

PHYSICAL SECURITY HANDBOOK



**CIS HB 1400-02A
APRIL 2000**

DEPARTMENT OF THE TREASURY
U.S. CUSTOMS SERVICE
CUSTOMS ISSUANCE SYSTEM

U.S. CUSTOMS SERVICE
OFFICE OF INTERNAL AFFAIRS
SECURITY PROGRAMS DIVISION
SECURITY MANAGEMENT BRANCH

FOREWORD

This handbook supersedes CIS HB 1400-02, "Physical Security Handbook," dated August 1989.

As the U.S. Customs Service faces the challenges of the new millennium, each of us must take steps to ensure the safety and security of Customs personnel and resources. We must recognize potential vulnerabilities and take swift action to correct weaknesses. It is our duty to Customs and the public to maintain a security program that is both aggressive and cost-effective.

With this in mind, the "Physical Security Handbook" was developed as a tool to educate and guide managers in addressing physical security issues. The new handbook is written to incorporate recent advances in security design, materials and electronic monitoring devices. Our goal is continuous improvement. Security preparedness is not a static condition; it is a dynamic process that should never be taken for granted.



Assistant Commissioner
Office of Internal Affairs

Distribution: G-25 All Managers/Supervisors

TABLE OF CONTENTS

<u>PART</u>		<u>PAGE</u>
1	GENERAL PROVISIONS	4
1.1	PURPOSE	5
1.2	RESPONSIBILITIES	5
1.3	SCOPE	7
1.4	GENERAL	8
1.5	IMPLEMENTATION	8
1.6	INTERPRETATIONS, WAIVERS, EXCEPTIONS	8
2	PHYSICAL SECURITY – THE PROCESS	9
2.1	VULNERABILITY ASSESSMENT	10
2.2	THREAT IDENTIFICATION	10
2.3	LINKAGE OF THREAT TO CUSTOMS	10
2.4	VULNERABILITIES	11
2.5	PHYSICAL SECURITY INSPECTION REPORT	11
2.6	RISK PRIORITIZATION	11
2.7	SECURITY CONTINGENCY PLANS	12
2.8	SECURITY AWARENESS	12
3	FACILITY AND OFFICE SECURITY LEVELS	14
3.1	GENERAL	15
3.2	LEVEL I	15
3.3	LEVEL II	15
3.4	LEVEL III	15
3.5	FACILITY AND OFFICE - SECURITY LEVEL MATRIX	16
3.6	RESTRICTED AREAS	18
3.7	SECURED AREAS	18
4	CONSTRUCTION REQUIREMENTS	20
4.1	GENERAL	21
4.2	LEVEL I	21
4.3	LEVEL II	22
4.4	LEVEL III	24
4.5	RESTRICTED AREAS	26
4.6	SECURED AREAS	27
4.7	VAULTS/STORAGE ROOMS FOR PERMANENT STORAGE	29
4.8	SEIZED PROPERTY ROOMS FOR PERMANENT STORAGE	33
4.9	STRONG ROOMS FOR PERMANENT/ TEMPORARY STORAGE	34

4.10	SECURITY CONTAINERS AND SAFES FOR TEMPORARY STORAGE	35
4.11	SENSITIVE COMPARTMENTALIZED INFORMATION FACILITIES (SCIFs)	35
4.12	DETENTION CELLS (RESERVED)	36
4.13	CASHIER/TELLER AREAS	36
4.14	ADDITIONAL PHYSICAL SECURITY MEASURES	38
5	CLASSIFIED DOCUMENT PROTECTION	45
5.1	GENERAL	46
5.2	SECURITY DURING OFFICE MOVES	46
5.3	FREEDOM OF INFORMATION/PRIVACY ACTS	46
6	TECHNICAL STANDARDS	48
6.1	BOMB THREATS	49
6.2	PROTECTIVE LIGHTING	50
6.3	INTRUSION DETECTION SYSTEMS (IDS)	56
6.4	ACCESS CONTROL SYSTEMS	62
6.5	BALLISTIC RESISTANT PROTECTIVE MATERIAL/ NIJ STANDARD 0108.01	65
6.6	FENCES	67
6.7	CLOSED CIRCUIT TELEVISION (CCTV)	71
6.8	ACOUSTICAL CONTROL/SOUND MASKING TECHNIQUES	73
6.9	INSPECTIONS AND REPORTS	75
7	EXHIBITS	78
7.1	MAS-HAMILTON X07 LOCK	79
7.2	9-GAUGE EXPANDABLE METAL	80
7.3	GSA APPROVED CLASS V SECURITY CONTAINER (SAFE)	81
7.4	GSA APPROVED CLASS VI SECURITY CONTAINER (5 DRAWER SAFE)	82
7.5	PUSH TO EXIT BUTTON FOR ACCESS CONTROL SYSTEM	83
7.6	ELECTRIC STRIKE FOR ACCESS CONTROL SYSTEM	84
7.7	PROXIMITY CARD READER FOR ACCESS CONTROL SYSTEM	85
7.8	SAMPLE PROXIMITY CARDS	86
8	ACRONYMS	87

PART I
GENERAL PROVISIONS

1 GENERAL PROVISIONS

1.1 PURPOSE

This handbook establishes a nationwide security policy to guide management in implementing U.S. Customs Service policy. Customs officials and managers are responsible for ensuring the uninterrupted operation of the U.S. Customs Service by taking all reasonable actions to prevent disruption, disclosure, or property destruction at all facilities utilized by Customs. What follows are the physical security guidelines for information, property, and facilities that require more than normal protection against disclosure, loss, damage, or destruction. There are some Customs offices that are co-located within a facility that is not owned by Customs. To the extent possible, these offices should attempt to comply with these physical security provisions.

This handbook is being distributed to management personnel responsible for safeguarding the U.S. Customs Service system: employees, information, monies, equipment, seized property, and facilities. The Office of Internal Affairs, Security Programs Division, Security Management Branch (SMB) is responsible for determining the security level of new or redesigned facilities. The Logistics Division in Indianapolis is responsible to ensure that the assigned security levels are met in new or existing facility plans.

1.2 RESPONSIBILITIES

The Office of Internal Affairs is responsible for oversight, planning, developing, evaluating, and managing the Customs-wide Physical Security Program and is responsible for issuing policies and procedures pertaining to the program. The Assistant Commissioner, Office of Internal Affairs, has overall responsibility for oversight and compliance with the U.S. Customs Service Physical Security Program.

The Security Management Branch (SMB), within the Office of Internal Affairs, has responsibility for classified document security, security in Headquarters facilities, and all related physical security matters within the Customs service.

All Headquarters organizations are responsible for the proper protection of documents and information within their area of responsibility. In all matters of protection of documents and information, guidance and oversight is provided by the SMB. Access to Headquarters facilities will be governed by Customs Directive 099-1440-013, "Headquarters Building Access Control Passes," dated October 15, 1990, or superseding directives.

Office of Internal Affairs personnel and other designated personnel operating under the direction of Internal Affairs are to be afforded complete unannounced, unrecorded, and unescorted access to all Customs facilities, where not

prohibited by other agency requirements and directives (e.g., Sensitive Compartmented Information Facilities (SCIF), Communications Security account facilities (COMSEC) and Secure Message Centers). Keys and combinations to Customs facilities will be provided to the Office of Internal Affairs personnel upon request, where not prohibited by other agency requirements or directives.

Internal Affairs physical security specialists, who are co-located in the Regional Special Agent in Charge offices, implement the Physical Security Program in the field. Headquarters and regional physical security specialists are responsible for conducting periodic physical security inspections to ensure compliance with this handbook. Inspections may be announced or unannounced.

Each Director, Field Operations, Customs Management Center (CMC), Special Agents in Charge, Office of Investigations, and Regional Special Agents in Charge, Office of Internal Affairs, or senior Customs official on site is directly responsible for implementing and maintaining the security policies and standards of this handbook, and reviewing procedures to ensure compliance with requirements of this issuance.

Each Director, Field Operations, Special Agent in Charge, Office of Investigations, Regional Special Agent in Charge, Office of Internal Affairs, or senior Customs official on site, shall designate an employee(s) to be responsible for all physical security matters within their respective jurisdictions. The names are to be forwarded, in writing, to SMB.

The Logistics Division is responsible for notifying the SMB of changes in existing physical security and must provide all plans for prospective locations of new facilities, plans to upgrade security for existing facilities, and plans implementing physical security procedures in new facilities. The SMB is responsible for providing physical security requirements to the Logistics Division for incorporation into these plans.

The Special Agents in Charge, Office of Investigations, are responsible for responding to threats directed against Customs personnel and facilities by non-Customs personnel, and providing appropriate action to ensure the protection and safety of those personnel and/or facilities. The Office of Internal Affairs is responsible for investigating threats directed at Customs personnel and facilities by Customs employees. The SMB is responsible for conducting physical security inspections for all Customs facilities.

The Assistant Commissioner, Office of Information and Technology, is responsible for information security matters regarding the physical security environments of Automated Information Systems (AIS) that process Sensitive But Unclassified (SBU); Official Use Only (OUO); Limited Official Use (LOU); and Internal Affairs Sensitive Information (IASI). The National COMSEC Office provides policy, procedures and guidance for COMSEC related matters within

the Customs Service.

All Customs managers and employees are responsible for providing security for all information, documents, and property with which they are entrusted, complying with all security requirements as stipulated in this handbook, and for reporting any violations through proper channels to the SMB. All discrepancies with regard to the safeguarding of classified documents shall be immediately reported to the Office of Internal Affairs (reference Customs Handbook 1400-03, Safeguarding Classified Information).

Sensitive Compartmentalized Information (SCI) shall only be stored in accordance with the specifications and requirements of the Central Intelligence Agency and in a facility accredited by the Assistant to the Secretary (National Security), Department of the Treasury. The Intelligence Division, Office of Investigations is the only Customs organization authorized and accredited to receive and store SCI. The Commissioner of Customs must approve any requests for additional facilities for the storage of SCI with the concurrence of the Treasury Department. After this approval is obtained, the construction plans, funding requirements and site survey information must be provided, as soon as possible, to the Assistant Commissioner, Office of Internal Affairs, in order to approve the technical adequacy of the project, and determine if all applicable security specifications have been met. The requesting office will be responsible for ensuring that all construction requirements are met to achieve accreditation to operate.

COMSEC Physical Security requirements are governed by National Security Telecommunications and Information System Security Committee Instruction (NSTISSI) 4005 dated August 1997 titled "Safeguarding Communications Security (COMSEC) Facilities and Material" and promulgated by the National Security Agency.

The Assistant Commissioner, Office of Training is responsible for developing a security education program for all employees attending training at the Federal Law Enforcement Training Center, Glynco, GA.

1.3 SCOPE

The scope of this handbook provides physical security policy guidance for the entire U.S. Customs Service. It is intended to provide specific requirements for all Headquarters facilities, field offices, and Logistics Division personnel in the performance of their duties. For specialized facilities and operations, this handbook is designed to augment existing directives and handbooks. Therefore, the Customs Issuance System should be consulted for any additional details pertaining to specialized operations or facilities.

1.4 GENERAL

The U.S. Customs Service has the responsibility of providing reasonable protection commensurate with the character and value of the information or property involved. Large facilities may require armed guard service, a perimeter electronic intrusion detection system (IDS), and a perimeter fence to meet security needs, while a small post of duty may require less.

These guidelines are intended to provide standardized protection throughout the U.S. Customs Service; however, there may be special situations where modifications will be necessary in order to comply with these guidelines. Any modifications must be approved by the SMB. Suggestions for changes to this handbook are encouraged and should be submitted to the Office of Internal Affairs, Security Management Branch.

1.5 IMPLEMENTATION

If implementation of the security specifications outlined in this handbook requires equipment purchases or alterations to space, the priority and time frame for such expenditures will depend on both the availability of funds and consideration of requirements in other program areas. Security enhancements shall be given the highest priority possible to comply with the security policy of this handbook.

