; and facility design requiring explosive safety considerations. The PDC keeps abreast of the state of the art in protective design through contacts with other U.S. Government agencies, foreign governments, and the private sector.

One of the excellent documents prepared by the PDC is the Security Engineering Manual [1]. First published in August 1987 and revised in January 1990, the manual presents the concepts of security engineering in a form which can be understood and used by both nontechnical people and design engineers. The manual provides guidance for establishing security design criteria for facility design and for designing facilities to resist acts of aggression by criminals, protestors, terrorists, and subversives. The design criteria include the assets requiring protection, the threats to those assets, the degree to which the assets should be protected from the threats, and any user-imposed constraints to the design. The design guidance is considered sufficient for programming level and concept (35 percent) level design. The security engineering design process discussed in Section II.B of this report briefly summarizes the process described in the Security Engineering Manual. Currently this manual is being revised and expanded and will be published as a series of joint Army and Air Force Technical Manuals [4].

Other documents prepared by the PDC include the following Corps of Engineers Guide Specifications (CEGS) and Engineering Technical Letters (ETL). Brief descriptions of these documents are included in Appendix B.

- o "Vehicle Barriers," CEGS 02835.
- o "Bullet Resistant Components," CEGS 13770.
- o "Bullet Resisting Glazings," ETL 1110-1-135.
- o "Fragment Retention Film for Glass," ETL 1110-1-136.
- o "Entry Points/Access Control Points," ETL 1110-3-392.
- o "Security Engineering Criteria for Medical Facilities," ETL 1110-3-398.

Guide specifications on blast resistant doors and windows, and test standards for the forced entry resistance of security structures and structural sub-assemblies are other documents being prepared by the PDC.

Key Asset Protection Program Construction Option (KAPPCO). One of PDC's activities is providing technical support to the DOD Key Asset Protection Program Construction Option (KAPPCO). KAPPCO is managed by the U.S. Forces Command (FORSCOM) Engineer and supports the KAPP described previously. KAPPCO is defined as "a system of engineer construction measures (e.g., barriers, berms, fencing, lighting, etc.) that significantly improves key asset defenses against threats such as vehicle bombs, thrown or placed bombs, standoff weapons, forced entry, and surveillance. In support of KAPP, KAPPCO serves as leverage to reduce the forces required to protect key assets." Primary PDC responsibilities under KAPPCO include: (1) serving as the FORSCOM Engineer's technical representative in the field; (2) participating in Key Asset vulnerability surveys with the Defense Investigative Service (DIS) and the State Area Command (STARC); and (3) providing 'expedient' protective defensive measure plans for incorporation into the STARC's defensive plans for key assets.

Other PDC responsibilities include: (1) developing categories of key assets from the Key Asset List; (2) developing weapon and tool mixes for each category of key asset; (3) developing generic guidebooks for each category of key asset; (4) developing a Protective Measures Catalog for KAPPCO [5]; and (5) providing training in security engineering and KAPPCO survey requirements to other DOD engineers.

Research. The Corps of Engineers is also actively involved in physical security research and development [6]. In addition to the PDC, the Construction Engineering Research Laboratory (CERL), and the Waterways Experiment Station (WES) are involved in this program. The program includes the two major areas of integrated physical security and terrorist threat protection, and is being done in cooperation with the Naval Civil Engineering Laboratory and the State Department. The objective of the research on integrated physical security, being performed by CERL, Champaign, Illinois, is to find new and improved ways to incorporate physical security into facilities at the most efficient time and in

the most effective manner. Terrorist threat protection research is carried out by the Structures Laboratory, WES, Vicksburg, Mississippi. The objective of this research is to determine the resistance of common building components and materials to the effects of various weapons, including small arms, antitank weapons, and explosives.

The Corps of Engineers is also doing research in intrusion detection systems (IDS) through the Cold Regions Research and Engineering Laboratory and WES in coordination with the Corps of Engineers' IDS Center of Expertise in Huntsville, Alabama.

B. Department of Energy

1. General

Among lead responsibilities assigned to the Department of Energy (DOE) in Part 7 of E.O. 12656 are the following:

> "(1) Conduct national security emergency preparedness planning, including capabilities development, and administer operational programs for all energy resources, ...
>
> "(2) Identify energy facilities essential to mobilization, deployment, and sustainment of resources to support the national security and national welfare, and develop energy supply and demand strategies to ensure continued provision of minimum essential services in national security emergencies."

2. Office of Energy Emergencies

As indicated above, the Department of Energy (DOE) is the lead government agency for energy emergency preparedness. Its mission is to ensure that adequate energy supplies are available to support the Nation's infrastructure during a national emergency. The DOE Office of Energy Emergencies (OEE), which was created in 1981 in response to Executive Order 11490, is responsible for dealing with energy system vulnerability concerns [7].

Recently, the OEE developed a Vulnerability Program whose purpose is to reduce the risks of energy system interruption. The Program consists of four phases. Phase I included case studies to determine the nature of vulnerabilities in the electric power, petroleum, and natural gas industries. This effort included considerable input from industry, Federal, State, and local governments. The results of the study are classified. Phase II establishes an industry outreach program which provides information and solicits industry/government joint cooperation. Phase III of the program includes additional case study exercises and other outreach efforts. Phase IV will identify national security vulnerabilities which cannot be addressed by the respective industries. This phase may include federally funded programs to remedy energy system vulnerability concerns [7]. At this time, Phases I, II, and III have been completed, and Phase IV is underway. DOE has established a threat notification system to alert energy industries. Notification consists of message describing a threat that could lead to aggressive actions.

Because of a growing concern about international terrorism, the NSC directed DOE to establish the Interagency Group on Energy Vulnerability (IGEV). The Group was charged with developing initiatives to decrease vulnerability and mitigate the impact on national security of any disruptions. In late 1988, the IGEV was terminated and its concerns and functions merged into a new interagency group, the Policy Coordinating Committee on Emergency Preparedness and Mobilization Preparedness, Standing Committee on Energy. In addition to DOE, committee members include the Departments of Defense, Justice, Interior, State, Transportation, and Treasury; Central Intelligence Agency; Federal Bureau of Investigation; Federal Emergency Management Agency; National Communications System; National Security Council; and the Nuclear Regulatory Commission.

3. Sandia National Laboratories

In support of the DOE nuclear safeguards and security program, Sandia National Laboratories, Albuquerque, New Mexico, has conducted many significant research programs pertaining to the physical protection of facilities. Results of these research efforts have been incorporated in numerous technical reports and manuals. Among excellent manuals prepared by Sandia are the following:

- o Access Delay Technology Transfer Manual [8]. The purpose of this manual is: (1) to define the role of barriers in a physical protection system; (2) to provide a central source of penetration times for barriers for physical protection systems effectiveness evaluations and for use by designers; and (3) to define methods for upgrading existing barriers and to define advanced concepts for new or replacement barriers with increased penetration times.

- o Entry-Control Systems Technology Transfer Manual [9]. This manual presents the general philosophy of entry-control systems and provides guidance on the selection, installation, and maintenance of entry-control equipment. Descriptions of available equipment and equipment under development are also included.

- o Video Assessment Technology Transfer Manual [10]. Guidelines for the selection, procurement, installation, testing, and maintenance of components used in the design of a video assessment system are provided in this manual.

C. Nuclear Regulatory Commission

One of the lead responsibilities assigned to the Nuclear Regulatory Commission in Part 21 of E.O. 12656 is as follows:

> "(1) Promote the development and maintenance of national security emergency preparedness programs through security and safeguards programs by licensed facilities and activities."

Title 10 Code of Federal Regulations, Part 73 (10 CFR 73) contains requirements for the physical protection of nuclear plants and materials. The purpose of these requirements is the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear

material at fixed sites and in transit and of plants in which special nuclear material is used. Design basis threats to protect against acts of radiological sabotage and to prevent the theft of special nuclear material are specified in Part 73.1 (a). The design basis threat for radiological sabotage[8] is as follows:

> "A determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment: (A) well-trained (including military training and skills) and dedicated individuals, (B) inside assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both, (C) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy, (D) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system."

Each licensee to operate a production or utilization facility must submit a physical security plan. Requirements for these plans are contained in Part 73.55 and include provisions for physical barriers, access control, detection aids (alarms), communications, testing and maintenance, and response. General criteria for the selection, training, equipping, testing, and qualification of individuals who will be responsible for protecting special nuclear materials, nuclear facilities, and nuclear shipments are included in Appendix B of Part 73. A good description and discussion of nuclear security operations is contained in Reference [11].

D. Department of State

Among lead responsibilities assigned to the Department of State (DOS) in Part 13 of E.O. 12656 are the following:

> "(1) Provide overall foreign policy coordination in the formulation and execution of continuity of government and other national security emergency preparedness activities that affect foreign relations;
>
> "(2) Prepare to carry out Department of State responsibilities in the conduct of the foreign relations of the United States during national security emergencies, under the direction of the President and in consultation with the heads of other appropriate Federal departments and agencies, including, but not limited to:

---

[8] "Radiological sabotage means any deliberate act directed against a plant or transport ... or against a component of such a plant or transport which could directly or indirectly endanger the public health and safety by exposure to radiation."

"(g) Protection of international organizations and foreign diplomatic, consular, and other official personnel and property, or other assets, in the United States, in coordination with the Attorney General and the Secretary of the Treasury;

"(i) Maintenance of diplomatic and consular representation abroad."

The DOS also has lead agency responsibility for terrorism outside the United States and is charged with maintaining the security of U.S. overseas diplomatic and consular facilities; conducting research and analysis on terrorism; and providing training for personnel of U.S. overseas missions on security and crisis management. Among DOS principal offices involved in these activities are: the Bureau of Diplomatic Security; the Bureau of Intelligence and Research; the Office of Foreign Building Operations; the Foreign Service Institute; and the Office of Foreign Missions [12].

U.S. diplomatic missions abroad are highly visible symbols of the U.S. government and therefore present a convenient and primary target for terrorism, as well as for hostile intelligence activities. To help ensure that every foreign service building and compound, regardless of location, has at least minimum built-in-safeguards, the DOS has developed a Security Manual for new office building projects [13]. This manual addresses security-related issues throughout the pre-design, design, construction, equipment installation, and turnover phases of a new office building.

The DOS has also supported a variety of research activities relating to the physical protection of U.S. diplomatic missions. Some of these activities have included the development of test methods to measure the forced entry, blast, and ballistic resistance of materials and assemblies (see Appendix B).

E. Department of Transportation

Two of the lead responsibilities assigned to the Department of Transportation (DOT) in Part 14 of E.O. 12656 are as follows:

"(1) Develop plans to promulgate and manage overall national policies, programs, procedures, and systems to meet essential civil and military transportation needs in national security emergencies;

"(2) Be prepared to provide direction to all modes of civil transportation in national security emergencies, including air, surface, water, pipelines, and public storage and warehousing, to the extent such responsibility is vested in the Secretary of Transportation. . . .

"(6) Develop plans and procedures in consultation with appropriate agency officials for maritime and port safety, law enforcement, and security over, upon, and under the high seas and waters subject to the jurisdiction of the United States to assure operational readiness for national security emergency functions."

The Secretary of Transportation oversees the nine operating Administrations which compose the Department. Each Administration is concerned with a specific form

of transportation. They are: the Federal Aviation Administration; the United States Coast Guard; Federal Highway Administration; National Highway Traffic Safety Administration; Federal Railroad Administration; Urban Mass Transportation Administration; Maritime Administration; Saint Lawrence Seaway Development Corporation; and Research and Special Programs Administration.

1. Federal Aviation Administration

The Federal Aviation Administration (FAA) was created under Title 6 of the Federal Aviation Act of 1958 to provide for the regulation and promotion of civil aviation in such a manner as to best foster its development and safety, and to provide for the safe and efficient use of airspace by both civil and military aircraft. Federal Aviation Regulations (FAR's) are promulgated under Title 14 of the Code of Federal Regulations (CFR). FAA standards are either regulatory or non-regulatory in nature. Those in the former category are found in various numbered parts of the FAR's and are subject to review in accordance with the Administrative Rulemaking Procedures in which the public participates.
The FAA regulates aviation security as part of its mission to maintain a safe aviation environment. Part 107, Airport Security, Title 14 CFR, prescribes aviation security rules governing the operation of airports regularly serving scheduled passenger operations of air carriers required to have a security program. Part 108, Airplane Operator Security, contains rules covering the following topics: security program (form, content, and availability); screening of passengers and property; prevention and management of hijackings and sabotage events; carriage of weapons; security of airplanes and facilities; use of X-ray systems; bomb or air piracy threats; use of explosive detection systems; etc. Part 108.18 dealing with use of X-ray systems requires systems put in service after July 22, 1985, to meet certain requirements of ASTM Standard F792 (see Appendix B).

The non-regulatory standards, which are generally contained in the FAA Advisory Circulars, serve principally as the means of providing safety information to the public with respect to aircraft operations or a related aeronautical interest. For example, Advisory Circular No. 150/5360-13, dated April 22, 1988, provides guidelines for the planning and design of airport terminal buildings and related access facilities. Guidance on various aspects of airport security -- security inspection stations, security fencing and lighting -- are included in this circular.

Another very important element of FAA's security program is the protection of FAA facilities such as air traffic control centers and the various computer and telecommunication systems which are vital to air traffic operations.