It is acknowledged that Customs facilities were designed and constructed based upon previous physical security guidelines. Customs facilities were not previously required to be designed and constructed to meet perimeter wall sound attenuation requirements. New construction of Customs facilities will be required to meet the sound attenuation requirement specified for a Level III facility (Part 4.4h). However, the highest priority shall be to maintain the integrity, safety and security of personnel, materials and information in existing facilities.

Storage of narcotics, weapons, currency, and other items of high value must meet the new requirements of Parts 4.6 through 4.10 of this handbook upon its issuance.

Other current U.S. Customs Service directives such as the U.S. Customs Firearms and Use of Force Policy, 4510-017, current version, and Customs Handbook 1400-03, Safeguarding Classified Information, should be consulted for further information on those specific subjects.

1.6 INTERPRETATIONS, WAIVERS AND EXCEPTIONS TO THIS HANDBOOK

All requests for interpretations, waivers, changes in requirements, and exceptions to the requirements of this handbook shall be forwarded in writing to the Assistant Commissioner, Office of Internal Affairs, U.S. Customs Service, 1300 Pennsylvania Avenue, Room 8.3A, Washington, D.C. 20229.

PART 2

PHYSICAL SECURITY – THE PROCESS

2 PHYSICAL SECURITY – THE PROCESS

2.1 VULNERABILITY ASSESSMENT

The physical security process begins with a vulnerability assessment. The vulnerability assessment consists of threat identification, linkage of the threat to Customs facilities, analyzing vulnerabilities to the threat identified, physical security required, review of existing protection, physical security inspection report, risk prioritization, cost of security, and security contingency plans. The senior Customs official at a particular facility is responsible for the threat identification, linkage of the threat to the Customs facility, analyzing the vulnerabilities to the threat identified, reviewing existing security protection, risk prioritization, local security contingency plans, and security awareness. The headquarters and regional physical security specialists are responsible for the production of the physical security inspection report and can be consulted for assistance with the vulnerability assessment. The elements of the vulnerability assessment are:

2.2 THREAT IDENTIFICATION

Have criminal or terrorist acts been committed in the area of the facility?

Do the acts committed relate to the facility?

Is there any intelligence on file relating to the potential for criminal or terrorist acts?

Are the activities occurring at the facility likely to draw the attention of criminals and/or terrorist organizations?

The general character of the external environment must be considered. A neighborhood with a high crime rate will require more extensive building security than a neighborhood with a low crime rate.

Continuous liaison with local police departments, intelligence units, and the Federal Bureau of Investigation (FBI) can provide pertinent information that will assist in identifying a specific threat. This is an Office of Investigations (OI) function, which should be handled through the servicing (OI) office.

2.3 LINKAGE OF THREAT TO CUSTOMS

Are the activities of the U.S. Customs Service likely to bring the facility to the attention of criminals and/or terrorist organizations?

Location within a geographic area where the U.S. Customs Service has a high enforcement profile is a factor. The type and value of equipment, complexity and

nature of operations, concentration of data, the consequences of any interruptions or loss (criticality), and whether the activity serves the public directly, or is strictly staff or supportive in nature, are all vital considerations directly relating to the degree of protection required. Facilities engaged in investigative/law enforcement functions or areas designated as "Secured Areas" in accordance with this handbook, will be expected to receive greater attention to physical security. Other considerations are whether the facility is temporary or permanent and the probability of expansion of operations. The nature of operations conducted by other tenants, if the building is not wholly occupied by Customs activities, will also affect proper planning.

2.4 VULNERABILITIES

A major consideration in establishing a security program for a particular activity is the building in which the activity is located and existing security measures. The number of floors, doors, windows, fire exits, the degree of ground level access and adjacent parking facilities will all have an effect on entry control problems. The material structure of the building, interior partitioning, ceiling and doors, will all affect the degree of security required to protect the public, employees and the contents of the facility.

The quantity and quality of police and fire protection afforded the immediate area should be determined. Emergency support from other than local police and fire departments, in the event of such occurrences as civil disorders, must also be considered. Vulnerability to terrorist attack and relative accessibility of the facility to disruptive elements must be addressed.

2.5 PHYSICAL SECURITY INSPECTION REPORT

Headquarters and regional physical security specialists will produce this report. This report is designed to provide the end user with the information necessary to adequately secure his/her facility (see Part 6.9).

2.6 RISK PRIORITIZATION

Risk prioritization is the concept which dictates that when there are limited resources available for protection, those areas most vulnerable must be given priority. For example, personnel safety must always be given priority, however, disregard for proper storage of seized narcotics may expose personnel to an even greater risk, if it appears vulnerable to those with a desire to obtain it through theft or force.

Security controls must never be relaxed to the point that controls for less valuable items are disregarded and accountability is lost.

2.7 SECURITY CONTINGENCY PLANS

Local directives should be written to cover all phases of security operations. They should be disseminated to all persons with a need-to-know and who are charged with security responsibilities. Such directives must provide instruction relative to the individual's security responsibility, authority, and the procedures for handling and reporting incidents. These directives must be kept current and reflect the routine needs of the facility as well as any unusual situation that requires special security measures.

In evaluating the need for and extent of Security Contingency Plans, the possibility of injury to personnel must be considered. This is especially relevant when addressing security measures taken during crisis situations (e.g., bomb threats, fires, terrorist incidents or natural catastrophes) to control government assets, to limit damage, to provide emergency services for containment of the incident and to restore activity to normal. Each Customs location must have a Continuity of Operations Plan (COOP) which will be utilized to restore operations after an event that has disrupted normal operations.

Situations that present unique and growing physical security problems include the handling of bomb threats and terrorist incidents. A Bomb Threat Contingency Plan must include:

Preventive measures to reduce the opportunities for the introduction of bombs; Procedures for evaluating and handling threatening messages; Policy on evacuation and safety of personnel; Procedures for obtaining assistance and support of local law enforcement and military bomb disposal units; and, Procedures in the event a bomb or suspect bomb is found on the premises and Procedures to be followed in the event of an explosion.

Part 6.1 of this handbook contains an Information Notice issued to all employees regarding the proper handling of Bomb Threats and the Bureau of Alcohol, Tobacco and Firearms pamphlet, "Bomb Threats and Physical Security Planning" which provides guidance on this subject.

2.8 SECURITY AWARENESS

The senior Customs official on site, or his/her designee, is responsible for the conduct of a physical security awareness program. The overall security effort will be ineffective unless all employees are aware of security requirements. The regional physical security specialist can provide guidance in this area. The following are methods of disseminating security information:

Special security bulletin boards can be installed throughout the facility on which are posted new security regulations;

Security articles can be published in the employee newspaper and/or in electronic media (internet web site), if these resources are available;

Pertinent articles that appear in the technical and popular press can be routed to members of the management staff: and,

Security posters are effective if the message is short, simple, and educational.

There are a number of training tools available for security orientations such as films, audiocassettes, round table discussions, lectures, programmed instructions, and seminars. SMB should be consulted regarding the availability of these items.

PART 3

FACILITY AND OFFICE SECURITY LEVELS

3 FACILITY AND OFFICE SECURITY LEVELS

3.1 GENERAL

SMB, based on the criteria listed below, determines the proper security classification level for all Customs facilities.

There are three security levels assigned to U. S. Custom's facilities; Levels I, II and III. Level I represents the minimum-security level, Level II represents medium security, and Level III represents the maximum security afforded to Customs facilities.

For the purposes of this handbook, all U. S. Customs facilities are defined as one of the following: Non-Border offices, Border offices, and Investigative/Law Enforcement offices. These definitions are not intended to be strictly adhered to. The location, function, and responsibilities associated with a particular facility may require that the level of security be adjusted. Additionally, specialized circumstances such as restricted or secured areas may dictate that requirements are greater or less than those indicated for that level. Changes in requirements may be authorized with the approval of the SMB.

Remote, sparsely staffed border facilities not routinely processing large numbers of people, vehicles, cargo, etc. will be afforded appropriate security based on vulnerability and assets to be protected. Situations such as this will require an exception to this section and should be addressed in accordance with Part 1.6 of this handbook.

3.2 LEVEL I (Minimum-security level)

Level I facilities typically include, but are not limited to Non-Border offices, Customs Houses, and Port Director's offices. Depending on the particular office's functions and responsibilities and the results of vulnerability assessments, these sites could be classified as Level II or Level III.

3.3 LEVEL II (Medium-security level)

Level II facilities typically include, but are not limited to Border-Crossing stations, Area Director's offices, Federal Inspection Service (FIS) areas, International Airports, and Cargo Inspection Facilities (Sea, Air, Land and Rail). Depending on the particular office's functions and responsibilities, these sites could be classified as Level III.

3.4 LEVEL III (Maximum-security level)

Level III facilities typically include, but are not limited to, offices that perform investigative/law enforcement functions, intelligence gathering activities, and

air/marine activities. Examples include: Special Agents In Charge offices, Office of Investigations; Regional Special Agents in Charge offices, Office of Internal Affairs; Resident Agent in Charge offices of the Office of Investigations and the Office of Internal Affairs; Customs Management Centers (CMC's); Customs Offices of Laboratories and Scientific Services (LABS); Aviation Branches and Units; Customs Data Centers; and, the National Law Enforcement Communications Center (NLECC).

NOTE: ANY LEVEL I, II, OR III FACILITY MAY HOUSE A TEMPORARY OR PERMANENT STORAGE VAULT, PROVIDED THE TEMPORARY OR PERMANENT STORAGE VAULT MEETS THE CONSTRUCTION STANDARDS AS DESCRIBED IN PARTS 4.7-4.10 OF THIS HANBOOK.

3.5 FACILITY AND OFFICE - SECURITY LEVEL MATRIX

The following matrix is a general guide for security levels for Customs facilities. This matrix does not contain all of the different Customs operations and facility types. Questions about Customs operations not listed can be addressed to the SMB or to regional physical security specialists

FACILITY AND OFFICE SECURITY LEVEL MATRIX – EXAMPLES

Facility	Level I	Level II	Level III
Customs Management Center *	X		
Strategic Trade Center/Reg. Audit *	X		
Area/Port Directors *		X	
Border Crossing Stations		X	
International Airports		X	
Inspection Stations		X	
Cargo Inspection Stations		X	
Mail Inspection Facility		X	
Service Headquarters			X
COMSEC Facilities and Offices			X
Financial Management Services Center			X
Customs Attaches **			X
Senior Customs Representatives **			X
Special Agents In Charge (OI)			X
Regional Special Agents In Charge (IA)			X
Counsel's Office			X
National Firearms Program Staff ***			X
Training Centers (Glynco) ***			X
Canine Enforcement Training Center***			X
National Aviation Center ***			X
Aviation Branches and Units***			X
Aviation Surveillance & Operations Branches ***			X
Air and Marine Int. Coord. Center***			X
P-3 Special Operations/Airborne Early Warning Branches ***			X
Electronics Maintenance Facility			X
NLECC/Orlando			X
Customs Data Centers			X
Technical Intelligence Branch (ERIN)			X
Interdiction Intelligence Branch (C3I)			X
El Paso Intelligence Center (EPIC)			X
Resident Agent in Charge (OI)			X
Resident Agent in Charge (IA)			X
Offices of Laboratories and Scientific Services (Labs)			X

* Depending on office functions and responsibilities, presence of a seizure vault and/or secured area, these sites could be classified at a Level II or III.

** Facilities subject to Department of State requirements.

*** Facilities may be located on Military bases and subject to DOD specifications.

3.6 RESTRICTED AREAS

A restricted area is a facility, area or room, to which access is restricted to authorized personnel only. The senior Customs official on site will determine the use of restricted areas. The use of restricted areas is an effective method of controlling movement of individuals, and eliminating unnecessary traffic through critical areas. Restricted areas decrease the opportunity for unauthorized disclosure of information or removal of property.