The main thrust of FAA's security research and development program initiated in 1976 has been on the development of automated detection equipment to screen passengers, baggage, and cargo for concealed deadly or dangerous weapons and explosives [14]. FAA has approached the problem of detecting the terrorists' tools, weapons, and explosives by focusing on detecting the fundamental properties of the threat. Mature technologies, like thermal neutron analysis, are currently undergoing airport testing, and other technologies are being pursued in anticipation of potential threats such as the nonmetallic handgun. The goal of the FAA research program is "to develop technology to fit into a

total security system to deter and defeat threats against air transportation [14]." Most of the FAA security research is carried out at the FAA Technical Center, Atlantic City, New Jersey. This center is at the forefront of FAA security research, and FAA is the lead agency for all Federal government research in explosive detection [15].

The President's Commission on Aviation Security and Terrorism report dated May 15, 1990, found that current aviation security systems are inadequate to provide protection against terrorist acts. Accordingly, the Congress passed and the President approved (November 16, 1990) the "Aviation Security Improvement Act of 1990" (P.L. 101-604). The Act establishes a position of Director of Intelligence and Security in the Office of the Secretary of Transportation and an Assistant Administrator of Civil Aviation Security in the FAA. In regard to measures to strengthen air transportation security, the Act requires the Assistant Administrator to review and, as necessary, develop:

> "(1) measures to strengthen controls over checked baggage in air transportation, such as measures to ensure baggage reconciliation and inspection of items in baggage of passengers which could potentially contain explosive devices;
>
> "(2) measures to strengthen control over individuals with access to aircraft;
>
> "(3) measures to improve testing of security systems;
>
> "(4) measures to ensure the use of best available x-ray equipment for air transportation security purposes; and
>
> "(5) measures to strengthen preflight screening of passengers."

2. U.S. Coast Guard

The Office of Marine Safety, Security, and Environmental Protection has responsibility for the U.S. Coast Guard's Port Safety and Security Program. Port safety is defined as the safeguarding of U.S. ports, waterways, port facilities, vessels, property, and persons in the vicinity of those ports from accidental harm. Port security is defined as the safeguarding of ports, from threats such as: thefts; destruction, loss, or injury from sabotage or other subversive acts; or other causes of a similar nature that are intentional [16].

The Port Safety Program is carried out by 47 U.S. Coast Guard Marine Safety Offices covering the entire United States, Puerto Rico, and the Virgin Islands. The Captain of the Port (COTP) is the Coast Guard person in port areas responsible for maintaining the safety and security of the port. Regulations for the protection and security of vessels, harbors, and waterfront facilities are promulgated by the U.S. Coast Guard in Part 6, Title 33, Code of Federal Regulations.

In response to the Achille Lauro incident in 1985, the International Maritime Organization (IMO) unanimously adopted the Measures to Prevent Unlawful Acts

Against Passengers and Crews on Board Ships. These measures, although not mandatory in the United States, provide practical guidance for:

- o developing written detailed security plans for ships and terminals;
- o assigning security duties to an officer of each ship and port personnel;
- o conducting facility surveys;
- o security equipment and procedures;
- o training;
- o standardizing procedures and formats for reports to national governments and IMO; and
- o improving exchange of information and intelligence.

The U.S. Coast Guard has also begun the development of U.S. Maritime Physical Security Standards which would be used as the basis for shipboard and facility security surveys in an effort to identify and overcome security shortfalls at U.S. commercial ports and facilities [16].

3. Urban Mass Transportation Administration

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 the development of mass transportation systems [17].

The Office of Safety, an independently operating functioning unit of UMTA, provides guidance, research support, and training assistance on transit safety and security matters. The role of this office, which reports directly to the administrator of UMTA, is to promote safety and security awareness within the transit industry. In the past, they have prepared guidelines and sponsored research studies on various aspects of transit safety, security and emergency preparedness. The Office of Safety has used research centers, such as the Transportation Systems Center in Cambridge, Massachusetts, to develop emergency preparedness guidelines for transit systems [18-20], to survey transit security problems and countermeasures [21, 22] and to examine emergency alarm systems [23].

4. Research and Special Programs Administration

The Office of Emergency Transportation in the Research and Special Programs Administration (RSPA) provides staff support to the Secretary for all emergency transportation matters including DOT continuity of operations and responses to

national security and domestic emergencies. The Transportation Systems Center (TSC), which is also a part of the RSPA, is the U.S. government's transportation research and analysis center. TSC's projects are in five major areas: Safety, Modernization, Strategic Mobility, Security, and Policy Analysis. Strategic mobility projects are concerned with methodologies and transportation data base development necessary to assess and plan for civil sector transportation requirements in times of natural disasters or threats to national security. Security projects include assessing surveillance needs and technologies, and computer/communication systems.

Among security requirements developed by the DOT are those for liquefied natural gas (LNG) facilities. These requirements, which are contained in Title 49 Code of Federal Regulations, Chapter I, Part 193, include: security procedures, protective enclosures, communications, lighting, monitoring, alternative power sources, and warning signs.

F. Department of Justice

Among lead responsibilities assigned to the Department of Justice (DOJ) in Part 11 of E.O. 12656 are the following:

> "(1) Provide legal advice to the President and the heads of Federal departments and agencies and their successors regarding national security emergency powers, plans, and authorities;
>
> "(2) Coordinate Federal Government domestic law enforcement activities related to national security emergency preparedness, including Federal law enforcement liaison with, and assistance to, State and local governments;
>
> "(7) Develop intergovernmental and interagency law enforcement plans and counterterrorism programs to interdict and respond to terrorism incidents in the United States that may result in a national security emergency or that occur during such an emergency."

Support responsibilities assigned to the DOJ include assisting "the heads of Federal departments and agencies, Sate and local governments, and the private sector in the development of plans to physically protect essential resources and facilities."

Among counterterrorism-related activities and programs pursued by the DOJ through the Federal Bureau of Investigation (FBI), the Justice Department's Criminal Division and the Immigration and Naturalization Service are the following:

- "Carries out its lead agency function to prevent, respond to, and investigate violent criminal activities of international and domestic terrorist groups within U.S. jurisdiction;
- "Collects and investigates intelligence on terrorists to predict potential movement or criminal activities;

- "Investigates terrorist incidents and related criminal activities using investigative techniques to identify, arrest, prosecute, and incarcerate those responsible; and

- "Maintains operational liaison with local law enforcement agencies throughout the United States [12]."

1. Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI), under the direction of the Attorney General, is the lead Federal agency responsible for preventing, interdicting, and investigating domestic and international terrorist activities. The FBI collects information about individuals, group memberships, associations, movements, etc., that serves as a basis for prosecution and builds an intelligence database for future prevention of terrorist acts [24].

The FBI's international terrorism is carried out under the auspices of the Counterterrorism Program[9]. The mission of the program is to detect, prevent, and react to unlawful violent activities of individuals or groups whose intent is to (1) overthrow the government; (2) interfere with the activities of a foreign government in the United States; (3) impair the functioning of the federal government; or (4) deprive Americans of their civil rights [24].

2. National Institute of Justice

The National Institute of Justice (NIJ) is the research branch of the Department of Justice (DOJ). The Institute's mission is to develop knowledge about crime, its causes and control. One of the activities carried out by the NIJ is the Technology Assessment Program (TAP). For about 20 years, the TAP has established minimum performance standards for equipment (e.g., body armor, weapons, handcuffs, patrol cars, communication equipment) used by law enforcement agencies, and has tested commercially available equipment against those performance standards.

The Office of Law Enforcement Standards (OLES) at NIST is funded by NIJ to develop the minimum performance standards mentioned above. OLES also conducts research on new technology and develops technical reports and guides on how equipment performs in the field. An Advisory Council composed of more than 40 nationally recognized criminal justice practitioners from Federal, State, and local agencies assess equipment needs and assist the program in setting priorities for the development of equipment standards, guides, test reports, and other special publications. The TAP Information Center (TAPIC) coordinates the Advisory Council's activities, selects certified laboratories to test equipment, oversees the testing process, and guided by NIJ and OLES, publishes Equipment Performance Reports documenting the test results. TAPIC also publishes Consumer

---

[9] Executive Order 12333, dated December 1, 1981, and related statues provide the authority for the FBI, pursuant to regulations established by the Attorney General, to conduct counterintelligence activities both within and outside the United States [24].

Product Lists of equipment that complies with NIJ standards. A number of the NIJ standards are described in Appendix B.

3. National Institute of Corrections

The National Institute of Corrections (NIC), Department of Justice, is a national center of assistance to corrections at the federal, state, and local levels. The goal of the agency is to aid in the development of a more effective, humane, safe, and constitutional correctional system. The Institute is both a direct service and a funding organization, with legislative mandates to provide training, technical assistance, and information services and to undertake research, evaluation, and policy and standards formulation to improve correctional practices at the state and local levels [25].

NIST Study. Because of building equipment and system performance problems in many new detention and correctional facilities, NIC funded a study (1986 - 1988) at the Center for Building Technology, National Bureau of Standards (now the Building and Fire Research Laboratory, National Institute of Standards and Technology). The general objective of this study was to develop guidelines, test methods and the technical bases for standards which would assist in the selection, application, and maintenance of building materials, equipment and systems for use in detention and correctional facilities [26].

During the first year of the study, emphasis was placed on identifying performance problems associated with various equipment and systems, and reviewing available guidelines and standards which might be applicable or useful in the design and construction of facilities. In general, it was determined there are only a few standards (test methods, specifications, practices) available which directly relate to special materials, equipment and systems used in detention and correctional facilities. Accordingly, when the architect and correctional official specify and select equipment and systems for a new facility, they have to rely, in most instances, on data from non-standard test methods, performance information based on prior use, recommendations from manufacturers and consultants, and their own judgement. Based on this information, recommendations were made regarding the need for developing specific criteria and standards to assist in improving the state-of-the-art of selecting materials, equipment and systems.

In the second year of the NIST study, preliminary performance criteria for materials, equipment and systems used in detention and correctional facilities were prepared [27]. The objectives of these criteria were: (1) to establish performance levels for building materials, equipment and systems which are consistent with the security and custody levels used in detention and correctional facilities; and (2) to establish standard performance measures with regard to security, safety, and durability for building materials, equipment and systems. Part I of the criteria report contained general considerations pertaining to the overall facility -- its mission, security levels, and operation; and various options and issues relating to the selection of the facility site. Part II contained requirements and criteria relating to the perimeter security of the facility (e.g, perimeter fencing and intrusion detection systems). Part III included requirements and criteria pertaining to

various building systems (e.g., walls, floors/roofs, doors, windows, glazing, locks, control center, alarms, and communications).

4. U.S. Marshals Service

The U.S. Marshals Service (USMS) of the Department of Justice is the agency with principal responsibility for the protection and security of federal judicial facilities. Other departments and agencies such as the Federal Bureau of Investigation (FBI) and the General Services Administration also assist the USMS in fulfilling this protective function. The FBI has no direct role in court security but supports the USMS by investigating threats against court officials and providing intelligence information.

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

- o "Judicial Facility Security Program, which provides security systems and equipment and court security officers;

- o "Courtroom Security Program, which provides deputy marshals for security in court proceedings and for other duties such as handling juries;

- o "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

- o "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 program [17]."

The Court Security Division has prepared several specifications for x-ray and metal detector screening equipment (see Appendix B) and is presently revising its Courts Design Guide.

G. General Services Administration

1. General

Some of the lead responsibilities assigned to the General Services Administration (GSA) in Part 18 of E.O. 12656 are as follows:

> "(1) Develop national security emergency plans and procedures for the operation, maintenance, and protection of federally owned and occupied buildings managed by the General Services Administration, and for the construction, alteration, and repair of such buildings;
>
> "(3) Develop national security emergency operational plans and procedures for the use of public utility services (other than telecommunications

services) by Federal departments and agencies, except for Department of Energy-operated facilities;

"(5) Develop plans and operating procedures for the use, in national security emergencies, of excess and surplus real and personal property by Federal, State, and local governmental entities."

GSA's Federal Protective Service (FPS), a part of the Public Building Service (PBS), provides a comprehensive security package to client/tenant Federal agencies throughout the United States, Puerto Rico, and the Virgin Islands. These agencies occupy approximately 6,800 GSA-owned, -controlled, or -leased buildings housing 930,000 employees and accommodating thousands of visitors daily. FPS's goal is to provide security and protection for the federal work place, prevent disruption of operations, and ensure the safety of employees and visitors nationwide [28].

2. Federal Product Descriptions

Under 41 CFR Part 101-29, the Administrator of GSA is responsible for establishing polices and procedures, in coordination with other agencies, for the preparation, coordination, approval, issuance, and maintenance of product descriptions in the Federal series of specifications, standards, and commercial item descriptions. Federal Supply and Services, GSA, is responsible for issuing and maintaining a handbook setting forth operating procedures and applicable definitions in the development of Federal product descriptions and for promulgating and maintaining an index of Federal specifications, standards, and commercial item descriptions. The Department of Defense (DOD) also lists Federal product descriptions in a DOD index of specifications and standards. There are approximately 6,000 Federal product descriptions in use, of which 50 percent have been assigned to other agencies.

3. Security Equipment

Another responsibility assigned to the GSA is the development of standards for security equipment to store classified information. As indicated in the Federal Register (Vol. 47, No. 123, page 27840, June 25, 1982), "The administrator of General Services shall, in coordination with agencies originating classified information, establish and publish uniform standards, specifications, and supply schedules for security equipment designed to provide secure storage for and to destroy classified information. Any agency may establish more stringent standards for its own use. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above and shall, to the maximum extent practicable, be of the type available through the Federal Supply System."

To assist GSA in the development of the standards and specifications mentioned above, the GSA has established an Interagency Advisory Committee on Security Equipment (IACSE) [29]. The committee has the following functions:

"a. Advises and assists the Assistant Commissioner for Commodity Management, FSS, in the development of specifications, standards, and test requirements for security equipment;

"b. Develops and recommends item requirements and performance standards for security equipment;

"c. Evaluates results of inspections and tests of security equipment;

"d. Provides a forum for the interchange of pertinent information of interest to the security community;

"e. Develops, maintains, and publishes a data base of specifications, standards, performance and product information of interest to the security community;

"f. Recommends practices and standards for use of security equipment; and

"g. Performs other activities to carry out the objectives of the Committee."

The committee consists of representatives from the following departments and agencies: Departments of Interior, State, Defense, Justice, Commerce, Energy, Treasury, Transportation, Veterans Affairs, Central Intelligence Agency, Federal Emergency Management Agency, United States Information Agency, General Services Administration, Nuclear Regulatory Commission, National Aeronautics and Space Administration, Environmental Protection Agency, and the United States Postal Service.

Some of the standards and specifications developed by GSA on definitions, security vault doors, combination locks, security filing cabinets, modular vault systems, etc., are briefly described in Appendix B.

IV. Selected Non-Government Activities

The purpose of this section is to present a brief review of various non-government activities pertaining to physical security or protection, especially those activities which relate to the development of standards, guidelines, design manuals, etc. Although more than ten private sector organizations (i.e., trade associations, professional societies) were contacted during the course of this study, only a few such organizations, as discussed in the following sections, are directly involved in the development of guidelines, manuals, standards, etc. In addition, for those organizations discussed, no attempt has been made to include all pertinent activities which that organization may be engaged.

A. Building Research Board

The Building Research Board (BRB) is one of operating units under the National Research Council, National Academy of Sciences (NAS). The National Research Council was established by the NAS in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and of advising the Federal government. Two recent BRB studies, which are pertinent to the scope and objectives of this report, are described in the following paragraphs.

U.S. Embassy Buildings. In late 1984, the U.S. Congress, responding to growing concerns over the security of U.S. Foreign Service personnel and facilities abroad, authorized the State Department to carry out advanced research on the development and application of state-of-the-art security measures. At the request of the State Department, the BRB established in 1985 the Committee on Research for the Security of Future U.S. Embassy Buildings. The committee's recommendations, which were contained in two 1986 reports (one classified and one unclassified), were concerned with security-related issues in virtually every aspect of the planning, design, construction, and management of the State Department's overseas buildings [30].

In brief, the committee recommended "that the State Department adopt a process of thorough and regular security impact assessments. Such a process would begin at the earliest stages of project conception and run throughout the life cycle of the embassy building, serving as the basis for designed responses to actual and perceived security threats." In addition, the committee also recommended:

> "rigorous new procedures, guidelines, and criteria for the identification and evaluation of sites for future embassy buildings taking into account a full range of security considerations and integrating them with other aspects of site development;
>
> "security-conscious site planning and design guidelines to ensure that maximum advantage is taken of the protection that can be afforded by site size, perimeter access controls, and landscape planning;
>
> "revised guidelines for the location and arrangement of functional areas within embassy buildings to ensure that the most vital and sensitive aspects of foreign operations are afforded maximum protection from threats of takeover and espionage;

"new guidelines and criteria for the protection of electrical, mechanical, and communications systems within buildings and for the use of state-of-the-art security and access-control systems as complements to security-conscious building design;

"changes in current State Department practices and procedures in such areas as capital construction program management, the selection and management of architects, engineers, and construction contractors, and the management of information about foreign buildings; and

"an ongoing building research and development program within the State Department, directed in part toward the improvement of physical and technical security in embassy buildings [30]."

Federal Office Buildings. Recognizing that many Federal agency security programs are designed to protect against theft, vandalism and other types of transgressions --not terrorist's acts, the BRB established another committee of experts in 1988 to develop a report that addresses measures and techniques to protect federal buildings, and the people and information within them, against acts of terrorism [31].

The Committee report offers the following recommendations:

"1. An ongoing security program should be developed and implemented by agencies that own or lease federal office buildings.

"2. Top management should be responsible for security policy and implementation.

"3. Security strategies should be developed with a clear understanding and assessment of the threat.

"4. A formal means of threat communication should be established.

"5. Every federal office building should undergo a vulnerability analysis.

"6. A base line or minimum level of protection should be established for each federal office building.

"7. Temporary protective measures should be systematically reviewed."

B. American Society for Industrial Security

The American Society for Industrial Security (ASIS) was officially incorporated in 1955. It currently has a headquarters staff of 42 and a membership of more than 24,000. One of the purposes of the ASIS is "to encourage, promote, aid in, and effect the voluntary interchange among the members of the Society, of data, information, experience, ideas, knowledge, methods, and techniques relating to the field of industrial security [32]."

Although the ASIS conducts a wide range of activities (i.e., seminars, training courses, certification program for professionals, exhibits, committee meetings,

liaison with government agencies, etc.) and publishes a monthly magazine, Security Management, it does not develop standards. Some ASIS members, however, do participate in other organizations or committees which develop standards. One indication of the broad range of ASIS activities is the following partial list of their standing committees: Disaster Management, Energy Security, Computer Security, Government Security, Physical Security, Retail Security, Terrorist Activities, Utilities Security, Telecommunications, and Transportation Security. The Physical Security Committee is concerned with the fundamentals of physical security: guard patrols, perimeter boundaries, and mechanical and electrical protection systems. It also initiates and promotes research and prepares suggested programs on physical security.

C. Electric Utilities

The Federal government has limited authority or responsibility to provide physical protection for energy systems. Individual utilities are responsible for protecting their physical plants and ensuring reliability. Utilities build redundancy into their systems and plan for inevitable but occasional equipment failure but do not consider multi-site sabotage when designing the systems [7].

North American Electric Reliability Council (NERC). NERC and its nine regional councils were established in the late 1960's to assist utilities in providing for the reliability and adequacy of electric generation, transmission, and distribution systems. In 1987, NERC established the National Electric Security Committee (NESC) to assess the degree of vulnerability to sabotage and terrorism. The committee established three working groups which dealt with physical security enhancements, operating strategies, and design and restoration improvements. The NERC Board of Trustees approved the committee report in October 1988 and most of the recommendations contained in the report have been implemented. Having completed its mission, the NESC was disbanded and related activities assigned to NERC's Engineering and Operating Committees or to the Regional councils or the utilities [7].

Edison Electric Institute (EEI). The EEI has established a security committee, which consists of 70 members who are responsible for physical protection of utilities' facilities. More than one-half of the committee's members, according to EEI, are ex-FBI agents or members of other law enforcement agencies. EEI's security committee facilitates security information exchange among its members, NERC, and government agencies [7].

D. National Cargo Security Council

The National Cargo Security Council (NCSC) is a non-profit corporation dedicated to the improvement of cargo security practices and procedures by shippers and transport carriers of all modes in the domestic and international commerce of the United States. The purposes of the NCSC are: (1) to improve cargo transportation security by providing leadership in voluntary industry efforts; (2) to act as a central clearinghouse for the collection and dissemination of information relating to trends, techniques, and results of efforts to prevent cargo crimes; (3) to articulate such purposes to the public in general, government agencies and commerce and industry matters relating to security of cargo; and (4) to assist and support voluntary and self-help initiatives by cities, transportation

centers, and industry cargo security groups to develop effective endeavors and programs to combat cargo crimes. The Council is headquartered in Washington, DC and has members from all segments of commerce and trade, as well as state and local police and Federal departments and agencies. The NCSC has revised and updated a "Guidelines for the Physical Security of Cargo," which was originally published by the Department of Transportation [33].

E. American Society for Testing and Materials

As discussed in Appendix A, there are some 400 private sector organizations involved in developing standards. Approximately 275 (69 percent) have ongoing standardization programs. The remainder have prepared a few standards, occasionally update them, but are not actively or routinely engaged in standards development.

Organized in 1898, the American Society for Testing and Materials (ASTM) is one of the largest voluntary standards development systems in the world. From the work of 133 technical standards-writing committees, ASTM publishes more than 8,000 standards each year in the 68 volumes of the Annual Book of ASTM Standards [34].

Of particular interest to this study is the work of ASTM Committee F12 on Security Systems and Equipment. Established in 1972, the scope of the committee is: "To develop and standardize terminology, test methods, specifications, performance specifications, classifications, and practices for security systems, components, and equipment for security of property and life and product counterfeit protection." Currently, the committee has about 160 members and has the following six standards-writing subcommittees: Systems, Products and Services; Anticounterfeiting Systems; Locking Devices; Controlled Access Security, Search, and Screening Equipment; Protective Containment Structures; and Definitions and Nomenclature.

To date, ASTM Committee F12 has developed about 20 approved standards and is working on about 10 new standards. For example, one of the new standards under development by the F12 Subcommittee on Systems, Products, and Services, is a guide for determining design criteria for the physical protection of a facility. This proposed new standard covers the planning phase of the security engineering design process described in Section II.B.1 of this report.

V. Discussion and Recommendations

A. Discussion

1. Protection of Essential Resources and Facilities

As defined in the proposed rulemaking (44 CFR Part 335), "essential resources and facilities," cover a wide variety of assets, both government and private. Similarly, protection for these essential resources and facilities is defined as a process which must deal with a "full spectrum of threats." Information on the various factors and elements involved in the planning, design, and construction of physical security or protection for various assets is presented in Section II. The primary reason for including this information was to indicate the broad range of topics and issues which should be considered in determining physical protection systems for essential resources and facilities.

Accordingly, it is important that FEMA guidance and information developed for other Federal agencies and the private sector should contain similar detailed information and data which are relevant for a wide range of assets and threats. Such guidance and information will also aid in establishing a more uniform process for the preparation of physical protection priorities and plans for essential resources and facilities. As discussed below, some of the needed information can be made available through the development of appropriate criteria and standards.

2. Standards

One of the objectives of this study is "to identify and compile existing standards and guidelines pertaining to the protection of facilities and resources." As described in Appendix A, a "standard" has a broad meaning. A standard can be a test method, a specification, a practice, a terminology, a guide, or a classification. Appendix A also briefly describes who develops standards in the United States and cites the various benefits of standardization.

Existing standards pertaining to physical security and protection which were identified in this study are briefly described in Appendix B. Of the 110 standards listed in Appendix B, 42 are Federal government standards and 68 are private sector standards. In a few cases, there is some duplication in the standards because the private sector standards were developed using the Federal standards as a starting point. The reverse may also be true (i.e., Federal standards were developed using the private sector standards as a starting point). To aid in locating a standard, the standards in Appendix B have been grouped into seventeen subject categories: general planning and design; fencing and gates; intrusion detection and alarms; vehicle barriers; walls and floors; doors; windows and glazing; ballistic resistance; access control; locks; vaults and storage systems; surveillance systems; screening devices; security seals; electrical; data transmission; and economics.

In the consideration of the topics and issues discussed in Section II, standards can be very useful and important tools in the selection of an acceptable physical protective system. For example, a standard guide would be very helpful in assessing the likely tactics and weapons to be used against a particular asset

in order that a design basis threat and a level of protection can be established. A standard specification would be an important aid in the selection and procurement of an intrusion detection system. In addition, a standard test method for determining forced entry resistance of wall systems would be a valuable resource in obtaining data which can be used to compare the forced entry resistance of one wall system with another wall system. Also, a standard economic practice would be useful in evaluating investments in different protective systems.

3. Federal Government and Private Sector Activities

During recent years, terrorist acts and threats, both domestically and internationally, have increased the awareness of government agencies and the private sector to the importance of physical security and the need to assess the level of protection provided to important assets. A brief review of various Federal government activities pertaining to physical security or protection is presented in Section III. Even though it was not possible to review all the pertinent activities of these selected few departments and agencies, the information collected does indicate that there is a substantial amount of Federal government activity being directed toward the planning, design, and research of physical security and protection systems. These activities include the preparation of design criteria and manuals; the development of standards; and the testing of security materials, components, and equipment. A number of these activities involve or impact the private sector, as well as State and local governments (i.e., DOD Key Asset Protection Program; DOE Vulnerability Program, DOJ Technology Assessment Program; FAA Security Program).

In a 1988 U.S. General Accounting Office (GAO) report of antiterrorism practices in two components of the nation's infrastructure -- federal court facilities and mass transit systems, GAO made the following pertinent comments [17]:

> "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."

In regard to the selected private sector organizations discussed in Section IV, there is also considerable interest and involvement in physical security and protection activities, including the development of standards. Since both the private and public sectors own essential resources and facilities, it is important that a close working and cooperative relationship be developed between both sectors for the protection of such resources and facilities.

B. Recommendations

1. Coordinated Program

Although there is some dialogue and sharing of information between various Federal departments and agencies regarding their particular physical security

programs, there remains, based on this study, an important need to develop a coordinated program for identifying and physical protecting national resources and facilities. Such a program should establish a clear and working relationship between the DOD Key Asset Protection Program and the physical protection programs being conducted by all other Federal Departments and agencies. In addition, this coordinated program can also be used to help establish priorities and resources for the collection and dissemination of physical security data and information and the development of national voluntary standards as discussed in the following recommendations

2. Physical Security Information and Data

Since limitations of this study did not permit a complete review of all pertinent Federal government activities relating to the physical protection of facilities and resources, it is recommended that such a comprehensive study be conducted. This study should identify and briefly describe various physical security activities and resource information (manuals, research data, standards) as well as list individual contacts (names, addresses, and telephone numbers) within the various Federal agencies. Information and data collected in the study would be a very useful resource for all Federal agencies having a responsibility for protecting essential resources and facilities. Such information would also be a useful resource in the coordination of Federal department and agency activities as discussed above. It is estimated the initial cost of this comprehensive study would be about $200,000. To keep the information relatively up to date and useful, it is also recommended that the report be revised on annual basis.