3.7 SECURED AREAS

A secured area is a specialized building, area or room that lies within a restricted area. A secured area can be an entire building that lies within a fenced-in perimeter. Examples of secured areas include, but are not limited to:

- a. Law enforcement data centers
- b. Narcotics storage areas
- c. Seized property storage areas
- d. Evidence rooms
- e. Centralized Examination Stations (CESs)
- f. Intelligence offices
- g. Communications centers
- h. Sensitive Compartmentalized Information Facilities
- i. Air/Marine operations centers
- j. Any area where sensitive or classified discussions take place on a regular basis
- k. Mail facilities/Mail rooms
- l. Federal Inspection Service (FIS) Areas
- m. Vaults/storage rooms (Technical equipment/Weapons/Ammunition)
- n. Express Consignment Operation facilities
- o. Customs Offices of Laboratories and Scientific Services (Labs)

- p. Cashiers/teller cages
- q. General Order (G.O.) storage areas
- r. Local Area Network (LAN) rooms
- s. Telephone switch rooms
- t. Other areas as identified by management

These secured area examples are not all-inclusive and do not suggest that a particular facility must be in a certain level. The physical security level of a particular facility will be determined by the SMB, at the time of new construction or renovation. Changes in the security level of the facility will be determined on a case-by-case basis by the SMB. Coordination between the SMB, Logistics Division, and the senior Customs official on site will be necessary to ensure that the proper security level is assigned to the individual facility.

Certain highly specialized facilities/areas may require additional security construction enhancements. Examples of specialized facilities/areas include, but are not limited to: seizure vaults, detention cells, LAB's, K9 Training Aid Storage Areas, and SCIF's.

PART 4
CONSTRUCTION REQUIREMENTS

4 CONSTRUCTION REQUIREMENTS

4.1 GENERAL

This section of the handbook outlines the construction requirements for Security Level I, II and III facilities. In addition, specific areas such as restricted areas, secured areas, vaults/storage rooms, strong rooms, SCIF's, detention cells, classified document storage rooms/containers, and teller operations are described in this section.

4.2 LEVEL I

Level I facilities typically include, but are not limited to Non-Border offices, Customhouses, and Port Director's offices. Depending on the particular office's functions and responsibilities, these sites could be classified as Level II.

- (a) Perimeter walls shall be constructed slab to slab.

The perimeter walls construction must be of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other opaque materials offering resistance to, and evidence of unauthorized entry into the area. If insert type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. Wall construction must extend from "true floor to true ceiling". When walls extend to a suspended (false) ceiling, the area above the suspended (false) ceiling must be secured by either 9-gauge expanded metal or by volumetric motion detectors connected to a Class A Central Monitoring Station. The expanded metal shall be in a 1-½ inches by 2 inches diamond pattern. If 9-gauge expanded metal is used it must be secured in such a manner that removal will show evidence of tampering. This expanded metal can only be utilized when sound attenuation (soundproofing) is not an issue for the respective Customs facility.

- (b) Perimeter doors must be 1-3/4 inches thick and constructed of solid wood or 12-gauge steel clad, hollow core metal door. Door frames must be constructed of equal strength as that of the door. All exterior perimeter doors must be equipped with deadbolt locks equipped with a manipulation resistant cylinder (e.g., brand name MEDECO or equivalent). Keys must be off the building master (i.e. not keyed like any other tenant's key) in facilities that are not solely occupied by Customs. Coordination must be made with the local fire marshal before construction to determine compliance with building codes associated with National Fire and Safety Association 101 (NFPA 101).

The deadbolts must have at least a 1-inch throw. Lock hardware placed on wood doorframes must be secured with stainless steel screws at least

3-inches long. Double doors must have at least one door secured from the inside with sliding deadbolts (e.g., Sargent and Greenleaf, model SM181) at the top and the bottom. Astragals (overlapping molding, preferably metal) must be used to inhibit access to lock bolts. Perimeter door hinge pins must be non-removable (peened, pinned, or spotwelded) or installed inside the room.

- (c) Windows must contain locks that are not susceptible to manipulation from the exterior. The lock must be of a type that requires the user to throw a bolt or latch or to slide a handle to lock or unlock the window. Spring-loaded latches are not acceptable. During non-duty hours, the windows must be closed and securely fastened.
- (d) An Intrusion Detection System (IDS) is not mandatory in a Level I facility unless there is a secured area located inside that facility. A secured area at a Level I facility may include but is not limited to government owned weapons and ammunition storage rooms. If a secured area is located inside the Level I facility, the entire site must have an IDS and the secured area must be a separate zone within the IDS. The IDS must be connected to a Class A Central Monitoring Station. There must be a backup method of communication set up with the Central Station, e.g. a wireless phone link (such as cellular) or an extra analog/digital telephone line so that if a telephone line is cut or otherwise interrupted, an alarm is activated at the Central Monitoring Station. Acknowledgement of an alarm condition by the Central Monitoring Station must take place within 30 seconds of the alarm. The Central Monitoring Station must dispatch the correct response (law enforcement, duty agent, etc.) For additional information regarding IDS, please see Part 6.3.
- (e) All technical equipment rooms, seized property rooms and government owned firearm storage rooms will meet the requirements of a Secured Area as defined in Part 3.7 of this handbook.

4.3 LEVEL II

Level II facilities typically include, but are not limited to Border-Crossing stations, Area Director's offices, Federal Inspection Service (FIS) areas, International Airports and Cargo Inspection Facilities (Sea, Air, Land, and Rail). Depending on the particular office's functions and responsibilities, these sites could be classified as Level III.

- (a) Perimeter walls shall be constructed slab to slab.

The perimeter walls construction must be of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other opaque materials offering resistance to, and evidence of unauthorized entry into the area. If

insert type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. Wall construction must extend from "true floor to true ceiling". When walls extend to a suspended (false) ceiling, the area above the suspended (false) ceiling must be secured by 9-gauge expanded metal. The 9-gauge expanded metal must be secured in such a manner that removal will show evidence of tampering. The expanded metal shall be in a 1-1/2 inches by 2 inches diamond pattern. The use of above wall volumetric motion detectors connected to a Class A Central Monitoring Station is not permitted in a Level II facility. When sound attenuation is an issue for a facility, the 9-gauge expanded metal will have to be augmented with other building materials to ensure an approved Sound Transmittal Class (STC) rating.

- (b) Perimeter doors must be 1-3/4 inches thick and constructed of solid wood or 12-gauge steel clad, hollow core metal door. Door frames must be constructed of equal strength as that of the door. All exterior perimeter doors must be equipped with dead bolt locks equipped with a manipulation resistant cylinder (e.g., brand name MEDECO or equivalent). Keys must be "off the building master" (not keyed like any other tenant's keys) in facilities that are not solely occupied by Customs. Coordination must be made with the local fire marshal before construction to determine compliance with building code(s) associated with National Fire and Safety Association 101 (NFPA 101).

The deadbolt locks must have at least a 1-inch throw. Lock hardware placed on wood doorframes must be secured with stainless steel screws at least 3-inches long. Double doors must have at least one door secured from the inside with sliding deadbolts (e.g., Sargent and Greenleaf, model SM181) at the top and the bottom. Astragals (overlapping molding, preferably metal) must be used to inhibit access to lock bolts. Perimeter door hinge pins must be nonremovable (peened, pinned, or spotwelded) or installed inside the room.

- (c) Windows must contain locks that are not susceptible to manipulation from the exterior. The lock must be of a type that requires the user to throw a bolt or latch or to slide a handle to lock or unlock the window. Spring-loaded latches are not acceptable. During non-duty hours, the windows must be closed and securely fastened.

Where there are Customs occupied office spaces on the first floor of a Level II facility and there are 96 square inches or greater of expansive glass exposed to the perimeter, glass breakage detectors must be installed in conjunction with a perimeter Intrusion Detection System (IDS) connected to a Class A Central Monitoring Station.

- (d) Intrusion Detection System (IDS). The exterior perimeter doors, walls and ceilings must have an IDS, and this IDS must be connected to a Class A Central Monitoring Station. There must be a backup method of communication set up with the Central Monitoring Station, e.g. a wireless phone link (such as cellular) or an extra analog/digital telephone line so that if a telephone line is cut or otherwise interrupted, an alarm is activated at the monitoring company. Acknowledgement of an alarm condition by the Central Monitoring Station must take place within 30 seconds of the alarm. The Central Monitoring Station must dispatch the correct response (law enforcement, duty agent, etc.). For additional information regarding IDS, please see Part 6.3.
- (e) All technical equipment rooms, seized property rooms and government owned firearms storage rooms will meet the requirements of a Secured Area as described in Part 4.6 of this handbook.

4.4 LEVEL III

Level III facilities typically include, but are not limited to offices that perform investigative/law enforcement functions, intelligence gathering activities, and air/marine activities. Examples include: Special Agents In Charge, Office of Investigations; Regional Special Agents in Charge offices, Office of Internal Affairs; Resident Agent in Charge offices of the Office of Investigations and the Office of Internal Affairs; Director, Field Operations offices; Customs Offices of Laboratories and Scientific Services (LABS); NLECC; and, the U.S. Customs Technical Intelligence Branch (ERIN).

- (a) All perimeter walls will be constructed slab to slab. Walls will be constructed of solid materials such as concrete, brick, metal, gypsum board, wood, or other materials offering protection against unauthorized entry into the area. If other than concrete or brick materials are used, 9-gauge expanded metal must be affixed to the interior of the walls. The expanded metal shall be in a 1-1/2 inches by 2 inches diamond pattern. A method shall be devised to prevent the removal of the expandable metal without leaving visual evidence of tampering. When walls extend only to a suspended (false) ceiling, the area above the suspended (false) ceiling must be secured by the use of 9-gauge expanded metal (in a diamond pattern as described above), secured in such a manner that removal will show evidence of tampering.
- (b) Perimeter doors (other than the main entrance door) must be 1-3/4 inches thick and constructed of solid wood or 12-gauge steel clad, hollow core metal door. Doorframes must be constructed of equal strength as that of the door. All exterior perimeter doors must be equipped with dead bolt locks equipped with manipulation resistant cylinder (e.g., brand name MEDECO or equivalent). Keys must be off the building master in facilities

that are not solely occupied by Customs. Coordination must be made with the local fire marshal before construction, to determine compliance with building code(s) associated with National Fire and Safety Association 101 (NFPA 101).

The deadbolts must have at least a 1-inch throw. Lock hardware placed on wood doorframes must be secured with stainless steel screws at least 3-inches long. Double doors must have at least one door secured from the inside with sliding deadbolts (e.g., Sargent and Greenleaf, model SM181) at the top and the bottom. Astragals (overlapping molding, preferably metal) must be used to inhibit access to lock bolts.

Perimeter door hinge pins that are located outside the office area must be non-removable (peened, pinned, or spot welded). All perimeter doors must have a door closer and astragal (metal plate on the outside of the locking mechanism to prevent tampering).

- (c) Windows must contain locks that are not susceptible to manipulation from the exterior. The lock must be of a type that requires the user to throw a bolt or latch or to slide a handle to lock or unlock the window. Spring-loaded latches are not acceptable. During non-duty hours, the windows must be closed and securely fastened.

Where there are Customs occupied office spaces on the first floor of a Level III facility, and there is 96 square inches or greater of expansive glass exposed to the perimeter, glass breakage detectors must be installed as an element of the Intrusion Detection System (IDS).

- (d) Intrusion Detection System (IDS). The perimeter and specialized areas within the site must have an IDS and the IDS will be connected to a Class A Central Monitoring Station. There must be a backup method of communication set up with the Central Monitoring Station, e.g. a wireless phone link (such as cellular) or an extra analog/digital telephone line so that if a telephone line is cut or otherwise interrupted, an alarm is activated at the Central Monitoring Station. Acknowledgement of an alarm condition by the Central Monitoring Station must take place within 30 seconds of the alarm. The Central Monitoring Station must dispatch the correct response (law enforcement, duty agent, etc.). For additional information on IDS, please refer to Part 6.3 of this handbook.
- (e) All technical equipment rooms, evidence rooms, and government owned firearm storage rooms will meet the requirements of a secured area, as defined in Part 4.6 of this handbook.
- (f) Closed Circuit Television (CCTV). All Level III facilities will use CCTV. At a minimum, CCTV will monitor the perimeter entrances and reception

areas. T-160 SVHS tapes or greater will be used to record CCTV images. CCTV images must be retrievable and operable over weekends and holidays. For more information, please refer to Part 6.7 of this handbook.