As appropriate, available and non-classified information on Federal physical security activities, such as a list of technical manuals or standards, etc., should also be made available to private sector organizations.

3. Development of National Voluntary Standards

In order to provide detailed guidance on physical protection to Federal departments and agencies and to owners of essential facilities and resources, it is recommended that the proposed criteria (44 CFR Part 335.6) be expanded or supplemented with standards. As discussed above, such standards can be used to help establish the required level of physical protection needed for specific assets and threats. In addition, other types of standards can be used to assist in the selection and evaluation of various protective materials and systems.

Proposed 44 CFR Part 335.7 indicates that "plans and strategies will be coordinated with FEMA by the Federal departments and agencies ... to assist them in developing Federal Standards ..." Although many Federal Departments and agencies may have a need to develop their own standards, such departments and agencies should also be encouraged to participate in voluntary standards bodies as outlined in OMB Circular No. A-119 (see Appendix A). Such participation can help reduce duplication of standards development efforts in the government sector and can greatly assist in developing high priority voluntary standards which could be used by both government and the private sector.

Among high priority national voluntary standards which should be developed are standard guides which would cover the planning and design phases of the security

engineering design process described in Section II. Such standards should be flexible enough to deal with the many different types of essential resources and facilities. As necessary, and to avoid duplication or conflicts, it is recommended that the development of criteria and standards be closely coordinated with the DOD Key Asset Protection Program and the Key Asset Protection Program Construction Option. To expedite the development of such standards, it is recommended that funding be made available to agencies that have developed pertinent background information and data such as U.S. Army Corps of Engineers Protective Design Center in order to develop draft standards and to assist in processing such draft standards into national voluntary standards for use by government and the private sector.

In regard to physical security equipment and systems, additional national voluntary standards need to be developed. Among high priority standards are specifications and test methods for intrusion detection systems, access control systems, and screening devices. Similarly, as mentioned above, to expedite the development of such standards, it is recommended that funding be made available to agencies that have developed pertinent background information and research data (see Section III).

The annual funding required for the development of the standards described above will depend on the total number of standards needed as well as the desired time table for completing all the desired standards. Initially, it is recommended that a minimum of $200,000 per year be made available to assist in the preparation of high priority standards.

VI. References

1. Security Engineering Manual, U.S. Army Corps of Engineers, Protective Design Center, Missouri River Division, Omaha District, January 1990 (For Official Use Only).

2. "DOD Key Asset Protection Program (KAPP)," Department of Defense Directive 5160.54, June 26, 1989.

3. "DOD Key Asset Protection Program Regulation," Department of Defense, Coordinating Draft DOD 5160.54-R, 23 February 1990.

4. Technical Manuals -- Security Engineering - Project Development, Concept Design, and Final Design, Army TM 5-853-1 -- Army TM 5-583-3, Air Force AFM 88-6, Vol. 1 -- Vol. 3, respectively, (Drafts - For Official Use Only).

5. A Protective Measure Literature Search and Product Catalog: Part I - Protection Equipment and Part II - Protective Measures, Key Asset Protection Program Construction Option (KAPPCO), November 1990 (For Official Use Only).

6. Security Engineering Update," U.S. Army Corps of Engineers, Missouri River Division, Omaha District, Protective Design Center, August 1990.

7. Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage, OTA-E-453, U.S. Congress, Office of Technology Assessment, June 1990.

8. Access Delay Technology Transfer Manual, Nuclear Security Systems Directorate, SAND 87-1926, Sandia National Laboratories, September 1989 (Not for Public Dissemination).

9. Entry Control Systems Technology Transfer Manual, Nuclear Security Systems Directorate, SAND 87-1927, Sandia National Laboratories, May 1989 (Not for Public Dissemination).

10. Video Assessment Technology Transfer Manual, Nuclear Security Systems Directorate, SAND 89-1924, Sandia National Laboratories, October 1989 (Not for Public Dissemination).

11. Utility Security Operations Management (For Gas, Water, Electric and Nuclear Utilities), Clay E. Higgins, Charles C. Thomas, Publisher, Springfield, Illinois, 1989.

12. Public Report of the Vice President's Task Force on Combatting Terrorism, February 1986.

13. Security Manual - New Office Building Projects, U.S. Department of State, Bureau of Diplomatic Security, December 1989 (Not for Public Dissemination).

14. "Research and Development," Lyle Malotky, Federal Aviation Administration, Joint Government-Industry Symposium on Transportation Security, Williamsburg, VA, March 21-22, 1990, pp. 94 - 112.

15. FAA Technical Center, Federal Aviation Administration, U.S. Department of Transportation, 1991.

16. "Maritime Terrorism," Admiral Joel D. Sipes, U.S. Guard, Joint Government-Industry Symposium on Transportation Security, Williamsburg, VA, March 21-22, 1990, pp. 185 - 189.

17. Domestic Terrorism -- Prevention Efforts in Selected Federal Courts and Mass Transit Systems, U.S. General Accounting Office, GAO/PEMD-88-22, June 1988.

18. Recommended Emergency Preparedness Guidelines for Rail Transit Systems, W.T. Hathaway, S.H. Markos, R.J. Pawlak, U.S. Department of Transportation, Research and Special Programs Administration, Transportation Systems Center, Cambridge, MA, UMTA-MA-06-0152-85-1, March 1985.

19. Recommended Emergency Preparedness Guidelines for Elderly and Disabled Rail Transit Passengers, W.T. Hathaway, S.H. Markos, J.N. Balog, U.S. Department of Transportation, Research and Special Programs Administration, Transportation Systems Center, Cambridge, MA, UMTA-MA-06-0186-89-1, August 1989.

20. Recommended Emergency Preparedness Guidelines for Urban, Rural, and Specialized Transit Systems, W.T. Hathaway, S.H. Markos, U.S. Department of Transportation, Research and Special Programs Administration, Transportation Systems Center, Cambridge, MA, UMTA-MA-06-0196-91-1, January 1991.

21. Case Studies of Transit Security on Bus Systems, E.O. Hargadine, Mandex, Inc., McLean, VA, sponsored by the Urban Mass Transportation Administration, UMTA-VA-06-0088-83-1, August 1983.

22. Transit Security: A Description of Problems and Countermeasures, R.A. Mauri, N.A. Cooney, G.J. Prowe, U.S. Department of Transportation, Research and Special Programs Administration, Transportation Systems Center, Cambridge, MA, UMTA-MA-06-0152-84-2, October 1984.

23. Emergency Alarm Systems: Improved Emergency Alarm/Response System, Metropolitan Transit Authority of Harris County, Metro Transit Police, Houston, TX, sponsored by the Urban Mass Transportation Administration

24. International Terrorism -- FBI Investigates Domestic Activities to Identify Terrorists, U.S. General Accounting Office, GAO/GGD-90-112, September 1990.

25. Annual Report for Fiscal Year 1984, U.S. Department of Justice, National Institute of Corrections, April 1985.

26. Standards for Building Materials, Equipment and Systems Used in Detention and Correctional Facilities, Robert D. Dikkers, Belinda C. Reeder, NBSIR 87-3687, National Bureau of Standards, November 1987.

27. Preliminary Performance Criteria for Building Materials, Equipment and Systems Used in Detention and Correctional Facilities, Robert D. Dikkers, Robert J. Husmann, James H. Webster, John P. Sorg, and Richard A. Holmes, NISTIR 89-4027, National Institute of Standards and Technology, January 1989.

28. "A Program for Professionalism," Ed Rao, Donna Gregory, Security Management, American Society of Industrial Security, Arlington, VA, February 1991, pp. 79 - 82.

29. "Interagency Advisory Committee on Security Equipment (IACSE)," GSA Order ADM 5420.15I, December 30, 1986.

30. The Embassy of the Future: Recommendations for the Design of Future U.S. Embassy Buildings, Committee on Research for the Security of Future U.S. Embassy Buildings, Building Research Board, National Research Council, National Academy Press, Unclassified Report, September 1986.

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

32. "35th Anniversary, 1955 - 1990," Special Supplement to Security Management, American Society for Industrial Security, 1990.

33. Guidelines for the Physical Security of Cargo," National Cargo Security Council, October 1987.

34. ASTM Annual Report - 1990," ASTM, Philadelphia, PA.

VII. Bibliography

1. Emergency Power Supplies for Physical Security Systems, Bowers, G. L.; Oak Ridge Y-12 Plant, TN, NTIS No: NUREG/CR-0509/HDM, November 1979.

2. "Perimeter Intrusion Alarm Systems," Regulatory Guide 5.44, Revision 2, U.S. Nuclear Regulatory Commission, Washington, DC, May 1980.

3. Current Methods for Evaluation of Physical Security System Effectiveness, Davidson, Robert B.; Rosengren, Jack W.; R and D Associates, Arlington, VA; NTIS No: AD-A109 726/0/HDM, May 1981.

4. "Development of Security Measures: Implementation Instructions for MIL-STD on Physical Security for DCS Facilities;" Otten, M.G.; Pierce, D.G.; Myracle, J. E.; Booz-Allen and Hamilton, Inc., Bethesda, MD, NTIS No: AD-A110 088/2/HDM, July 1981.

5. "Development of a Draft Physical Security Military Standard for Defense Communications System Facilities," Gieske, Harry A.; Otten, Michael G.; Pierce, Donald C.; Richards, Donald R.; Stevens, Jennie; Booz-Allen and Hamilton, Inc., Bethesda, MD., NTIS No: AD-A110 011/4/HDM, December 1981.

6. Building Security, Stroik, J., Editor, ASTM Special Technical Publication 729, ASTM, Philadelphia, PA, 1981.

7. High Security Locking Devices -- A State-of-the-Art Report, Stroik, J., NBSIR 81-2233, NBS, Gaithersburg, MD, January 1982.

8. Intrusion Detection Systems Handbook, SAND76-0554, Sandia National Laboratories, Albuquerque, New Mexico, August 1983.

9. Physical Security: Practices and Technology, Charles Schnabolk, Butterworth Publishers, 1983.

10. Design for Security, Second Edition, Richard J. Healy, John Wiley & Sons, 1983.

11. Security Design for Maximum Protection, Richard J. Gigliotti and Ronald C. Jason, Butterworth Publishers, 1984.

12. Commercial Intrusion Detection Systems (IDS), Design Manual 13.02, Naval Facilities Engineering Command, Alexandria, VA, September 1986.

13. Security Managers Desk Reference, Richard S. Post and David A. Schachtsiek, Butterworth Publishers, 1986.

14. Total Facility Control, Don T. Cherry, Butterworth Publishers, 1986.

15. Base Vulnerability Assessment Guide, J. Ferritto, S. Ashley, E. Becker, B. Keane, B. Rail, J. Tancreto, Naval Civil Engineering Laboratory, Port Hueneme, CA, April 1987.

16. Physical Security: Protection of Assets at U.S. Navy Bases, U.S. General Accounting Office, Washington, DC., NTIS No: PB88-134994/HDM, October 1987.

17. Blast Vulnerability Guide, M.G. Whitney, D.E. Ketchum, M.A. Polcyn, Southwest Research Institute for the Naval Civil Engineering Laboratory, Port Hueneme, CA, October 1987.

18. Design Guidelines for Physical Security of Fixed Land-Based Facilities, MIL-HDBK-1013/1, NAVFAC, 1987.

19. Intrusion Detection Systems, Second Edition, Robert L. Barnard, Butterworth Publishers, 1988.

20. Structures for Enhanced Safety and Physical Security, Proceedings of the Specialty Conference sponsored by the Structural Division of the American Society of Civil Engineers, Theodor Krauthammer, Editor, American Society of Civil Engineers, NY, NY, 1989.

21. "Terrorism and the Communication Utilities: A National Security Concern," Green, L.G., Army War College, Carlisle Barracks, PA, NTIS No: AD-A208 668/4/HDM, February 1989.

22. Aviation Security -- Training Standards Needed for Extra Security Measures at Foreign Airports, U.S. General Accounting Office, GAO/RCED-90-66, December 1989.

23. Security Engineering, Intrusion Detection Systems, Revised Final Draft, Technical Manual 5-853-4, R.E. Timm & Associates for the U.S. Army Corps of Engineers, Huntsville Division, March 1990.

APPENDIX A

An Overview of Standards Terminology and the Standards Development Process

Overview of Standards

The American Society for Testing and Materials (ASTM) defines a standard as "a rule for an orderly approach to a specific activity, formulated and applied for the benefit and with the cooperation of all concerned [1][1]." A more specific definition of a standard provided by the National Standards Policy Advisory Committee is "a prescribed set of rules, conditions, or requirements concerning definitions of terms; classification of components; specification of materials, performance or operation; delineation of procedures; or measurement of quantity and quality in describing materials, products, systems, services, or practices" [2]. In terms of building design and construction, a standard may be a specific set of requirements or instructions for the testing, design, manufacture, installation, and use of a building material, component or system [3].

A standard exists when an agreement has been obtained on its content. The level of agreement may range from a consensus of employees of an organization (company standard) to a full consensus developed by representatives of all sectors that have an interest in the use of the standard (consensus standard). Consensus standards generally receive the highest level of recognition by regulators and others involved in the building process because of the rigorous procedural requirements and broad participation in the process. They are more readily accepted and used than are industry standards developed under limited participation procedures [4].