- (g) All Level III facilities must have a secure reception area. Reception areas must be protected to National Institute of Justice (NIJ) type III ballistic resistant standards, as described in Part 6.5 of this handbook, including all doors, windows, and transaction trays.
- (h) Sound Attenuation. Perimeter walls, ceilings and floors of the entire office space will have a Sound Transmission Class (STC) rating of 45, or better. The interview room will have an STC rating of 45. Individual offices will have a minimum STC rating of 40. The 9 gauge expanded metal used above the perimeter and other walls will have to be augmented with other building materials to ensure an approved STC rating. Certain facilities may require more stringent STC levels. This determination will be made during the vulnerability assessment. For more information regarding sound attenuation, please refer to Part 6.8 of this handbook.

4.5 RESTRICTED AREAS

A restricted area is a facility, area or room to which access is restricted to authorized personnel only. The senior Customs official on site will determine the use of restricted areas. Restricted areas are effective methods of controlling movement of individuals and eliminating unnecessary traffic through critical areas, thereby decreasing the opportunity for unauthorized disclosure of information or removal of property.

Facilities/areas/rooms designated as restricted areas must be prominently posted with signs indicating such, and must also be marked with names and telephone numbers of responsible personnel to be contacted if the room is found open. These signs must be bilingual in appropriate locations on the northern and southern borders.

Fenced areas should have gate areas posted with signs 3 feet by 3 feet with lettering of contrasting color to the background and at least 1-inch high and ½ - inch wide. At intervals of about 30-feet, signs bearing the following must be posted on fences:

**WARNING
RESTRICTED AREA - KEEP OUT
AUTHORIZED PERSONNEL ONLY**

IT IS UNLAWFUL TO ENTER THIS AREA WITHOUT PERMISSION OF THE UNITED STATES CUSTOMS SERVICE. ALL PACKAGES, BRIEFCASES, AND OTHER CONTAINERS BROUGHT INTO OR BEING REMOVED FROM THIS AREA ARE

SUBJECT TO INSPECTION (41 CFR 101-20.301). ALL PERSONNEL AND PROPERTY UNDER THEIR CONTROL WITHIN THIS RESTRICTED AREA MAY BE SUBJECT TO SEARCH [INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 USC 797 (1976)].

Restricted Areas shall be separated from non-restricted areas by physical barriers that will control access. Floor to ceiling partitions, bank-type partitions, portable dividers and screens, rows of file cabinets or similar barriers may suffice for this purpose, dependent upon the nature of the operation. **Ropes and stanchions are not acceptable.**

The number of entrances will be kept to a minimum and each entrance must be controlled. Adequate control will be provided by locating the desk of a supervisor or other responsible employee at the entrance to assure that only authorized persons enter. Where feasible, counters may be installed to provide service to employees who need not actually enter the area.

Most Restricted Areas will be expected to meet Secured Area requirements of this handbook, unless it can be shown that this is unnecessary or not possible. However, in no case will the type of construction used reduce the degree of protection required of items within the area. The Headquarters and Regional Physical Security Specialists shall be advised of all Restricted Areas not meeting Secured Area requirements.

Use of a Restricted Area register for sign-in/sign-out will be at the discretion of management based on local conditions. Such conditions will include size of the area, number of required entrances, physical configuration, number of visits by persons not normally assigned, and the location in relation to other work areas.

If management determines a restricted area register must be maintained, it will be located at each entrance of each restricted area determined to require it. Each person entering who is not assigned to the area will fill out the register in ink. The entry control person will verify the name and signature and will note the time of entry and departure. The supervisor responsible for the area will determine criteria for entry authorization. A prepared list of those with access may be necessary.

4.6 SECURED AREAS

A secured area is a specialized building, area or room that lies within a restricted area. A secured area can be an entire building that lies within a fenced-in perimeter.

a. WALLS

(1) Construction shall be slab to slab. Walls will be constructed of poured in

place, concrete tilt-up walls; cinder block; brick or steel. Gypsum board walls, 5/8-inches thick, may be utilized, provided that they are fitted with 9-gauge expanded metal affixed to the wall studs. The expanded metal shall be in a 1-1/2 inches by 2 inches diamond pattern.

b. DOORS/LOCKS

- (1) Perimeter doors must be 1-3/4 inches thick and constructed of solid wood or 12-gauge steel clad, hollow core metal door. Doorframes shall be of appropriate strength. The perimeter doors should be equipped with a deadbolt lock with manipulation resistant cylinders (e.g., brand name MEDECO or equivalent). Keys must be "off master" in buildings shared with other entities. Coordination must be made with the local fire marshal before construction, to determine compliance with building code(s) associated with National Fire and Safety Association 101 (NFPA 101). The deadbolt should have a minimum 1-inch throw. Lock hardware placed on wood doorframes must be secured with stainless steel screws at least 3-inches long.
- (2) Double doors should have at least one door secured from the inside with sliding deadbolts (e.g. Sargent and Greenleaf model SM181) at the bottom and top. Astragals (overlapping molding, preferably metal) should be used to inhibit access to lock bolts.
- (3) Door hinge pins must be non-removable (peened, pinned, or spot welded) or installed inside the room. All perimeter doors must have door closers.
- (4) To facilitate daily operations, an access control device or system may be utilized. Examples such as mechanical pushbutton locks, electronic push button locks, digital touch pads with key override and proximity card readers may be utilized to augment the deadbolt lock. During non-working hours, the deadbolt lock will be engaged.

c. WINDOWS

- (1) Windows will be non-removable double pane and sealed. Window must have locks that are not susceptible to manipulation from the exterior. The lock must be of a type that requires the user to throw a bolt or latch, or to slide a handle to lock or unlock the window. Spring-loaded latches are not acceptable. During non-duty hours the windows must be closed and securely fastened. Glass break detectors covering the windows shall be an integral element of the IDS.

d. CEILINGS

- (1) Construction shall be concrete slab or 9-gauge expanded metal. The

expanded metal shall be in a 1-1/2 inches by 2 inches diamond pattern.

e. INTRUSION DETECTION SYSTEM (IDS)

- (1) A Secured Area must have an Intrusion Detection System linked to a Class A Central Monitoring Station. If the office or building has an IDS, the Secured Area IDS may be linked to that IDS, as a separate zone (see Part 6.3).

f. OPENINGS IN SECURED AREAS

- (1) Openings in any part of a secured area are not permitted unless they are protected from entry. If the opening is in excess of 96 square inches, ½-inch steel bars must be installed in the opening in a manner to prevent unauthorized entry.

PARTS 4.7- 4.10 PERTAIN TO THE PERMANENT OR TEMPORARY STORAGE OF SEIZED DRUGS (NARCOTICS/CONTROLLED SUBSTANCES), WEAPONS, AMMUNITION, AND OTHER HIGH VALUE ITEMS. TEMPORARY STORAGE REFERS TO STORAGE OF 72 HOURS OR LESS, AND PERMANENT STORAGE REFERS TO STORAGE OF MORE THAN 72 HOURS.

4.7 VAULTS AND STORAGE ROOMS FOR PERMANENT STORAGE

A permanent vault must be either constructed or modular, in compliance with Parts 4.7a and 4.7b, below.

a. Vaults for Permanent Storage

This section specifies the standards for the construction of vaults and seized property rooms used as permanent storage facilities. These standards apply to all new construction, reconstruction, alterations, modifications, and repairs to existing vaults. All permanent storage vaults must have an Intrusion Detection System (IDS) (see Part 6.3), an Access Control System (ACS) (see Part 6.4), and a Closed Circuit Television System (CCTV) (see Part 6.7).

(1) Floors, Walls and Ceilings (New Construction)

The construction will consist of reinforced concrete with a minimum thickness of 8-inches. The concrete mixture will have a minimum compressive strength of at least 3000-psi at 28 days curing. Reinforcing will be accomplished with 2 grids of #5 Rebar, a minimum of 5/8-inch diameter, positioned centrally in the concrete pour and spaced horizontally and vertically 6-inches on center. The bars will be tied together in the contiguous walls and firmly anchored in the floor and

ceiling.

If concrete can not be poured due to location, space parameters, or other similar compelling reasons, the walls shall be constructed of 8-inch concrete blocks (cinder block is **not** acceptable). The concrete blocks shall be reinforced with #6 Rebar set vertically, 6-inches on center. The holes in the blocks through which the Rebar is set must be completely filled with concrete so that the Rebar is firmly anchored.

(2) Floors, Walls and Ceilings (Existing Structures)

Existing floors, walls and ceilings not meeting the standards of new construction (minimum thickness of 8-inches) can be modified by the addition of steel plating, a minimum of ¼-inch thick. The steel plates are to be welded at 6-inches on center, vertically and horizontally, with 1-inch welds to supporting steel members of a minimum thickness equal to that of the plate. If the supporting members are to be placed in a contiguous floor and ceiling of reinforced concrete, they must be either firmly anchored to and/or embedded into the floor and ceiling. If the floor and/or ceiling construction contains less than 8-inches of reinforced concrete, then a steel liner, a minimum ¼-inch thick, must be installed on the inside floor and/or ceiling. If existing construction is less than 8-inches of reinforced concrete, equivalencies can be attained through the waiver process. Please see Part 1.6 of this handbook.

(3) Vault Doors

The vault shall be equipped with a GSA approved Class V single or double leaf metal door, e.g. Overly, Mosler, or Hamilton.

(4) Vault Lock

The vault shall be equipped with a MAS-Hamilton X-07 combination lock, or like upgrade.

(5) Emergency Exit

Vaults will not contain an emergency exit unless mandated by local fire code(s).

If it is determined that a second means of egress is required, it shall consist of an approved Department of State (DOS) 15 minute Forced Entry (FE) resistance emergency exit door, e.g. Norshield NS1400-S.

(6) **Exit Hardware**

If the emergency exit door is mandated (see (5) above), it shall contain a high security exit panic device, e.g. Von Duprin Model EE99EO, D-Tex panic emergency exit device. The door shall not contain any exterior hardware.

(7) **Vault Vestibule**

A vestibule is required in a vault when access to the vault or secured area is in public view. If a vault contains a vestibule, the entrance portal shall contain a 12-gauge hollow metal door and frame. The door shall be equipped with a tamper resistant MEDECO D-11 (or equivalent) deadbolt and keyed lock set.

At large vaults, an overhead door leading from the vestibule to the exterior may be installed.

Overhead doors will be the roll up, flush fitting type. The door will be metal, dual slat manufactured with 12, 14, or 16-gauge exterior slats and 18, 20, 22, or 24-gauge interior slats with insulated centers. The doors are to be factory fitted with a slide bolt that can be extended through each of the metal slide rails. Each slide bolt will be fitted to the door within 6-inches of the floor and designed to accommodate the use of a high security padlock. A dealer after-market, manufacturer approved slide bolt locking system will be acceptable. The doors will be fitted with the appropriate electric motor system supplied by the manufacturer. The motor system shall have a manual override feature in the event the motor fails. Chains used to operate the door manually shall be of such a length that the door can be easily operated from the floor. An eyebolt will be affixed into the concrete in the area of the chain to allow the use of a high security padlock as an additional security feature. The electric control buttons and the manual override feature will be located so that they cannot be reached by cutting a hole through the door.

(8) **Storage Rooms within a Vault**

When the vault is segmented into separate storage areas, each storage area will have a separate zone on the IDS. Additionally, there will be sufficient CCTV coverage for each storage area (e.g. in the aisles between shelving). CCTV coverage will depend on the configuration and layout of the vault. SMB can be consulted for CCTV specifications.

(9) **Vault Openings (ventilation ducts, wire runs, etc.)**

Openings in any part of a permanent storage vault are not permitted

unless they are protected from entry. If the opening is in excess of 96 square inches, steel bars (Rebars) must be installed in 2 directions forming a grid. The bars must be #5 Rebar and configured so that their centers are 6-inches apart in each direction when concrete is used. The bars must be #6 Rebar and configured so that their centers are 8-inches apart vertically when masonry is used.