Types of Standards. ASTM develops six different types of full consensus standards which are defined in the following paragraphs [1]. Other standards developing organizations such as the American Society of Mechanical Engineers (ASME), Building Hardware Manufacturers Association (BHMA), National Fire Protection Association (NFPA), etc. produce similar types of standards which may have different names and definitions.

"A standard test method is a definitive procedure for the identification, measurement, and evaluation of one or more qualities, characteristics, or properties of a material, product, system, or service that produces a test result." An example of this type of standard is ASTM F1233, Test Method for Security Glazing Materials and Systems, which is used to evaluate the resistance of security glazing materials against various threats -- ballistic impact, blunt and sharp tool impacts, etc.

---

[1] Numbers in brackets pertain to references listed on page 52.

"A standard specification is a precise statement of a set of requirements to be satisfied by a material, product, system, or service that also indicates the procedures for determining whether each of the requirements is satisfied." An example of a standard specification is ASTM A585, Specification for Aluminum-Coated Steel Barbed Wire. It contains requirements for aluminum-coated steel barbed wire consisting of a strand of two wires, coated before fabrication, with 4-point barbs.

"A standard practice is a definitive procedure for performing one or more specific operations or functions that does not produce a test result." A good example of this type of standard is ASTM E917, Practice for Measuring Life-Cycle Costs of Buildings and Building Systems. This practice describes step-by-step procedures for using the life-cycle cost method.

"Standard terminology documents contain definitions and descriptions of terms, or explanation of symbols, abbreviations, and acronyms." ASTM F471, Definition of Terms Relating to Combination Locks, is such a standard.

"A standard guide offers a series of options or instructions, but does not recommend a specific course of action. Where a standard practice prescribes a general usage principle, a guide only suggests an approach." An example of this standard type is ASTM F1029, Guide for the Selection of Physical Security Measures for a Facility. It contains information to aid in the selection of effective security measures to deter or detect an attack on a facility. These measures depend upon the threat level and the asset (risk) level of the facility.

"A standard classification is a systematic arrangement or division of materials, products, systems, or services into groups based on similar characteristics such as origin, composition, properties, or use." An example of this standard type is ASTM F832, Classification for Security Seals. It covers classifications for categories of commercially available seals.

Performance vs. Prescriptive Standards. A prescriptive standard is quite specific in nature giving details of usage or design procedures for a building material, component or system. An example of a prescriptive requirement would be that wall framing shall be 2 x 4 wood studs on 16-inch centers. A performance standard prescribes objectives, conditions and criteria to be accomplished and allows broad leeway for the designer to achieve results. The performance statement for the above condition would be that the wall system shall be designed to specified loading and deformation criteria allowing the innovative designer freedom to select the materials and other specific construction details.

Standards Development Process

Organizations Involved. Currently, the U.S. standardization community maintains more than 94,000 standards [5]. Table A shows the various categories of standards developers and their output. The private sector has prepared about 45% of the total. As indicated in Table A, private sector organizations that are active in standards development can be categorized in three groups: scientific and professional societies, trade associations, and

standards developing organizations. At any time during the past 20 to 30 years some 400 private sector organizations have been developing standards. Approximately 275 organizations have ongoing standardization programs. The remainder have prepared a few standards, occasionally update them, but are not actively or routinely engaged in standards development.

TABLE A. U.S. STANDARDS AND THEIR DEVELOPERS

Government	Number of Standards	
Defense	38,000	40%
Federal (GSA)	6,000	6%
Other	8,500	9%
	52,500	55%
Private Sector		
Scientific & Professional Societies	13,000	14%
Trade Associations	14,500	16%
Standards Developing Organizations	14,000	15%
	41,500	45%
Total	94,000	

Of the 52,500 government standards, 38,000 have been prepared by the Department of Defense (DOD), and 6,000 are Federal standards and specifications developed for Federal procurement under the auspices of the General Services Administration (GSA). It is estimated that another 8,500 standards have been developed by federal agencies such as the Occupational Safety and Health Administration (OSHA), the Environmental Protection Agency (EPA), and the Food and Drug Administration (FDA).

More than 11,000 (12%) standards are applicable to building and construction. More than 200 government and private sector organizations develop standards in this sector.

According to Toth [5], the number of available standards may not be indicative of their value to industry and commerce. The real value of standards is realized only when they are used. Standards developers indicate that 80% of the orders for individual standards are for 15 or 20% of the total number published.

The standards of the 20 major private sector standards developers (Table B) constitute 75 percent of the nongovernment standards database.

Legal Aspects. In addition to its technical credibility, a standard must rest on sound legal principles if it is going to stand the tests of time and use. In the United States, there are four principles which impact standards development: due process, restraint of trade, authority and responsibility,

TABLE B. 20 MAJOR NON-GOVERNMENT STANDARDS DEVELOPERS

	Number of Standards
Aerospace Industries Association	3,000
American Association of Cereal Chemists	370
American Assoc. of State Highway & Transportation Officials	1,100
American Conference of Governmental Industrial Hygienists	700
American National Standards Institute	1,400*
American Oil Chemists Society	365
American Petroleum Institute	880
American Railway Engineers Association	300
American Society of Mechanical Engineers	745
American Society for Testing and Materials	8,500
Association of American Railroads	1,350
Association of Official Analytical Chemists	1,900
Cosmetic, Toiletry and Fragrance Association	800
Electronic Industries Association	600
Institute of Electrical and Electronics Engineers	575
National Fire Protection Association	275
Society of Automotive Engineers	5,100
Technical Association of the Pulp and Paper Industry	270
Underwriters Laboratories	630
U.S. Pharmacopeia	4,450

*Published and copyrighted by ANSI.

and liability. Among other important points, due process provides everyone on a standards committee with a voice in the development of a standard, including an opportunity for anyone to appeal if they are dissatisfied. In order for standards to avoid restraint of trade violations, measures must be taken to prevent them from unreasonably restricting competition by stifling innovation or by excluding potential competitors from established markets. The third principle, authority and responsibility, requires that organizations have authorization in their charters for developing standards, have written procedures for developing, promulgating and maintaining standards, etc. The fourth legal principle, liability, is especially of interest to individuals working on standards development committees. In the case of ASTM, which is a nonprofit corporation chartered in Pennsylvania, members of a nonprofit corporation are not personally liable for debts, liabilities, or obligations of the corporation.

Benefits of Standardization

In addition to improving safety and safeguarding health, standards serve to greatly simplify commerce in a highly industrialized society and provide a common language that promotes the flow of goods between buyer and seller. Thousands of standards are available for referencing in building codes, construction specifications, purchase orders, etc. Other commercial benefits of standards include [1]:

- Greater user confidence in commodities purchased.
- Better understanding of how to use commodities.
- Improved organizational integration, especially between sites.
- Better quality control.
- Lower inventories for both producer and user through elimination of unnecessary grades.
- Earlier delivery because of the ability to stock standard items.
- Better performance at lower prices through reduced need for negotiations and more efficient inspection and testing.

Federal Government in the Voluntary Standards Developing Process

OMB Circular No. A-119 [6] recognizes the existence of many standards prepared by private voluntary standards bodies which are appropriate or adaptable for the Government's use. Through participation in, and support for, private standards making activities, Federal agencies may benefit greatly from private expertise and will avoid the wasteful duplication of cost and effort involved in developing their own in-house standards. Such standards development, when properly conducted, can increase productivity and efficiency in industry, expand opportunities for international trade, conserve resources, and improve health and safety.

The OMB Circular states that it is the policy of the Federal Government in its procurement and regulatory activities to:

"a. Rely on voluntary standards, both domestic and international, whenever feasible and consistent with law and regulation pursuant to law;

"b. Participate in voluntary standards bodies when such participation is in the public interest and is compatible with agencies' missions, authorities, priorities, and budget resources; and

"c. Coordinate agency participation in voluntary standards bodies so that (1) the most effective use is made of agency resources and representatives; and (2) the views expressed by such representatives are in the public interest and, as a minimum, do not conflict with the interests and established views of the agencies."

The circular recommends that voluntary standards be given preference over non-mandatory Government standards unless use of such standards would have significant disadvantages. Priority should be given to voluntary standards based on performance criteria in lieu of design, material, or construction criteria. Voluntary standards adopted by Federal agencies should be referenced in appropriate publications, regulatory orders, or in-house documents. Federal agencies are not prohibited from developing and using Government standards in the event that voluntary standards bodies cannot or do not develop a needed, acceptable standard in a timely fashion.

References (Appendix A)

1. "Standards Make the Pieces Fit," ASTM, 1916 Race Street, Philadelphia, PA 19103.

2. "The ABC's of Standards - Related Activities in the United States," Maureen A. Breitenberg, NBSIR 87-3576, National Bureau of Standards, Gaithersburg, MD, May 1987.

3. "Standards -- Tools for Excellence," Robert D. Dikkers, Corrections Today, American Correctional Association, April 1987.

4. "International Harmonization of Standards," James G. Gross, Proceedings of the Eighth Structures Congress - Prospects for International Practice, American Society of Civil Engineers, New York, NY, May 1990.

5. "Standards Activities of Organizations in the United States," Robert B. Toth, Editor, NIST Special Publication 806, National Institute of Standards and Technology, Gaithersburg, MD, February 1991.

6. "Federal Participation in the Development and Use of Voluntary Standards," Office of Management and Budget (OMB) Circular A-119, October 26, 1991.

Appendix B -- Brief Descriptions of Selected Standards Pertaining to Physical Security and Protection

TABLE OF CONTENTS

1.0 ACRONYMS

ANSI	American National Standards Institute, Inc.
ASTM	American Society for Testing and Materials
BHMA	Builders Hardware Manufacturers Association
CEGS	Corps of Engineers Guide Specification
ETL	Engineering Technical Letter (Corps of Engineers)
FCGS	Federal Construction Guide Specification
HPW	H.P. White Laboratory, Inc.
ICBO	International Conference of Building Officials
LESL	Law Enforcement Standards Laboratory, NIST (now the Office of Law Enforcement Standards)
MIL	U.S. Military Specification
NAAMM	National Association of Architectural Metal Manufacturers
NBS	National Bureau of Standards (now NIST)
NIJ	National Institute of Justice
NILECJ	National Institute of Law Enforcement & Criminal Justice (now NIJ)
NIST	National Institute of Standards and Technology
SD	U.S. Department of State
SDI	Steel Door Institute
UL	Underwriters Laboratories, Inc.
USMS	United States Marshals Service

2.0 GENERAL PLANNING & DESIGN

ASTM E1334-90 Practice for Preparing a Serviceability Rating of a Building or Facility

Scope: A definitive procedure for objectively and reliably rating the capability of a facility to perform to any required level of functionality. It can also be used to compare how well different buildings or facilities can meet any given set of serviceability requirements, despite differences such as location, structure, mechanical systems, age and building shape.

ASTM F967-87 Practice for Security Engineering Symbols

Scope: Practice for using symbols to depict security systems and equipment requirements for architectural or engineering drawings. Eight pages of symbols. Symbol categories are: Annotation, Access Control, Annunciation: Console/Panel, Annunciation: Devices, Barriers and Vehicle Controls, Communications, Electrical, Lighting, Miscellaneous, Sensors, Surveillance, Switches, and Door and Locking Hardware.

ASTM F1029-86 Guide for the Selection of Physical Security Measures for a Facility

Scope: Aid in the selection of effective security measures to deter or detect an attack on a protected facility. Four threat levels based on skill of attacker and four asset (risk) levels -- residential, commercial, industrial, and very high risk facilities are defined. A threat/physical security matrix identifies protective measures and instrumentation applicable for protecting the above facilities from the various threat levels.

ETL 1110-3-398-1988 (Corps of Engineers) Engineering and Design - Security Engineering Criteria for Medical Facilities

Scope: Provides security engineering criteria which establish the minimum design requirements for security against potential hostile aggression for the design and construction of Army health facilities. Discusses the security engineering design process, modes of aggression, protective measures and design strategies, and cost strategies.

FED-STD-800-89 Terms, Definitions and Symbols for Security Equipment and Practices

Scope: Provides terms, definitions and symbols for security equipment and practices used by government agencies.

ICBO - 88 Uniform Building Security Code

Scope: Establishes minimum standards to make dwelling units resistant to unlawful entry. Allows jurisdictions to enact the code as Chapter 41 of the Uniform Building Code (UBC). Addresses obstructing exits, tests and identification, entry vision, swinging doors, sliding doors, and windows. Includes UBC Standards No. 41.1 and 41.2 (see below).

UBC Standard No. 41.1 - Tests for Doors and Locking Hardware Used for Security
Part I - Swinging Doors and Locking Hardware on Such Doors
Deadbolt Lock Tests: static dead-bolt load test, lock impact, cylinder core tension test, cylinder torque, bolt impact.
Door and Bolt Impact Tests: impacts to panels and flush face doors; bolt and rail or stile impact test.
Part II - Horizontal Sliding Door Assemblies
Hand manipulation; tool manipulation; static load

UBC Standard No. 41.2 - Tests for Window Assemblies
Hand manipulation; tool manipulation; static load and locking device test

3.0 FENCING & GATES

3.1 Electric-Fence Controllers

UL 69-87 Electric Fence Controllers

Scope: Covers electric fence controllers to be employed on lighting or power circuits in accordance with the National Electrical Code, NFPA 70. Covers both battery operated and lighting or power circuits of 125 volts or less, or combination controllers. Ten performance tests are specified.

3.2 Chain Link Fencing & Gates

ASTM A116-88 Specification for Zinc-Coated (Galvanized) Steel Woven Wire Fence Fabric

Scope: Covers zinc-coated steel fabric suitable for farm field, railroad, and highway, right-of-way and similar fencing, having a series of horizontal (line) wires with vertical (stay) wires woven or wrapped around the line wires, forming rectangular openings. Provides mostly design information. One test is weight of zinc coating.

ASTM A392-89 Specification for Zinc-Coated Steel Chain-Link Fence Fabric

Scope: Covers fence fabric, zinc-coated before or after weaving. Tests for weight of coating in accordance with A90 and shall meet minimum breaking strengths specified in A817 when tested in accordance with A370.

ASTM A491-89 Specification for Aluminum-Coated Steel Chain-Link Fence Fabric

Scope: Covers fence fabric, aluminum-coated before weaving. Test for weight of coating as specified in A817.

ASTM F552-86 Definitions of Terms Relating to Chain-Link Fencing

Scope: About 50 items defined and 16 illustrations provided.

ASTM F567-84 Practice for Installation of Chain-Link Fence

Scope: Covers installation procedure including site preparation, post location and setting, terminal post bracing, top rail and tension wire, chain-link fabric, barbed wire, gates, etc.

ASTM F573-84 Specification for Residential Zinc-Coated Steel Chain-Link Fence

Scope: Covers 11 1/2-gage (2.87 mm) steel chain-link fence fabric, zinc-coated after weaving. Specifies weave, size of mesh (2 1/8 in.), breaking strength (750 lbf), size of wire, height of fabric (up to 60 inches).

ASTM A584-88 Specification for Aluminum-Coated Steel Woven Wire Fence Fabric

Scope: Covers aluminum coated steel fence fabric suitable for such uses as railroad or highway right-of-way and similar fencing, having a series of horizontal (line) wires with vertical (stay) wires woven or wrapped around the line wires, forming rectangular openings. Test for minimum weight of coating.

ASTM F626-89a Specification for Fence Fittings

Scope: Covers materials, coating requirements, and inspection of fence accessories: post line caps, rail/brace ends, sleeves-top rail, tie wires and clips, tension and brace bands, tension bars, truss rods, and barb arms.

ASTM F668-88 Specification for Poly (Vinyl Chloride) (PVC)-Coated Steel Chain-Link Fence Fabric

Scope: Covers fabric coated before weaving. Nominal heights 3, 3.5, 4, 5, 6, 7, 8, 9, 10 and 12 feet. Largely design specification in which class of PVC coating, the color, the size of mesh, size of wire, the height and length of fabric in each roll of fabric must be identified.

ASTM F669-85 Specification for Strength Requirements of Metal Posts and Rails for Industrial Chain-Link Fence

Scope: Covers strength requirements of metal posts and rails for heavy and light industrial chain-link fence up to 12 feet high with a spacing of posts not exceeding 10 ft. Posts and rails may have any cross-sectional shape that will meet this specification's requirements. Heavy industrial fence - most rigid and mechanically durable. Light industrial fence - 80% of load bearing capability of heavy industrial fence. Strength and stiffness criteria specified. Satisfactory designs are classified by product/special requirement as follows: A120, steel pipe (Specification A120), aluminum pipe, steel pipe (commercial standards), roll formed steel shapes, hot-rolled shapes, and alternative designs.

ASTM A702-87 Specification for Steel Fence Posts and Assemblies, Hot Wrought

Scope: Covers steel fence posts and assemblies manufactured from hot-wrought sections and intended for use in field and line fencing. The posts are available in tee, channel, or U or Y-bar shapes or angle shapes. Tests are for tensile strength, hardness, weight and zinc coating.

ASTM F761-85 Specification for Strength Requirements of Steel Posts and Rails for Residential Chain-Link Fence

Scope: Similar to F669 except it covers steel posts and rails for residential chain link fence up to 6 ft. high with line posts at a maximum spacing of 10 ft.

ASTM A817-86 Specification for Metallic-Coated Steel Wire for Chain-Link Fence Fabric

Scope: Covers steel wire (2 types of coatings) used for the manufacture of chain-link fence fabric. Tests for weight of coating and adherence of coating.

ASTM F900-84 Specification for Industrial and Commercial Swing Gates

Scope: Covers detailed requirements for chain-link fence gates, gate posts and accessories for both single and double swing-type gates for industrial and commercial application.

FCGS 02444-85 Fence, Chain-Link

Scope: Design specification that relies heavily on RR-F-191 specifications. Provides general guidance for installation. No performance specifications or test methods.

RR-F-191-90 Fencing, Wire and Post, Metal (Gates and Chain-link Fencing Fabric and Accessories)

Scope: Specification covers general requirements for chain link fencing and accessories. Cites ASTM Standards D3951, D3953 and F552.

3.3 Barbed Wire/Tape

ASTM A121-86 Specification for Zinc-Coated (Galvanized) Steel Barbed Wire

Scope: Covers zinc-coated steel barbed wire, consisting of a strand of two wires, in a number of sizes and constructions with two classes (weights) of zinc coating. Orders must identify number of spools, size and construction, class of coating, copper-bearing steel, if required. Specifies size and permissible variations. Test methods for weight of coating (A90) and breaking strength.

ASTM A585-86 Specification for Aluminum-Coated Steel Barbed Wire

Scope: Covers aluminum-coated steel barbed wire, consisting of a strand of two wires, coated before fabrication, with 4-point barbs. Two types are provided as specified by the spacing of the barbs. Test methods for weight of coating (A90) and breaking strength.

MIL-B-52775-81 Barbed Tape, Obstacle, General Purpose and Barbed Tape, Fence Topping

Scope: Covers three types of stainless steel barbed tapes. References MERADCOM drawings TA13220E8351, Barbed Tape, Obstacle, General Purpose, Stainless Steel (another MERADCOM drawing is referenced in California prison design specs). Inspection for breaks or cracks is required using at least 10x magnification. If defects are not clearly identifiable, then E165 for liquid penetrant inspection is required. Quality Assurance section defines acceptable quality levels (% defective).

RR-F-191/1A-76 Fencing Wire (Barbed Wire)

Scope: Covers specific requirements for barbed wire of five types: zinc-coated, aluminum coated, aluminum clad, copper clad, plastic coated. Mostly a detailed design specification although tests are specified for coating weight and thickness and "breaking strength" (a non-standard tensile test).

4.0 INTRUSION DETECTION & ALARMS

UL 639-87 Intrusion-Detection Units

Scope: Covers intrusion detection equipment for burglary-protection signaling systems to be employed in outdoor and indoor locations to automatically indicate the presence of an intruder by actuating electrical control circuits. Installation of intrusion - detection units are covered by UL681. Numerous performance tests are listed.

UL 1076-88 Proprietary Burglar Alarm Units and Systems

Scope: Applies to construction, performance and operation of equipment intended for use in proprietary burglar alarm units/systems employed to protect against burglary. Normally intended for indoor use. Numerous performance tests are listed.

CEGS 16725-90 Intrusion Defection Systems

Scope: Provides requirements for an intrusion detection system including operator interaction, and overall system supervision and control. Products included interior sensors, exterior sensors, alarm communication system, and wire and cable.

LESL-RPT-0305.00-74 Terms and Definitions for Intrusion Alarm Systems

Scope: Several terms related to intrusion alarm systems are defined.

NIJ-0308-77 Sound Sensing Units for Intrusion Alarm Systems

Scope: Establishes performance requirements and methods of test for sound sensing devices that respond to attack noises at frequencies up to 10 kHz and are intended for use in intrusion alarm systems to provide premise-protection of vaults and other secure areas. These devices cause the initiation of a local audible alarm or the transmission of an alarm signal to a central station. Characteristics addressed are those that affect the reliability of the device, with emphasis on those that affect its false alarm susceptibility and its tamper resistance.

NIJ-0321-84 Control Units for Intrusion Alarm Systems

Scope: Establishes performance requirements and test methods for intrusion alarm control units used in protecting residential and commercial premises. Upon actuation of an intrusion sensing device or the detection of a trouble condition, the control unit may initiate a local audible alarm, transmit an alarm signal to a central station. The performance characteristics addressed are those that affect the reliability of the device with emphasis on those that affect false alarm susceptibility and tamper resistance.

W-A-00450B-73 Alarm System, Interior, Security, Components for

Scope: Covers security alarm system units which are designated to conform to the standards for security equipment as set forth in National Security directives. Highly resistive to neutralization and compromise by covert or surreptitious attack. Types included:

1) balanced magnetic switch; 2) conductive foil; 3) breakwire; 4) light threshold motion detector; 5) infra-red light beam detector; 6) passive IR detector; 7) vibration detector; 8) capacitance detector; 9) ultrasonic motion detector; 10) microwave-radio frequency motion detector; 11) pressure motion detector; 12) closed-circuit television motion detector.

Performance tests include:

Neutralization and Compromise test: "various methods shall be attempted using tools and devices not exceeding the quantity capable of being carried in two cases (not more than 10" x 20" x 27" per case)." Shall withstand attempts to neutralize or compromise for not less than 12 hours.

Stability: high temperature (120 degrees F for 4 hours); low temperature (32 degrees F for 36 hours); humidity (over 85% relative humidity for 240 hours).

5.0 VEHICLE BARRIERS

CEGS-02835-88 Guide Specification for Military Construction - Vehicle Barriers

Scope: Sets forth barrier performance requirements and a description of products including retractable vehicle barriers, vehicle crash gate, manual vehicle crack beam, electrical work, control panel and miscellaneous equipment. Installation and field testing requirements are also provided.

6.0 WALLS & FLOORS

ASTM E72-80 Methods of Conducting Strength Tests of Panels for Building Construction

Scope: Cover procedures for determining the structural properties of segments of wall, floor, and roof constructions.

Wall tests: compressive load, tensile load, transverse loads, concentrated load, impact load, racking loads
Floor tests: transverse load, concentrated load, impact loads (E695 and E661)
Roof tests: transverse load, concentrated load

ASTM E695-85 Method of Measuring Relative Resistance of Wall, Floor, and Roof Construction to Impact Loading

Scope: Covers the measurement of the relative resistance of wall, floor, and roof construction to impact loading. Not applicable to doors. Intended to be applied to relatively light construction, including but not limited to wood floor and roof systems, partitions framed with wood or steel studs, steel floor or roof decking systems, steel siding and wall panels.

HPW-TP-0400.01 - July 1985 Forced Entry Resistance of Structural Materials (Opaque and Transparent); Test Procedures and Acceptance Criteria

Scope: Sets forth test requirements for determining the forced entry resistance of materials and/or devices to be used in structures. Field-type tests are conducted with a six-member team of young, muscular males using a variety of tools (sledge, crowbar, hammer, chisels, battering ram, etc.). Test specimen is considered to be forcibly entered when it has a hole which allows passage of either a solid, incompressible object (12" x 12" x 8") or a solid, incompressible, right cylinder (12" x 12"). Similar to SD-STD-01.01.

SD-STD-01.01 - May 1983 Forced Entry Resistance of Structural Materials (Opaque and Transparent); Test Procedures and Acceptance Criteria

Scope: Sets forth test requirements for determining the forced entry resistance of materials and/or devices to be used in structures. Similar to HPW-TP-0400.01.

7.0 DOORS

ANSI/SDI 100-85 Recommended Specification for Standard Steel Doors and Frames

Scope: For swinging steel doors and frames, offers a number of choices in both regular and fire door and frame construction and design. The user must select from the specification the specific grades of doors and frames that best apply to the project. References several ASTM, ANSI, and other SDI standards. Those that may be useful include:

SDI 107	Hardware on Steel Doors (Reinforcement -- Application)
SDI 109	Hardware for Standard Steel Doors and Frames
SDI 119	Proposed Performance Test Procedures for Steel Doors Frames and Frame Anchors
ANSI A151.1	Test Procedure and Acceptance Criteria for Physical Endurance for Steel Doors and Hardware Reinforcing

ASTM F476-84 Test Methods for Security of Swinging Door Assemblies

Scope: Cover door assemblies of various materials and types of construction for use in wall openings to deter unwanted intruders and "break-in" crimes. Eleven tests: Static Bolt Load, Jamb/Wall Stiffness, Knob Impact; Cylinder-Core Tension; Cylinder-Body Tension; Knob Torque; Cylinder Torque; Cylinder-Impact; Door Impact; Hinge Impact, Hinge Pin Tensile Load; Bolt Impact. Pass/fail tests. Based on NILECJ 0306.00. Sets out door assembly minimum requirements (Grades 10, 20, 30, and 40). References California Building Security Standards study on means of forcible entry. Sets out acceptance criteria recommended in NILECJ 0306.00.

ASTM F571-87 Practice for Installation of Exit Devices in Security Areas

Scope: Information for installing exit devices used in areas of security to achieve the greatest security possible without violating the requirements and spirit of ANSI/NFPA 101 Code for Safety to Life from Fire in Buildings and Structures.

References:

ASTM F476
ANSI/BHMA A156.3 for Exit Devices - should be consulted
ANSI/BHMA A156.5 for Auxiliary Locks and Associated Products
UL 305 Panic Hardware
ANSI/UL 1034 Burglary Resistant Electric Locking Mechanisms

ASTM F842-83 Test Methods for Measurement of Forced Entry Resistance of Horizontal Sliding Door Assemblies

Scope: Methods to determine the ability to restrain, delay, or frustrate forced entry. Methods apply to horizontal sliding door assemblies for use in single and multi-family residential dwellings. Three types are classified. Intended to establish a measure of resistance to attacks by unskilled or opportunistic burglars. The following tests are included:

1) Disassembly - tools used for 5 minutes from exterior
2) Hand Manipulation - 2 adult males for 5-10 minutes
3) Tool Manipulation - 1 individual with tools for 5 or 10 minutes
4) Static Load on Panels and Locking Device Resistance
5) Glazing Impact - uses impactor described in CPSC 16 CFR 1201.