If the opening is to contain ducts, piping and/or wiring conduits, they shall pass through snug fitting sleeves at the time of construction. If the opening contains a duct in excess of 96 square inches, the Rebar described above must be installed. All minor openings between pipes, conduit, ducts and sleeves shall be caulked.

(10) Windows

(New construction)

No newly constructed vaults shall have windows in the interior vault area. However, vault vestibule areas may have windows on exterior walls. If a vault location has a vestibule with a window on an exterior wall, it shall be of a ballistic resistant material rated at National Institute of Justice type III or greater, and measures shall be taken to prevent visual surveillance of the activities within the facility. A steel barred frame consisting of number 5 Rebar (5/8-inch diameter) formed steel, located on 6-inch horizontal rows, shall be mounted to the frame and anchored on the window's interior side.

(Existing Construction)

Existing windows shall contain a steel barred frame.

(11) Exterior Lighting

All vaults (permanent, modular, and temporary) shall be illuminated sufficiently on the exterior to deter unauthorized entry and illegal activity. Adequate lighting shall be maintained during non-operating hours to insure adequate luminance for CCTV monitoring, or infrared/motion sensor cameras will be used. For further details, see Part 6.2.

(12) Closed Circuit Television (CCTV) (see Part 6.7 for additional information)

CCTV cameras will cover the entire vault to include: all vault/vestibule entrances, vault/vestibule interiors, security cages, storage rooms within a vault, and the vault exterior area. The facility's responsible official shall determine the exact camera location(s) with recommendations made by the SMB, Regional Physical Security Specialist, or vendor. The CCTV

system shall be linked to a video recorder and the location of the recorder shall be determined by the Port Director. Recorded videotapes shall be maintained for a minimum 30 days after the date of the last recording, before being reused.

(13) Fences

Stand-alone vault facilities must be secured with a perimeter fence. The perimeter fence must meet or exceed the specifications included in Part 6.6 of this handbook. At no time shall a perimeter wall of a facility be substituted for a complete perimeter fence. The perimeter fence should be located 30-feet away from the vault, when possible.

b. Modular Vaults

Modular vaults shall be used to meet special requirements, i.e. short installation time, space, weight requirements and under special circumstances, in the absence of a permanent vault. Modular vaults shall meet the Underwriters Laboratories (UL) standard 608 for class M, 15 minute forced entry, and the walls; ceilings and floors shall meet the construction standards of a permanent vault.

4.8 SEIZED PROPERTY ROOMS FOR PERMANENT STORAGE

Seized Property Rooms: All permanent seized property storage rooms must have an IDS, an Access Control System, and CCTV monitoring. Please refer to Parts 6.3, 6.4, and 6.7 of this handbook. The following standards apply to all permanent seized property rooms located within Customs facilities:

a. Seized Property Rooms

(1) Seized Property Rooms must meet the standards of a secured area. Perimeter walls shall be constructed slab to slab and be constructed of masonry block, brick, or Gypsum partitioning with 1 layer of 5/8-inch Gypsum board on each side of the stud and 1 layer of 9-gauge expanded metal on the inside of the area. The expanded metal shall be in a 1-1/2 inches by 2-inches diamond pattern. The expanded metal will be attached to metal supports and spot welded at 6-inch intervals. If wood supports are used to attach the expanded metal, the support shall be no less than 2-inches by 4-inches. The expanded metal shall be securely anchored to the wood support by stainless steel screws and washers, the screws being no less than 3-inches in length. The screws and washers will be installed at no less than 6-inch intervals. The expanded metal shall be affixed in a manner to prevent tampering or to show evidence of attempts of removal.

- (2) Ceiling: The ceiling shall be reinforced with 9-gauge expanded metal as defined in paragraph (1) above.
- (3) Door/Frame: The door and frame will be 12-gauge, steel clad, hollow core, and metal.
- (4) Hinges: Hinge pins shall be non-removable (pinned, peened or spot welded) or installed on the door interior.
- (5) Lock: The lock shall be a manipulative resistant deadbolt (MEDECO or equivalent).
- (6) IDS: The seized property room shall have an IDS. Examples of IDS systems include balanced magnetic switches, dual technology volumetric motion detectors and CCTV. This IDS will be connected to a Class A central station monitoring facility. There must be a backup method of communication set up with the Central Station, e.g. a wireless phone link (such as cellular) or an extra analog/digital telephone line so that if a telephone line is cut or otherwise interrupted, an alarm is activated at the monitoring company. Acknowledgement of an alarm condition by the Central Monitoring Station must take place within 30 seconds of the alarm. The Central Station must dispatch the correct response (law enforcement, duty agent, etc.). For additional information on IDS, please see Part 6.3.
- (7) Access control: To facilitate daily operations, an access control device will be used at all seized property rooms. Examples such as mechanical push button locks; electronic push button locks and proximity card readers may be utilized to augment the deadbolt lock. During non-working hours, the deadlock will be engaged.

4.9 THE TERM “STRONG ROOM” APPLIES TO STORAGE ROOMS LOCATED AT OLDER CUSTOM HOUSES AND PORTS OF ENTRY.

STRONG ROOMS MAY BE USED AS A PERMANENT OR TEMPORARY STORAGE FACILITIES. PORT DIRECTORS WILL DETERMINE THE USE OF STRONG ROOMS, E.G. PERMANENT OR TEMPORARY STORAGE. IF USE WILL BE PERMANENT STORAGE, THE STRONG ROOM MUST MEET THE CONSTRUCTION STANDARDS DESCRIBED IN PART 4.7. IF USED AS A TEMPORARY STORAGE FACILITY, THE FOLLOWING STANDARDS APPLY:

- (1) Strong rooms must be lined with steel or 9-gauge expanded metal. The expanded metal shall be in a 1-1/2 inches by 2-inches diamond pattern.
- (2) The outer door shall have an integral three-position, spin dial combination lock.

- (3) If equipped with an inner door, the door shall have either a three position, spin dial combination lock or key deadbolt lock.
- (4) If the inner door is equipped with a key lock it shall be keyed off the building master. The keys shall be secured in a GSA approved Class V security container.
- (5) If a strong room, designated to be used as permanent storage, cannot meet the construction standards of permanent storage (Part 4.7) of this handbook because of national historic status, then a request for a waiver must be submitted to the Assistant Commissioner, Office of Internal Affairs, pursuant to Part 1.6 of this handbook.
- (6) Strong Rooms must have an IDS. The IDS will be connected to a Class A Central Monitoring Station. There must be a backup method of communication set up with the Central Monitoring Station, e.g. a wireless phone link (such as cellular) or an extra analog/digital telephone line so that if a telephone line is cut or otherwise interrupted, an alarm is activated at the monitoring company. Acknowledgement of an alarm condition by the Central Monitoring Station must take place within 30 seconds of the alarm. The Central Monitoring Station must dispatch the correct response (law enforcement, duty agent, etc.). For additional information regarding IDS, please see Part 6.3.

4.10 SECURITY CONTAINERS AND SAFES FOR TEMPORARY STORAGE

Security containers and safes should be located within a secured or restricted area.

- a. Existing containers shall be GSA approved, Class V, 2 or 5 drawer storage containers, with single or multiple spin dial combination locks, e.g. Mosler, Sargent & Greenleaf, MAS Hamilton X-07 (or like upgrade).
- b. New containers will meet the requirements of Part 4.10 (a) above, and must withstand 10 minute forced entry.

NOTE: If the container weighs less than 500 pounds empty, it shall be bolted to the floor.

If a particular location cannot place a security container or safe in a restricted or secure area, please refer to Part 1.6.

4.11 SENSITIVE COMPARTMENTALIZED INFORMATION FACILITIES (SCIFs)

Any Customs component planning construction of a SCIF must notify the Internal

Affairs SMB, prior to any procurement or contracting activity. The SMB will act as the point of contact with the SCIF accreditation authority, which is either the Department of the Treasury or the Central Intelligence Agency through the Department of the Treasury, depending upon clearance level.

4.12 DETENTION CELLS

(RESERVED)

4.13 CASHIER/TELLER AREAS

a. General

- (1) Teller operations are defined as areas where monies, fees, tariffs, fines, penalties, and collections are transacted between the public and Customs personnel. The exact construction of the teller area and the type of security containers needed will depend on the average daily holdings, the location of the U.S. Customs Service office, and other considerations. Headquarters and/or regional physical security specialists must be consulted before any new area is anticipated or any change to an existing teller area is made.

b. Physical Security for Teller Operations

- (1) Perimeter walls for teller areas must be constructed slab to slab. The construction must be of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other opaque materials offering resistance to, and evidence of unauthorized entry into the area. If insert type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. When walls extend only to a suspended (false) ceiling, the wall area above the suspended (false) ceiling must be secured by the use of 9-gauge expanded metal, secured in such a manner that removal will show evidence of tampering.
- (2) Perimeter doors must be at least 1 ¾-inch thick, constructed of solid wood or be 12-gauge steel clad, hollow core metal doors. Door frames must be constructed of equal strength as that of the door. All exterior perimeter doors must be equipped with deadbolt type locks equipped with manipulation resistant cylinder (e.g., brand name MEDECO or equivalent). Keys must be off the building master in facilities that are not solely occupied by Customs. The deadbolts must have at least a 1-inch throw. Lock hardware placed on wood doorframes must be secured with stainless steel screws at least 3-inches long. Double doors must have at least one door secured from the inside with sliding deadbolts (e.g., Sargent and Greenleaf, model SM181, at the top and the bottom). Astragals (overlapping molding, preferably metal) must be used to inhibit

access to lock bolts. Perimeter door hinge pins must be non-removable (peened, pinned, or spotwelded) or installed inside the room.

- (3) The teller window will have a physical separation between the teller and the customer. This separation must be made by NIJ type III bullet resistant material with a pass through drawer. If the teller window is located on the perimeter wall of the building, facing the outside, that window must have type III bullet resistant material with a type III pass through drawer. The entire wall surrounding the teller window must meet the same bullet resistant standard as the window.
- (4) A Closed Circuit Television (CCTV) system is required to record transactions/activity at the teller window, as well as the entire interior teller area.
- (5) The teller operation may be located in the same area as other operations.
- (6) Excess currency will not be kept in the teller area. As often as business permits, currency in excess of the change making funds will be transferred to a GSA approved Class V security container. It is preferable to have this container located in a room away from the teller area. However, if this cannot be accomplished, the regional physical security specialist should be consulted for assistance in determining the most secure alternate locations.
- (7) In high-risk situations, the use of appropriate IDS and duress/panic alarm systems will be utilized. The duress/panic alarm should sound in the building control center, if one exists, or at the local police station or at an approved central station where appropriate response is assured. The IDS alarm must be monitored by a UL approved Class A Central Monitoring Station.
- (8) Cash drawers will be locked and the key removed if the teller must leave the teller area. If the teller must be away for 15 minutes or longer, the cash box will be removed and locked in a GSA approved Class V security container.
- (9) Cash drawers shall be emptied, and cash boxes stored in the security container at the end of each workday.
- (10) Keys and lock combinations for cash drawers, cash boxes, and safes shall be protected against compromise and changed as required.
- (11) Deposit pick-up schedules, under armored car contracts, should provide for the final pick-up of the day to be made at or about the time the teller operations close. The contract schedule should be flexible enough to

allow for extra, short notice pick-ups during the days when the total value of receipts is unusually high. However, if the recommended final pick-up time or extra pick-up provisions involve premium charges which would significantly increase total contract costs, a cost/benefit decision on whether to incur the increases will be made by the responsible persons. When economically feasible or when amounts to be transported are extremely large, contract couriers should be used.

4.14 ADDITIONAL PHYSICAL SECURITY MEASURES

To enhance the level of protection or to establish a level of protection commensurate with the threat, the following measures should be implemented where applicable. The following physical security measures should be reviewed by the appropriate Director, Field Operations, Special Agent in Charge, or Regional Special Agent in Charge for applicability at the Customs facilities under their purview.

a. Recommended Protection

- (1) Uniformed, armed guard service (Part 4.15d) with two-way radio communication capability.
- (2) Identification cards affixed with a photograph of employees.
- (3) Exterior protective lighting (Part 6.2).
- (4) Interior controls for Restricted Areas (Part 3.6).
- (5) Security glazing in all accessible areas, entrance doors, and guard houses; and bullet resistant glazing and materials where indicated by vulnerability assessment (Part 6.5).
- (6) Employee security orientation, and management/employee security awareness programs.
- (7) Perimeter security fences and guards houses [if applicable, (Part 6.6)].
- (8) Security file cabinets and safes (Part 4.10).
- (9) Package inspection programs.
- (10) Visitor controls, and escort program.
- (11) An Intrusion Detection System [IDS (Part 6.3)].
- (12) Silent duress/panic alarms (an alarm activated by an individual faced with

a threatening situation).

- (13) Local emergency exit alarm and evacuation plan.
- (14) Closed Circuit Television (CCTV), (Part 6.7).
- (15) Access Control Systems, e.g., card reader systems, mechanical or electronic access control devices, (Part 6.4).
- (16) If sensitive or classified discussions occur within a facility, the physical security guidelines contained in Customs Directive 1400-11, Technical Surveillance Countermeasures (TSCM) must be complied with and measures taken to ensure appropriate sound attenuation.

b. Ballistic Resistant Protective Material

- (1) Ballistic refers to a moving object such as a bullet, rock, or other projectile. Ballistic capabilities generally vary from vandal resistance to military rifle resistance.
- (2) Ballistic resistant protective material must be mounted in frames that provide ballistic protection equivalent to the ballistic resistant protective material.
- (3) Areas surrounding ballistic resistant protective material should also have equivalent ballistic protection. Generally, $\frac{1}{4}$ -inch of ballistic rated steel, or its equivalent, would be sufficient for protection against a high power rifle. National Institute of Justice Standard 0108.01, "Ballistic Resistant Protective Materials", part 6.5, provides testing standards that can be incorporated into a statement of work for procurement of ballistic protective construction.

c. Perimeter Security

- (1) When applicable, each facility containing a secured area, should be protected by a perimeter fence with appropriate gates to facilitate pedestrian and vehicular traffic to enter the facility on a controlled access basis. In addition to the paragraphs below, part 6.6 provides guidance on fencing. When fence gates are opened to ingress or egress, uniformed, armed security guards may be required to monitor each opening to ensure against unauthorized access.
- (2) Loading docks, kitchen entrances, and boiler room doors are normally weak links in building perimeter security. The installation of fencing around these entrances, with the gates alarmed and/or controlled by guards, strengthens the security of these areas.

- (3) Initial control for entry into a facility will be exercised at the authorized entrance. Each authorized entrance may require protection by a guard when not closed and locked.
- (4) All persons entering the property on foot will be allowed access upon presentation of proper identification or an authorized visitor pass. Persons in vehicles may be permitted to enter without being identified if the vehicle has an authorized vehicle identification sticker, dependent upon the level of security required. Visitors will be directed to the building entrance designated for visitors where they will be issued a non-photo identification badge.

d. Security Guard Service

- (1) Where applicable and legally feasible, facilities should employ a fulltime, uniformed, armed protective service utilizing the negotiated, and multi-year contract with option to renew. General criteria for the use of armed guards is as follows:
 - (a) Critical to the National Security. Loss of the building and the operations conducted in the building will have an immediate and serious impact on the National Security mission.
 - (b) Critical to maintaining the agency mission. Loss of the building and the operations in the building will have an immediate and serious impact on the agency's ability to perform its mission.
 - (c) The building contains extensive holdings of classified information, valuable materials, and irreplaceable records/documents.
 - (d) Security guards may also be needed to conduct screening of visitors to the building and operate metal detectors and package X-ray machines. They may also be required to monitor open or unlocked entrances and exits during times of building evacuation.
- (2) An annual 24-hour guard post consists of 8,760 staff-hours. Since an individual works approximately 1,770 productive staff-hours yearly, it takes five guards to cover one annual 24-hour post. Security guards will be required at the following 24-hour posts, depending on the facility:
 - (a) 24-hour building entrance
 - (b) CCTV console
 - (c) Internal patrol
 - (d) External patrol

- (3) Each security guard must successfully pass an appropriate background investigation by the GSA or USCS contract background investigators to determine suitability to protect federal facilities.
- (4) Each security guard, required to be armed, shall be properly trained and certified in the use of firearms in accordance with GSA standards. Each security guard, trained and certified, shall carry a fully loaded and holstered firearm at all times while on duty, unless prohibited by local statutes or agency directives, e.g. Customs Directive 4510-17, U.S. Customs Firearms and Use of Force Policy, dated July 22, 1996, or superseding directives.
- (5) A full-time, on-site guard supervisor must be on duty at each major facility for each shift of guards.
- (6) Request for security guard service will be submitted to the Logistics Division for GSA controlled space or to the Procurement Division for Customs controlled space.

e. Tours and Visitors

- (1) The need to maintain reasonable security at facilities containing secured areas, at all times requires that only authorized visitors be permitted to enter the site. Providing tours for interested non-Customs related individuals or groups for purposes of orienting them with Customs operations should be on a case-by-case basis.
- (2) Historic sites open to the public require vigilance on the part of every employee. Every employee must be required to report suspicious activity and must know where to report it. Guards must be constantly reminded of the potential for bombings, terrorist attacks and the potential for stay behind intruders.
- (3) Visitors to Customs controlled spaces are prohibited from using cameras and video recording devices. The senior Customs official on site may grant exceptions to this policy on a case-by-case basis.

f. Interior Security and Control

- (1) Each responsible senior Customs official on site will institute internal security controls as necessary to properly protect the site and preserve the confidentiality of operations and protect classified and sensitive information and government property. Control of the internal movements of personnel within a facility is necessary to ensure that only authorized personnel are permitted in secured areas and that visitors do not wander through the facility unescorted.

g. Locking Mechanisms

- (1) Key activated locks are most often used for securing interior and exterior doors. They offer normal protection for most agency offices. Some problems with these type of locking devices is the ease with which the keys can be duplicated or the locks picked to gain access. Another problem is loss of keys, thereby requiring rekey of the respective lock to which the key belonged and reissuance of keys. For this reason, caution must be exercised in the distribution and control of keys. Also, the use of high security locks, e.g., Medeco, is advised as the keys are difficult to duplicate.
- (2) There are a variety of key activated pin tumbler padlocks available; however, the degree of protection varies. A padlock with hardened shank offers normal protection. If the padlock is used in connection with a hasp and bar, care must be taken to ensure that the screws mounting the hasp and bar to the cabinet cannot be removed when the padlock locks the bar and hasp. The drawers to the cabinet should not be able to be pulled open, when the bar and hasp are on the cabinet. The bottom of the file cabinet should not have a false or open bottom. **Under no circumstances shall classified material be stored in barlock or padlock cabinets.**
- (3) There are several types of combination padlocks offering varying degrees of protection. The most secure are the "manipulation-resistant" locks. Locks meeting the requirements of Federal Supply Schedule Specification FF-P-110, which is published by GSA should be used for securing lock bar filing cabinets and other types of file cabinets. An example of a lock meeting the Federal Supply Schedule Specification FF-P-110 is the Sargent and Greenleaf model 8077A.
- (4) Combinations to locks must be changed when the lock is placed in use (combination changed from the factory set combination); when a person who knows the combination no longer requires access; when the combination has been compromised or suspected to have been compromised or when the combination lock is found unlocked on the cabinet. When a combination lock is taken out of service, it must be returned to the factory set combination.

h. Control and Safeguarding of Keys and Combinations

Access to a locked area, room or file cabinet can only be controlled if the key or combination is controlled. When an unauthorized person knows a combination or a key is lost, the security provided by that combination or key is lost.

- (1) Combinations will be given only to those who have a need to have access to the building, room or file cabinet. Combinations will be committed to memory. They must not be written on calendar pads, desk blotters, or any other item even though it is carried on one's person or hidden away. A record of the combination should be forwarded to the next higher authority and placed in a secure container. Combinations should be changed when person(s) having knowledge of a combination no longer require access to the area.
- (2) Keys will be issued only to persons having a need to have access to the building, room or file cabinet. The number of duplicate keys will be kept to a minimum. The key issued to an individual shall be entered onto that person's property accountability record. Keys must be recovered when a person leaves the organization. Keys must be properly safeguarded by the individual it was issued to in order to preclude loss of the key. Keys must not be left in unlocked desk drawers or other unsecured places. Keys must not be loaned to others.
- (3) Supervisors will assign keys to personnel under their supervision and are responsible for proper key control. Proper key control consists of the utilization of a paper or automated log on which the person assigned a key must acknowledge receipt. At the discretion of the senior Customs manager on site, locks will be changed when a key has been reported/discovered missing.
- (4) Duplicate keys will be kept to a minimum and safeguarded in a secure container or safe under the control of the supervisor. It is recommended that keys be stamped with: "**DO NOT DUPLICATE-U.S. GOVERNMENT PROPERTY**".
- (5) Padlocks will be placed inside the file cabinet or container or locked to the hasp to prevent the malicious switching of padlocks while the container is open.

i. Windows

- (1) Windows, air conditioning ducts and any openings that exceed 96 square inches and vulnerable to forced entry, should be secured with 9 gauge expanded metal, half inch steel bars spaced at 6" intervals with spreader bars at 6" on center, or be protected by an IDS.

j. Cleaning

- (1) Janitors must clean all Customs facilities/space during working hours, when Customs personnel are present. Janitors must not be provided keys to the facility or otherwise afforded access to Customs space that would enable them to enter the site/space without any Customs personnel

present. Normally, janitors do not need to be escorted in Customs space, however, if sensitive or classified discussions take place or classified/sensitive documents are at the site, then consideration must be given to having a Customs employee sanitize the site of any such documents, warn personnel present that the janitors are in the area, and escort the janitors during their cleaning.

k. Personnel Identification System

- (1) Personal recognition is the best form of acknowledgement that a person is authorized to be in a Customs facility or space.
- (2) The use of a personnel identification system (badge system) is necessary in locations where the number of employees exceeds 50.
- (3) The senior Customs official where a badge system is implemented is responsible for oversight and administration of the badge program. Personnel and equipment must be provided to properly administer a badge system.
- (4) Any identification system or badge system, not already authorized by the SMB will require SMB approval before implementation. The request for approval along with a description of the system will be sent to SMB.
- (5) Identification cards/badges will be recovered when personnel leave the site due to resignation, termination, retirement, etc. A complete re-issuance of badges, for all employees must be accomplished when the number of badges lost exceeds ten percent of the overall number of badges issued. The senior Customs official or his/her designee will maintain records that will document the number of lost badges. Monthly reviews of these records will be conducted to ascertain the ten percent level. Customs employees are responsible for safeguarding their badges from loss or misuse.
- (6) If temporary or visitors badges are used, a strict accounting of their issuance must be maintained either by manual or electronic means. Temporary and visitors badges must be collected when the person leaves the facility. Daily inventories of these badges must be conducted. Missing badges (possibly due to loss or theft) constitute a possible security risk and could require a design change and new issuance. The Customs official in charge of the facility is responsible for deciding when it is appropriate to take this action.

PART 5

CLASSIFIED DOCUMENT PROTECTION

5 CLASSIFIED DOCUMENT PROTECTION

5.1 GENERAL

The Safeguarding Classified Information Handbook, CIS HB 1400-03, provides policy guidance for the storage and handling of administratively controlled and classified information. Questions regarding document or information security should be directed to the appropriate field Internal Affairs Office or to the SMB.

5.2. SECURITY DURING OFFICE MOVES

All office moves and relocations require planning to properly protect and account for all information and government property. Careful consideration must be given to the circumstances of the move, the distance involved, and the method to be used in making the move. All sensitive, official use only, limited official use and/or classified information will be transported in locked cabinets or sealed packing cartons while in transit. Accountability will be maintained to ensure that cabinets or cartons do not become misplaced or lost during the move. A complete inventory of all classified and sensitive documents will be made prior to and immediately upon completion of an office move to ensure accountability.