The annex provides suggested measured performance for 4 Grade levels (10, 20, 30, and 40). The appendix also cites documents of the following organizations: National Woodwork Manufacturers Association; Architectural Aluminum Manufacturers Association; ICBO; NILECJ; and California Crime Technological Research Foundation Report.

ANSI/BHMA A156.1-81 Butts and Hinges

Scope: Provides cyclical, lateral, and vertical wear tests, together with finish tests requiring salt spray exposures. Individual hinge types are described and identified with code numbers.

NAAMM HMDF-1-87 Guide Specifications for Detention Security Hollow Metal Doors and Frames

Scope: Provides background on advantages of using hollow metal doors versus bar-grille construction. Intended to be used for developing job specifications. It must be edited to fit specific job requirements.

Includes 5 performance tests:

- o static load, rack test, impact load (requires security hinge to withstand 50 impact blows of 200 lb-ft directed at the door within 6 inches of the hinge), removable glazing stops test and bullet resistance (cites procedure in UL 752, Bullet-Resisting Equipment); and
- o 2 tests for surface finish (ASTM B117 salt spray for 150 hrs. and D1735 water fog test for organic coating for 200 hours).

Metal must meet ASTM A366 or A569.

For fabrication methods and product quality, doors must meet standards set out in NAAMM Fire-Rated Hollow Metal Doors and Frames, 2nd Edition, 11/83; and NAAMM Hollow Metal Manual, 2/87.

NBS Pub 480-22-77 Terms and Definitions for Door and Window Security

Scope: Glossary of definitions for those terms most frequently encountered concerning door and window security. Terms for alarm systems are not included.

NILECJ-STD-0306.00-76 Physical Security of Door Assemblies and Components

Scope: Performance requirements and test methods for resistance of doors to forced entry. Concerned with typical entry doorways in residences and some small businesses (single pedestrian use, hinged swinging doors). Included are requirements for both the total door assembly and individual components, such as the hinges, lock, door, jamb/strike, and jamb/wall. Addresses capability to frustrate the "opportunity" crimes. Skilled methods of entry used to gain access are not addressed. Door assemblies and components are classified by relative resistance to forced entry. Door assembly tests: bolt projection strike hole, bolt pressure, jamb/wall stiffness, knob impact, cylinder core tension, cylinder body tension, knob torque, cylinder torque, cylinder impact, door impact, hinge impact, bolt impact.

NIJ Std 0318.00-80 Physical Security of Sliding Glass Door Units

Scope: Performance requirements and test methods for resistance to forced entry of sliding glass door units intended for use in residences. Two classes of units:

Class I - minimum level of physical security (designed to prevent entry by unskilled burglars)

Class II - moderate level (designed to prevent entry by most semi-skilled burglars). Does not address rarely used methods of gaining entry nor those only used by skilled burglars.

Class III - requires higher latch loading resistance, door panel removal resistance (vertical only), locking device strength, fixed panel fastening strength, meeting stile fastening strength as well as glazing impact strength.

8.0 WINDOWS & GLAZING

ASTM F588-85 Test Methods for Resistance of Window Assemblies to Forced Entry, "Excluding Glazing"

Scope: Cover window assemblies of various materials and types of construction for use in wall openings to deter unwanted intruders. Five types of window assemblies are classified. Intended to establish a measure of resistance for window assemblies subjected to attacks (other than impacting glazing materials) by unskilled or opportunistic burglars. Annex A1 provides suggested guidelines for acceptance criteria for performance levels. Tests include: hand manipulation, tool manipulation, static load and locking device strength resistance.

ASTM F1233-89 Test Method for Security Glazing Materials and Systems

Scope: Provides procedures for evaluating the resistance of security glazing materials and systems against the following threats: ballistic impact, blunt tool impact, sharp tool impacts, thermal stress and chemical deterioration. Annexes provide information on physical implement testing and recommended protection level ratings.

NIJ 0316.00-80 Physical Security of Window Units

Scope: Performance requirements and test methods for the resistance of forced entry of window units intended for use in residences and some small businesses. The skilled or rarely used methods of gaining entry is not addressed.

Four Classes: I - minimum level of physical security
II - moderate level of physical security
III - medium level of physical security
IV - relatively high level of physical security

Mode of Operations:

Type A (Sliding,), Type B (Outswinging), Type C (Inswinging), Type D (Pivoted), Type E (Fixed), and Type F (Security Window: defined as units having metal bars fastened to the exterior of the window frame for the purpose of preventing entry.)

Includes performance tests for: resistance to voiding, locking device stability, locking device strength, window strength, impact strength for glazing, sash frame, and security bars.

NIJ 0319.00-80 Metallic Window Foil for Intrusion Alarm Systems

Scope: Provides performance requirements and methods of test for metallic window foil used in intrusion alarm systems as a sensor to detect the breakage of glass. Standard only applies to metallic foil for use on glazing materials consisting solely of glass.

NIJ Report 301-85 Test Method for the Evaluation of the Penetration Resistance of High-Security Glazing Subjected to a Combined Attack of Heat and Mechanical Impact

Scope: Describes test method and equipment required to evaluate the penetration resistance of high-security glazing subjected to a combined attack of thermal and mechanical impact.

UL 972-89 Burglary Resisting Glazing Material

Scope: Requirements cover clear, translucent, or opaque glazing material intended for indoor/outdoor use principally as a substitute for plate glass windows or show case panels and intended to resist burglarious attacks of the "hit and run" type. Four types of impact tests:

1) Multiple impact (shall withstand five 50 foot-lb. impacts of a steel ball, 3-1/4" diameter, weighing 5 lb., dropped from 10 ft.)
2) Thermal Conditioning for Outdoor Use (shall withstand five 40 foot-lb. impacts of a steel ball, 3-1/4" diameter, weighing 5 lb., dropped from 8 ft. onto thermally conditioned samples -- 120 degrees F and 14 degrees F)
3) Thermal Conditioning for Indoor Use (shall withstand five 50 foot-lb. impacts of a steel ball, 3-1/4" diameter, weighing 5 lb., dropped from 10 ft. onto thermally conditioned samples -- 95 degrees F and 55 degrees F)
4) High-Energy Impact (shall withstand one impact of over 200 foot-lb. of a steel ball, 3-1/4" diameter, weighing 5 lb., dropped from 40 ft.)

ETL 1110-1-135-1987 (Corps of Engineers) Engineering and Design - Bullet Resisting Glazing

Scope: Provides information and guidance on the use of bullet resisting glazing for buildings including a glossary of terms; discussion of relevant standards; description of materials including glass, plastics and composites; and related considerations including sound transmission, attack resistance, fire resistance, and blast resistance.

ETL 1110-1-136-1987 (Corps of Engineers) Engineering and Design - Fragment retention Film for Glass

Scope: Provides guidance for using fragment retention films for glass which is beneficial in decreasing the hazards associated with the shattering of glass subjected to explosives effects, projectile impacts, and forced entry. Blast, projectile and forced entry tests are discussed.

9.0 BALLISTIC RESISTANCE

HPW TP-0300.00 - May 1984 Ballistic Resistance of Structural Materials (Opaque and Transparent); Test Procedures and Acceptance Criteria

Scope: Sets forth requirements for determining the ballistic resistance of building materials intended for use in buildings and structures (or portions thereof) which may be attacked by small arms fire. Three ratings are specified: Minimum (Submachine gun and 12 gauge shotgun); Rifle; and Rifle (Armor Piercing). Similar to SD-STD-02.01.

UL 752-90 Bullet Resisting Equipment

Scope: Requirements cover materials, devices, and fixtures used to form bullet-resisting barriers designed to protect against robbery or holdup. "Bullet-resisting" signifies that protection is provided against complete penetration, passage of fragments of projectiles, or spalling (fragmentation) of the protective material to the degree that injury would be caused to a person standing directly behind the bullet-resisting barrier. Ratings: medium-small arms, high-small arms, super-small arms, and high-powered rifle. Several test methods included.

NIJ 0108.01-85 Ballistic Resistant Protective Materials

Scope: Establishes minimum performance requirements and methods of test for all ballistic resistant materials (armor) intended to provide protection against gunfire, with the exception of police body armor and ballistic helmets. Six levels of performance are classified depending on weapons and ammunition used ranging from a 38 caliber handgun to an armor piercing rifle.

SD-STD-02.01 - March 1986 Ballistic Resistance of Structural Materials (Opaque and Transparent); Test Procedures and Acceptance Criteria

Scope: Sets forth requirements for determining the ballistic resistance of building materials intended for use in buildings and structures (or portions thereof) which may be attacked by small arms fire. Three ratings are specified: Minimum (Submachine gun and 12 gauge shotgun); Rifle; and Rifle (Armor Piercing). Similar to HPW-TP-0300.00.

CEGS-13770 (Draft October 1989) - Guide Specificatcn for Military Construction - Bullet Resistant Components

Scope: Sets forth requirements for bullet resistant components such as doors, windows, louvers, gunports, pass drawers, deal trays and speaking apertures. Lists appropriate standards, description of products, performance requirements, and installation guidelines. Provides Table of Relative Ballistic Standards for various weapons.

10.0 ACCESS CONTROL

UL 294-88 Access Control System Units

Scope: Applies to construction, performance and operation of systems intended to regulate/control (1) entry into an area or (2) access to or the use of a device(s) by electrical, electronic or mechanical means. Contains numerous tests including destructive and nondestructive attack tests of 5 minute duration. If alarm is activated during attack, duration is reduced to 2 minutes.

ETL 1110-3-392-1988 (Corps of Engineers) Engineering and Design - Entry Points/Access Control Points

Scope: Provides engineering guidance for designers and implementers for installation of facility entry access control points. Includes threat analysis, design and operation considerations, and a glossary of terms related to access control. Tables of information are provided on authorization verification techniques, biometrics identity verification techniques, weapons and explosive contraband detector techniques, and access control system guidelines.

CEGS 16752-1990 Guide Specifications for Electronic Entry Control Systems

Scope: Includes descriptions of various entry control systems and related materials and equipment, testing and training procedures, operational and maintenance considerations, and specific applications such as personnel identification control and surveillance.

11.0 LOCKS

ASTM F471-82 Definitions of Terms Relating to Combination Locks

Scope: About 50 terms used to describe various aspects of combinations locks are defined.

ASTM F883-84 Performance for Padlocks

Scope: Contains environmental, functional, operational, security requirements. Included are function descriptions, cycle tests, operational tests, environmental tests, forcing tests, and surreptitious entry tests. No effort has been made to include criteria for specially made padlocks used by the Defense Department or others in highly sensitive locations. Describes grades and various levels of performance to provide users with criteria upon which to select suitable padlocks.

ANSI/BHMA A156.2-83 Bored and Preassembled Locks and Latches

Scope: Establishes requirements for bored and preassembled locks and lock trim. Includes performance tests, operational, strength and finish tests, and dimensional criteria. Levels of performance for bored locks are set forth, and an appendix with a users guide is provided.

ANSI/BHMA A156.5-84 Auxiliary Locks and Associated Products

Scope: Contains requirements for auxiliary bored and mortise locks, rim locks, and cylinders. Included are security tests, operational tests, finish tests, and dimensional criteria. Refers to UL 1034 in regard to electric strikes. Test criteria specified for three grades of locks.

ANSI/BHMA A156.11-85 Cabinet Locks

Scope: Establishes requirements for cabinet locks used on doors, drawers, and furniture. Included are cycle, operational, strength, and finish tests; and dimensional criteria.

ANSI/BHMA A156.12-86 Interconnected Locks and Latches

Scope: Establishes requirements for interconnected locks and includes security tests, operational tests, cycle tests, finish tests, and dimensional criteria.

ANSI/BHMA A156.13-80 Mortise Locks and Latches

Scope: Establishes requirements for mortise locks and latches and includes performance tests, security tests, operational tests, finish tests, and dimensional criteria.

UL 437-86 Key Locks

Scope: Covers key locks categorized as follows: door locks, locking cylinders, security container key locks, and two-key locks. Four performance tests including endurance test, attack resistance tests, salt spray corrosion test, and polymeric materials tests. Attack resistance test time for door locks and locking cylinders is 10 minutes for picking and impression; and 5 minutes for forcing, drilling, sawing, prying, pulling, and driving using various hand tools. Effective date of many of these requirements is September 1, 1987.

UL 1034-88 Burglary Resistant Electric Locking Mechanisms

Scope: Requirements apply to the construction, performance and operation of burglary-resistant electric locking mechanisms and their related devices, such as control unit, control switch, power supply, and the like, used to secure and release doors, and the like by applying or removing electrical power. About 30 performance tests including: forcing tests (pushing and torque) and tool attack tests (5 minute duration with specified hand tools).

CEGS-08701-86 Hardware: Prison-Locking Devices

Scope: Specifies four types of deadlocks:

A. for swinging doors with or without gang-locking device;
B. for swinging doors without gang-locking device;
C. for swinging doors of cabinets;
D. for sliding doors, with or without gang-locking device.

This is a design specification. No performance tests are included.

FF-P-110-72 Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)

Scope: Covers both dial and push button designs. Required to resist opening by surreptitious and manipulation techniques for specified periods of time. No forced entry requirements. Test methods include:

a) manipulation technique; b) surreptitious attack; c) radiographic; d) direct tension; e) jar test with tension; f) jar test without tension; g) padlock shackle; and h) drop test.