Classified and sensitive documents will remain in the custody of an U.S. Customs employee throughout the move. Government property shall be protected commensurate with the property involved. Small items of high value will be packed in cartons or moved in locked cabinets. The senior Customs official, on site, or his/her designee is responsible for the overall move and accountability for documents/property.

5.3 FREEDOM OF INFORMATION/PRIVACY ACTS

In accordance with the Freedom of Information Act (FOIA), U.S. Customs Service records and manuals are generally available to the public. However, certain classes of information are exempt from disclosure and must be protected from unauthorized access. Among the categories of information which may be exempt from disclosure and must be secured are classified National Security information; proprietary business and commercial information; investigative records; case files; manuals and instructions to Customs personnel relating to law enforcement techniques and procedures; internal policy memoranda and information pertaining to individuals.

The Privacy Act of 1974 provides that an individual's privacy will be protected by the use of safeguards to prevent the disclosure of any record pertaining to that individual without his or her consent, unless such disclosure falls within one of several exceptions set forth in the Act [5 USC 552a(b)]. However, the Act also provides that an individual may gain access to records pertaining to himself or herself, except in cases where the records are contained in a system of records

properly exempted from the access provisions of the Act.

The FOIA provides that all non-exempt portions of records must be disclosed and that the government may waive exemptions. The authority to determine the applicability of exemptions under the Act to particular records and the authority to grant or deny requests for access to U.S. Customs Service records has been delegated to the various managers at Customs Headquarters who have custody of the records or have jurisdiction over the subject matter.

All U.S. Customs records and information falling within the categories identified above must be maintained and protected from unauthorized access until the appropriate Customs official having authority to grant or deny requests under the FOIA has determined their availability for release.

PART 6

TECHNICAL STANDARDS

THIS SECTION CONTAINS INFORMATION ON BOMB THREATS, PROTECTIVE LIGHTING, INTRUSION DETECTION SYSTEMS, ACCESS CONTROL SYSTEMS, BALLISTIC RESISTANT MATERIAL, WINDOW GLAZING, FENCES, CLOSED CIRCUIT TELEVISION, ACOUSTIC CONTROL, AND INSPECTIONS AND REPORTS.

PART 6

TECHNICAL STANDARDS

6.1 BOMB THREAT CHECKLIST

INFORMATION NOTICE

NUMBER: 00-003

ISSUE DATE: January 21, 2000

EXPIRES: December 29, 2000

SUBJECT: Reporting Bomb Threats

The purpose of this Notice is to establish guidelines for reporting Bomb Threats at U.S. Customs facilities. Prior planning is essential. Each SAIC, Director/Field Operations, STC Director and Air/Marine Branch Chief is responsible for formulating an action plan for responding to a bomb threat incident. The action plan should include coordination with federal, state and local agencies who may respond to the scene or assist in some manner with the bomb threat situation. The action plan will be shared with all employees, in accordance with Customs Directive 099 4510-019, entitled "Management of Critical Incidents". The Office of Investigations has jurisdiction for investigating threats against USCS employees and facilities.

The Commissioner's Situation Room at Headquarters will be notified as soon as practicable of the circumstances of the threat. The notification shall be made at a time that it is safe to do so. The phone number of the Commissioner's Situation Room is 1-877-748-7666 or 202-927-0425.

IF YOU RECEIVE A BOMB THREAT OVER THE TELEPHONE, OR IN WRITING, OR RECEIVE A SUSPICIOUS PACKAGE, PLEASE DO THE FOLLOWING:

FOR TELEPHONE THREATS:

- DO NOT ACTIVATE THE FIRE ALARM SYSTEM.
- Remain calm so you can get as much information from the caller as possible. Refer to the USCS "Bomb Threat Check-List", attached to this Notice.
- If possible, ask a co-worker to listen in on the call with you to help you remember key details later.
- Do not hang up or use the phone line the bomb threat call is on. It may be possible to trace the location of the call.
- From a different telephone, notify local law enforcement by dialing 911 or the Federal Protective Service if in a federal building. If necessary, contact the FBI, ATF, and other appropriate agencies.
- Carefully describe the nature of the emergency.
- State the building's name, street address, floor and suite/room.
- Answer all questions from local law enforcement. Do not hang up until the operator releases you. Provide a call back number.
- Notify the nearest USCS Office of Investigations field office.
- Follow the instructions of the authorities when they arrive.
- If instructed, evacuate the building. Follow the evacuation procedures as outlined in your building's Occupant Emergency Plan (OEP).



FOR WRITTEN BOMB THREATS OR SUSPICIOUS PACKAGES:

- DO NOT ACTIVATE THE FIRE ALARM SYSTEM.
- Avoid unnecessary physical handling of the written threat. This evidence will be analyzed by the authorities for fingerprints, postmarks, handwriting, and typewriting.
- Do not touch or otherwise disturb any suspicious packages!
- Notify local law enforcement by dialing 911 or the Federal Protective Service if in a federal building. If necessary, contact the FBI, ATF, and other appropriate agencies.
- Carefully describe the nature of the emergency. State the building's name, street address, floor and suite/room.
- Answer all questions from local law enforcement. Do not hang up until the operator releases you. Provide a call back number.
- Notify the nearest USCS Office of Investigations field office.
- If instructed, evacuate the building. Follow the evacuation procedures as outlined in your building's Occupant Emergency Plan (OEP).



Assistant Commissioner
Office of Internal Affairs

Attachment



U.S. CUSTOMS SERVICE BOMB TREAT CHECK-LIST

Exact Date/Time Of Call: _____

Exact Words Of Caller:

QUESTIONS TO ASK:

1. When is the bomb going to explode? _____
2. Where is the bomb? _____
3. What does it look like? _____
4. What kind of bomb is it? _____
5. What will cause it to explode? _____
6. Did you place the bomb? _____
7. Why? _____
8. Where are you calling from? _____
9. What is your address? _____
10. What is your name? _____

CALLER'S VOICE (Circle)

Calm	Disguised	Nasal	Angry	Broken
Slow	Stutter	Sincere	Lisp	Rapid
Deep	Crying	Squeaky	Excited	Stressed
Loud	Slurred	Normal	Accent	Giggling

If voice is familiar, whom did it sound like? _____

Were there any background noises? _____

Additional Comments: _____

Person receiving call: _____

Telephone number call received at: _____

- over -

BACKGROUND SOUNDS:

- | | |
|--|--|
| <input type="checkbox"/> Street noises | <input type="checkbox"/> Factory machinery |
| <input type="checkbox"/> Crockery | <input type="checkbox"/> Animal noises |
| <input type="checkbox"/> Voices | <input type="checkbox"/> Clear |
| <input type="checkbox"/> PA System | <input type="checkbox"/> Static |
| <input type="checkbox"/> Music | <input type="checkbox"/> Local |
| <input type="checkbox"/> House noises | <input type="checkbox"/> Booth |
| <input type="checkbox"/> Motor | <input type="checkbox"/> Office machinery |
| <input type="checkbox"/> Other _____ | |

THREAT LANGUAGE:

- | | |
|---|--|
| <input type="checkbox"/> Well spoken (educated) | <input type="checkbox"/> Incoherent |
| <input type="checkbox"/> Foul | <input type="checkbox"/> Taped |
| <input type="checkbox"/> Irrational | <input type="checkbox"/> Message read by
threat maker |

REMARKS:

Report call immediately to:

Phone number: _____

Date: / /

Name: _____

Position: _____

Phone number: _____

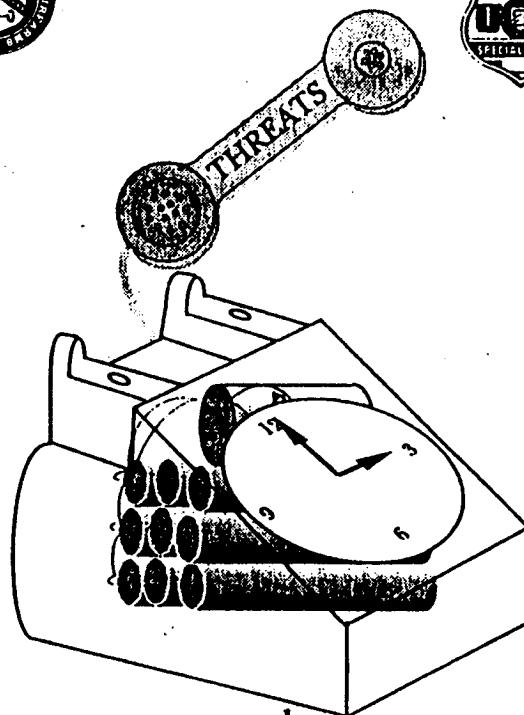
Department of the Treasury
Bureau of Alcohol, Tobacco and Firearms
Washington, D.C. 20228

Official Business
Penalty for Private Use, \$300

Postage and Fees Paid
Department of the Treasury
Treas 564



BOMB



and
**Physical
Security Planning**

DEPARTMENT of the TREASURY Bureau of Alcohol, Tobacco and Firearms
ATF P 7550.2 (7/87)



Bombs

Bombs can be constructed to look like almost anything and can be placed or delivered in any number of ways. The probability of finding a bomb that looks like the stereotypical bomb is almost nonexistent. The only common denominator that exists among bombs is that they are designed or intended to explode.

Most bombs are homemade and are limited in their design only by the imagination of, and resources available to, the bomber. Remember, when searching for a bomb, suspect anything that looks unusual. Let the trained bomb technician determine what is or is not a bomb.

Bomb Threats

Bomb threats are delivered in a variety of ways. The majority of threats are called in to the target. Occasionally these calls are through a third party. Sometimes a threat is communicated in writing or by a recording.

Two logical explanations for reporting a bomb threat are:

1. The caller has definite knowledge or believes that an explosive or incendiary bomb has been or will be placed and he/she wants to minimize personal injury or property damage. The caller may be the person who placed the device or someone who has become aware of such information.
2. The caller wants to create an atmosphere of anxiety and panic which will, in turn, result in a disruption of the normal activities at the

facility where the device is purportedly placed.

Whatever the reason for the report, there will certainly be a reaction to it. Through proper planning, the wide variety of potentially uncontrollable reactions can be greatly reduced.

Why Prepare?

If you accept the two aforementioned explanations for reporting that a bomb is about to go off, you can better prepare to foil the bomber or threat maker.

Through proper preparation, you can reduce the accessibility of your business or building and identify those areas that can be "hardened" against the potential bomber. This will limit the amount of time lost to searching, if you determine a search is necessary. If a bomb incident occurs, proper planning will instill confidence in the leadership, reinforce the notion that those in charge do care, and reduce the potential for personal injury and property loss.

Proper planning can also reduce the threat of panic, the most contagious of all human emotions. Panic is sudden, excessive, unreasoning, infectious terror. Once a state of panic has been reached, the potential for injury and property damage is greatly increased. In the context of a bomb threat, panic is the ultimate achievement of the caller.

Be prepared! There is no excuse for not taking every step necessary to meet the threat.

How to Prepare

In preparing to cope with a bomb incident, it is necessary to develop two separate but interdependent plans, namely a physical security plan and a bomb incident plan.

Physical security provides for the protection of property, personnel, facilities, and material against unauthorized entry, trespass, damage, sabotage, or other illegal or criminal acts. The physical security plan deals with prevention and control of access to the building. In most instances, some form of physical security may be already in existence, although not necessarily intended to prevent a bomb attack.

The bomb incident plan provides detailed procedures to be implemented when a bombing attack is executed or threatened. In planning for the bomb incident, a definite chain of command or line of authority must be established. Only by using an established organization and procedures can the bomb incident be handled with the least risk to all concerned. A clearly defined line of authority will instill confidence and avoid panic.