FF-L-2740-89 Combination Locks

Scope: Covers changeable, combination locks designed to be mounted on safes, security files, vault doors and similar items. Items covered are materials, design, construction, security, quality assurance, and testing procedures.

MIL-L-29151-75 Locks and Lock Sets, Exterior, Ordnance, High Security

Scope: Covers key operated, high security, dead-bolt locks and lock sets, for the securing of sensitive ordnance materials. Uses several test methods including: hardness (E18), fog (B117), picking and bypassing test, key integrity test, operational test, impact test (lock shall be . . . substantially struck six times in different directions with a mallet weighing no more than 12 ounces), operational temperature test, drop test, wear test, and forced entry tests (specifies 10 types of tools, each not exceeding 10 lb. and with other restrictions, to be used to defeat the lock in less than 7 man-minutes).

MIL-H-29181-78 Hasp, High Security, Shrouded, for High and Medium Security Padlock

Scope: Covers two styles of hasps for high security padlocks. Uses two tests including: hardness (E18) and impact (E23 - notched bar impact testing of metallic materials).

MIL-P-43607-80 Padlock, Key Operated, High Security, Shrouded Shackle

Scope: Covers one type of key operated, high security, shrouded shackle padlock that employs a dead bolt locking mechanism. Uses several test methods including: surreptitious neutralization test (can the padlock be compromised without it appearing to be such), wear resistance, drop tests, shackle pull-out test, low temperature shock test, forced entry tests (specifies using, but not limited to, 6 sets of tools, not exceeding a total of 20 lb. and with other restrictions, to be used to defeat the padlock in less than 5 minutes of accumulated work time, excluding preparation, rest, and safety precaution periods), heat resistance, low temperature operation, key integrity test, fog test, key hardness, key deformation resistance, operating key function, control key function, cylinder interchangeability.

12.0 VAULTS & STORAGE SYSTEMS

AA-D-600-90 (AA-D-2757-90) Door, Vault, Security

Scope: Covers security vault doors designed to conform to the minimum standards for physical security equipment as required by the Information Security Oversight Office Directive governing the safeguarding of national security information. Doors are rated for protection against unauthorized entry for periods of time specified. References several government specifications and one voluntary standard (ASTM B-633 Standard Specification for Electrodeposited Coatings of Zinc, on Iron and Steel). Mostly design requirements, however there are four performance tests: door test for sturdiness; surreptitious and forced entry test (elaborate empirical test); entry by radiological techniques; and finish tests.

AA-V-2737-90 Modular Vault Systems

Scope: Provides requirements of a modular vault system intended to comply with the standards for security equipment required in the Information Security Oversight Office. A vault covered by the specification provides a minimum of 15 minutes of protection against a multilevel tool attack.

AA-F-00363C-90 Filing Cabinet, Security, Maps and Plans, General Filing, and Storage

Scope: Covers uninsulated, security filing cabinets designed to conform to the standards for physical security set forth in the Information Security Oversight Office.

ASTM F1090-87 Classification for Bank and Mercantile Vault Construction

Scope: Classification is for the use and guidance of those who purchase, design, construct, install, approve, or modify storage vault enclosures, intended for the protection of assets against loss due to forced entry.

ASTM F1247-89 Specification for Intrusion Resistant Generic Vault Structures

Scope: Specification is for the use and guidance of those who purchase, design, construct, install, approve, or modify generic vault enclosures, intended for the protection of valuables against loss due to forced entry. Includes descriptions of terms, classifications, materials, practices, and methods to be followed in constructing, fabricating, or modifying intrusion resistant generic vaults.

13.0 SURVEILLANCE SYSTEMS

ASTM F572-89 Practice for Application of Film Security Cameras in Financial Institutions

Scope: Guide for use in determining the type (continuous, demand, or special application) of film cameras that can be used adequately in financial institutions. Contains minimum standards to be exercised in the placement and installation of these cameras.

UL 983-88 Surveillance Camera Units

Scope: Covers surveillance cameras and accessories intended for use at mercantile and banking premises to provide a means of recording images of holdup attempts or other activities in the area. Camera may be designed to operate automatically, by manual actuation, or have dual capability. May take single frame, rapid sequence or motion pictures.

NILEC-Guide-0301.00-74 Selection and Application Guide to Fixed Surveillance Cameras

Scope: Provides information on the types of fixed surveillance cameras available, and their application in combating retail crime.

CEGS 16751-90 Guide Specification for Closed Circuit Television Systems

Scope: Provides requirements for closed circuit television systems for use in preparing project specifications. Relies heavily on existing standards in providing a description of the system and its installation and maintenance.

14.0 SCREENING DEVICES

ASTM C1112-88 Guide for Application of Radiation Monitors to the Control and Physical Security of Special Nuclear Material

Scope: Describes the state-of-the-art of radiation monitors for detecting special nuclear material (SNM) in order to establish the context in which to write performance standards for the monitors. Provides information for selecting, calibrating, testing, and operating such radiation monitors when they are used for the control and protection of SNM.

ASTM F792-88 Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas

Scope: Covers the use of ionizing radiation imaging techniques for the detection of questionable items such as weapons and devices to trigger explosives, in order to determine their presence in hand-carried baggage, packages, checked or unaccompanied luggage, cargo, or mail screening points for controlling access to secure areas.

ASTM F947-90 Test Method for Determining Low-Level X-Radiation Sensitivity of Photographic Films

Scope: Method determines the maximum x-ray sensitivity coefficient of film/processing combinations for low quantities of x-ray exposure to silver halide photographic film. The coefficient can be used to assess the relative susceptibility of films to damage from x-ray exposure, such as that encountered in airport and similar security screening systems.

ASTM F1039-87 Test Method for Measurement of Low Level X-Radiation Used in X-Ray Security Screening Systems

Scope: Method establishes the procedures for measuring the ionizing radiation inside the radiation chamber of a low level X-ray security screening system.

NILECJ-STD-0601.00-74 Walk-Through Metals Detectors for Use in Weapons Detection

Scope: Provides performance requirements and test methods for walk-through metal detectors intended to indicate the presence of metal, in excess of a predetermined amount, carried on a person in a specific space.

NILECJ-STD-0602.00-74 Hand-Held Metal Detectors for Use in Weapons Detections

Scope: Provides performance requirements and method of tests for hand-held metal detectors used for determining the location of metal weapons carried on a person.

NILECJ-STD-0603.00-75 X-Ray Systems for Bomb Disarmament

Scope: Provides requirements and methods of test for portable x-ray systems for use in bomb disarming operations, but not for use in mass or routine screening of parcels or baggage.

USMS - 1-30-91 Specifications - Security X-Ray Screening Machines

Scope: Contains x-ray equipment requirements including maximum weight, allowable dimensions, resolution, penetration, film safety, type of detection system, operational mode, electrical power conditions, maintenance support, demonstration of satisfactory performance, installation and training, and warranty services.

USMS - 1-12-91 Specifications - Vehicle Mounted Mobile Security X-Ray Screening System

Scope: Covers requirements for vehicle and an auxiliary power unit, as well as x-ray screening equipment.

USMS - 1-20-91 Specifications - Walk-Through Metal Detector

Scope: Includes requirements for type of weapon to be detected, a self-diagnostic system, electrical power conditions, false alarms, weight, adjustments, life expectancy, warranty, etc. A separate testing protocol for the operational testing of walk-through metal detectors has also been issued (7-23-90).

15.0 SECURITY SEALS

ASTM F832-90 Classification for Security Seals

Scope: Covers categories of commercially available seals. Classification is based on their configuration and the material from which they are made. Types of seals are: Wire, Padlock, Strap, Cable, Bolt, Cinch or Pull-Up, Twist, Scored, and Label.

ASTM F946-85 Guide for Establishing Security Seal Control and Accountability Procedures

Scope: Covers procedures for maintaining a continuous line of accountability for security seals from the time of manufacture to destruction of the seal subsequent to its use.

ASTM F1157-90 Practice for Classifying the Relative Performance of the Physical Properties of Security Seals

Scope: Presents methods for testing the physical properties of security seals. The various tests include particular apparatus or procedural specifications required for different types of security seals.

16.0 ELECTRICAL

NFPA 110 - 85 Emergency and Standby Power System

Scope: Covers performance requirements for power systems providing an alternative source of electrical power to loads in buildings and facilities in the event that the normal power source fails. Includes power sources, transfer equipment, controls, supervisory equipment, and all related electrical and mechanical auxiliary and accessory equipment needed to supply electrical power to the load terminals of the transfer equipment. Also covers installation, maintenance, operation, and testing requirements as they pertain to performance of an emergency power supply system.

UL 924-85 Emergency Lighting and Power Equipment

Scope: Covers battery powered emergency lighting and power equipment for use in ordinary indoor locations in accordance with NEC. Such equipment is intended to supply automatically illumination or power or both to critical areas and equipment in the event of failure of the normal supply or in the event of accident to elements of a system intended to supply, distribute, and control power and illumination essential to safety of human life.

17.0 DATA TRANSMISSION

CEGS 16753-1989 Guide Specifications - Wireline Data Transmission Media (DTM) for Security Systems

Scope: Covers requirements for a half or full duplex wire line data transmission media for communication between a local device and a central processor. Provides a description of a system and its components, and installation and maintenance procedures.

CEGS 16754-1989 Guide Specifications - Fiber Optics Data Transmission Media (DTM) for Security Systems

Scope: Provides requirements for fiber optics data transmission media for analog or digital communications. Provides a description of a system and its components, and installation and maintenance procedures.

18.0 ECONOMICS

ASTM E833-85a Definitions of Terms Relating to Building Economics

Scope: Contains definitions relating to the economic evaluation of building construction as used in other standards under the jurisdiction of ASTM Committee E6 on Performance of Building Constructions.

ASTM E917-83 Practice for Measuring Life-Cycle Costs of Buildings and Building Systems

Scope: Establishes a procedure for evaluating the life-cycle costs (LCC) of buildings and building systems. Procedures for use of the LCC method are described step-by-step. The LCC method results in an economic evaluation that encompasses the net effect, over time, of designing, purchasing, leasing, constructing/installing, maintaining, operating, repairing, replacing, and disposing of buildings or building systems.

ASTM E964-83 Practice for Measuring Benefit-to-Cost and Savings-to-Investment Ratios for Buildings and Building Systems

Scope: Provides a recommended procedure for calculating and interpreting the benefit-to-cost ratio (BCR) and saving-to-investment ratio (SIR) of building designs and systems. The BCR and SIR are numerical ratios that indicate the economic value of a project by the size of the ratio.

ASTM E1057-85 Practice for Measuring Internal Rates of Return for Investments in Buildings and Building Systems

Scope: Establishes a procedure for calculating and interpreting internal rate-of-return's (IRR) for building designs and systems. The IRR provides the compound rate of interest that equates the stream of dollar benefits or savings to dollar costs over some defined study period.

ASTM E1074-85 Practice for Measuring Net Benefits for Investments in Buildings and Building Systems

Scope: Provides a recommended procedure for calculating and interpreting the net benefits (NB) method in the evaluation of building designs and systems. The NB method, sometimes called the net present value method, calculates the difference between discounted benefits (or savings) and discounted costs as a measure of the cost effectiveness of a project.

ASTM E1121-86 Practice for Measuring Payback for Investments in Buildings and Systems

Scope: Provides a recommended procedure for calculating and applying the payback method in evaluating building designs and building systems. The payback method accounts for all monetary values associated with an investment up to the time at which cumulative net benefits,discounted to present value, just pay off initial investment costs.

ASTM E1185-87 Guide for Selecting Economic Methods for Evaluating Investments in Buildings and Building Systems

Scope: Guide identifies types of building design and building system decisions that require economic analysis and recommends ASTM practices, adjuncts, and computer programs that may be used to implement the appropriate economic methods for each decision type.

ASTM E1369-90 Guide for Selecting Techniques for Treating Uncertainty and Risk in the Economic Evaluation of Buildings and Building Systems

Scope: Guide recommends techniques for treating uncertainty in input values to an economic analysis of a building investment project. Also recommends techniques for evaluating the risk that a project will have a less favorable economic outcome than what is desired or expected.

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4618

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
July 1991

4. TITLE AND SUBTITLE

Standards for the Physical Protection of National Resources and Facilities

5. AUTHOR(S)

Robert D. Dikkers

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER
IAA No. EMW-90-E-3279

8. TYPE OF REPORT AND PERIOD COVERED
Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

Federal Emergency Management Agency
Washington, DC 20472

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

In regard to a Federal Emergency Management Agency (FEMA) responsibility for the protection of essential resources and facilities, NIST conducted a study whose objectives are: (1) to identify and compile existing standards and guidelines pertaining to the protection of facilities and resources; and (2) to prepare a plan and strategies for developing national standards which may be needed to assist Federal departments and agencies in the protection of their facilities and resources.

A review of factors and considerations involved in the planning and design of physical protection for facilities and resources is discussed along with a description of physical security activities of selected Federal departments and agencies and non-government organizations. General information on standards and brief descriptions of 110 standards pertaining to physical security and protection are included in Appendices.

Recommendations are made for:(1) the conduct of a comprehensive study to identify and describe Federal agency physical security activities and resources information; and (2) the development of national voluntary standards which would cover the planning and design phases of the security engineering design process as well as various physical security equipment and systems.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

Assets; emergency preparedness; essential resources and facilities; Federal government; physical security; security engineering; standards; threats.

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
88

15. PRICE
A05

ELECTRONIC FORM