Establishing a chain of command is easy if there is a simple office structure, one business, one building. However, if a complex situation exists, a multi-occupant building for example, a representative from each occupant entity should attend the planning conference. A leader should be appointed and a clear line of succession delineated. This chain of command should be printed and circulated to all concerned parties.

In planning, you should designate a command center to be located in the switchboard room or other focal point of telephone or radio communications. The management personnel assigned to operate the center should have the authority to decide whatever action should be taken during the threat. Only those with assigned duties should be permitted in the center. Make some provision for alternates in the event someone is absent when a threat is received. Obtain an updated blueprint or floor plan of your building and maintain it in the command center.

Contact the police department, fire department, or local government agencies to determine if any assistance is available to you for developing your physical security plan or bomb incident plan. If possible, have police and/or fire department representatives and members of your staff inspect the building for areas where explosives are likely to be concealed. (Make a checklist of these areas for inclusion in command center materials.) Determine whether there is a bomb disposal unit available, how to contact the unit, and under what conditions it is activated. In developing your bomb incident plan, you must also ascertain whether the bomb disposal unit, in addition to disarming and removing the explosives, will assist in searching the building in the event of a threat.

Training is essential to deal properly with a bomb threat incident. Instruct all personnel, especially those at the telephone switchboard, in what to do if a bomb threat is received. Be absolutely certain that all personnel assigned to the command center are aware of their duties. The positive aspects of planning will be lost if the leadership is not apparent. It is also

Perhaps entrances and exits can be modified with a minimal expenditure to channel all visitors through someone at a reception desk. Individuals entering the building would be required to sign a register indicating the name and room number of the person whom they wish to visit. Employees at these reception desks could contact the person to be visited and advise him/her that a visitor, by name, is in the lobby. The person to be visited may decide to come to the lobby to ascertain that the purpose of the visit is valid. A system for signing out when the individual departs could be integrated into this procedure.

Such a procedure may result in complaints from the public. If the reception desk clerk explains to the visitor that these procedures were implemented in his/her best interest and safety, the complaints would be reduced. The placement of a sign at the reception desk informing visitors of the need for safety is another option.

Responding to Bomb Threats

Instruct all personnel, especially those at the telephone switchboard, in what to do if a bomb threat call is received.

It is always desirable that more than one person listen in on the call. To do this, a covert signaling system should be implemented, perhaps by using a coded buzzer signal to a second reception point.

A calm response to the bomb threat caller could result in obtaining additional information. This is especially true if the caller wishes to avoid injuries or deaths. If told that the building is occupied or cannot be evacuated in

time, the bomber may be willing to give more specific information on the bomb's location, components, or method of initiation.

The bomb threat caller is the best source of information about the bomb. When a bomb threat is called in:

- Keep the caller on the line as long as possible. Ask him/her to repeat the message. Record every word spoken by the person.
- If the caller does not indicate the location of the bomb or the time of possible detonation, ask him/her for this information.
- Inform the caller that the building is occupied and the detonation of a bomb could result in death or serious injury to many innocent people.
- Pay particular attention to background noises, such as motors running, music playing, and any other noise which may give a clue as to the location of the caller.
- Listen closely to the voice (male, female), voice quality (calm, excited), accents, and speech impediments. Immediately after the caller hangs up, report the threat to the person designated by management to receive such information.
- Report the information immediately to the police department, fire department, ATF, FBI, and other appropriate agencies. The sequence of notification should be established in the bomb incident plan.

— Remain available, as law enforcement personnel will want to interview you.

When a written threat is received, save all materials, including any envelope or container. Once the message is recognized as a bomb threat, further unnecessary handling should be avoided. Every possible effort must be made to retain evidence such as fingerprints, handwriting or typewriting, paper, and postal marks. These will prove essential in tracing the threat and identifying the writer.

While written messages are usually associated with generalized threats and extortion attempts, a written warning of a specific device may occasionally be received. It should never be ignored.

Decision Time

The most serious of all decisions to be made by management in the event of a bomb threat is whether to evacuate the building. In many cases, this decision may have already been made during the development of the bomb incident plan. Management may pronounce a carte blanche policy that, in the event of a bomb threat, total evacuation will be effective immediately. This decision circumvents the calculated risk and demonstrates a deep concern for the safety of personnel in the building. However, such a decision can result in costly loss of time.

Essentially, there are three alternatives when faced with a bomb threat:

1. Ignore the threat.
2. Evacuate immediately.
3. Search and evacuate if warranted.

Ignoring the threat completely can result in some problems. While a statistical argument can be made that very few bomb threats are real, it cannot be overlooked that bombs have been located in connection with threats. If employees learn that bomb threats have been received and ignored, it could result in morale problems and have a long-term adverse effect on your business. Also, there is the possibility that if the bomb threat caller feels that he/she is being ignored, he/she may go beyond the threat and actually plant a bomb.

Evacuating immediately on every bomb threat is an alternative that on face value appears to be the preferred approach. However, the negative factors inherent in this approach must be considered. The obvious result of immediate evacuation is the disruptive effect on your business. If the bomb threat caller knows that your policy is to evacuate each time a call is made, he/she can continually call and force your business to a standstill. An employee, knowing that the policy is to evacuate immediately, may make a threat in order to get out of work. A student may use a bomb threat to avoid a class or miss a test. Also, a bomber wishing to cause personal injuries could place a bomb near an exit normally used to evacuate and then call in the threat.

Initiating a search after a threat is received and evacuating a building after a suspicious package or device is found is the third, and perhaps most desired, approach. It is certainly not as disruptive as an immediate evacuation and will satisfy the requirement to do something when a threat is received. If a device is found, the evacuation can be accomplished expeditiously while at the same time avoiding the potential danger areas of the bomb.

After the room has been divided and a searching height has been selected, both individuals go to one end of the room division line and start from a back-to-back position. This is the starting point, and the same point will be used on each successive searching sweep. Each person now starts searching his/her way around the room, working toward the other person, checking all items resting on the floor around the wall area of the room. When the two individuals meet, they will have completed a "wall sweep." They should then work together and check all items in the middle of the room up to the selected hip height, including the floor under the rugs. This first searching sweep should also include those items which may be mounted on or in the walls, such as air-conditioning ducts, baseboard heaters, and built-in wall cupboards, if these fixtures are below hip height.

The first searching sweep usually consumes the most time and effort. During all the searching sweeps, use the electronic or medical stethoscope on walls, furniture items, and floors.

Second Room-Searching Sweep

The individual in charge again looks at the furniture or objects in the room and determines the height of the second searching sweep. This height is usually from the hip to the chin or top of the head. The two persons return to the starting point and repeat the searching technique at the second selected searching height. This sweep usually covers pictures hanging on the walls, built-in bookcases, and tall table lamps.

Third Room-Searching Sweep

When the second searching sweep is completed, the person in charge again determines the next searching height, usually from the chin or the top of the head up to the ceiling. The third sweep is then made. This sweep usually covers high mounted air-conditioning ducts and hanging light fixtures.

Fourth Room-Searching Sweep

If the room has a false or suspended ceiling, the fourth sweep involves investigation of this area. Check flush or ceiling-mounted light fixtures, air-conditioning or ventilation ducts, sound or speaker systems, electrical wiring, and structural frame members.

Have a sign or marker indicating "Search Completed" conspicuously posted in the area. Place a piece of colored Scotch tape across the door and door jamb approximately 2 feet above floor level if the use of signs is not practical.

The room searching technique can be expanded. The same basic technique can be applied to search any enclosed area. Encourage the use of common sense or logic in searching. If a guest speaker at a convention has been threatened, common sense would indicate searching the speakers platform and microphones first, but always return to the searching technique. Do not rely on random or spot checking of only logical target areas. The bomber may not be a logical person.

In conclusion, the following steps should be taken in order to search a room:

1. Divide the area and select a search height.
2. Start from the bottom and work up.
3. Start back-to-back and work toward each other.
4. Go around the walls and proceed toward the center of the room.
5. Evacuate the building.
6. Do not permit re-entry into the building until the device has been removed/disarmed, and the building declared safe for re-entry.

Suspicious Object Located

It is imperative that personnel involved in a search be instructed that their only mission is to search for and report suspicious objects. Under no circumstances should anyone move, jar or touch a suspicious object or anything attached to it. The removal or disarming of a bomb must be left to the professionals in explosive ordnance disposal. When a suspicious object is discovered, the following procedures are recommended:

1. Report the location and an accurate description of the object to the appropriate warden. This information should be relayed immediately to the command center, which will notify the police and fire departments, and rescue squad. These officers should be met and escorted to the scene.
2. If absolutely necessary, place sandbags or mattresses, never metal shields, around the suspicious object. Do not attempt to cover the object.
3. Identify the danger area, and block it off with a clear zone of at least 300 feet, including floors below and above the object.

Handling of the News Media

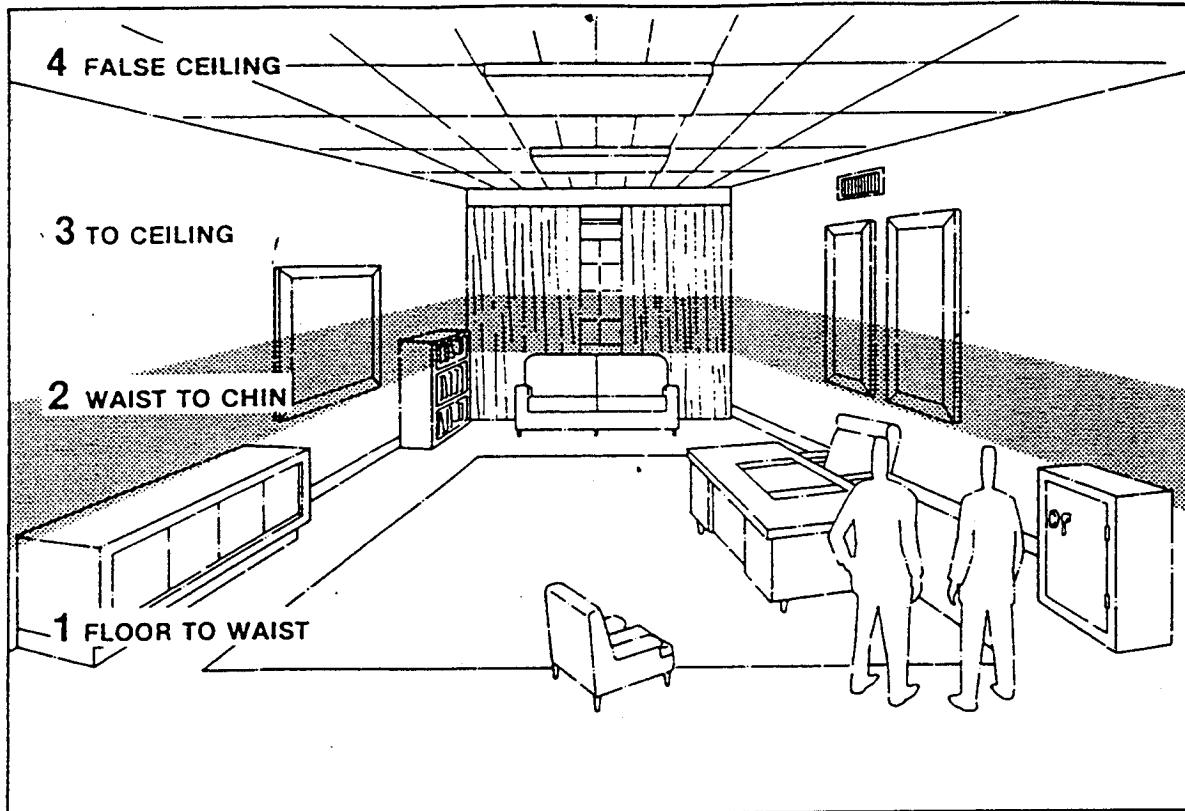
It is of paramount importance that all inquiries from the news media be directed to one individual appointed as spokesperson. All other persons should be instructed not to discuss the situation with outsiders, especially the news media.

The purpose of this provision is to furnish the news media with accurate information and to see that additional bomb threat calls are not precipitated by irresponsible statements from uninformed sources.

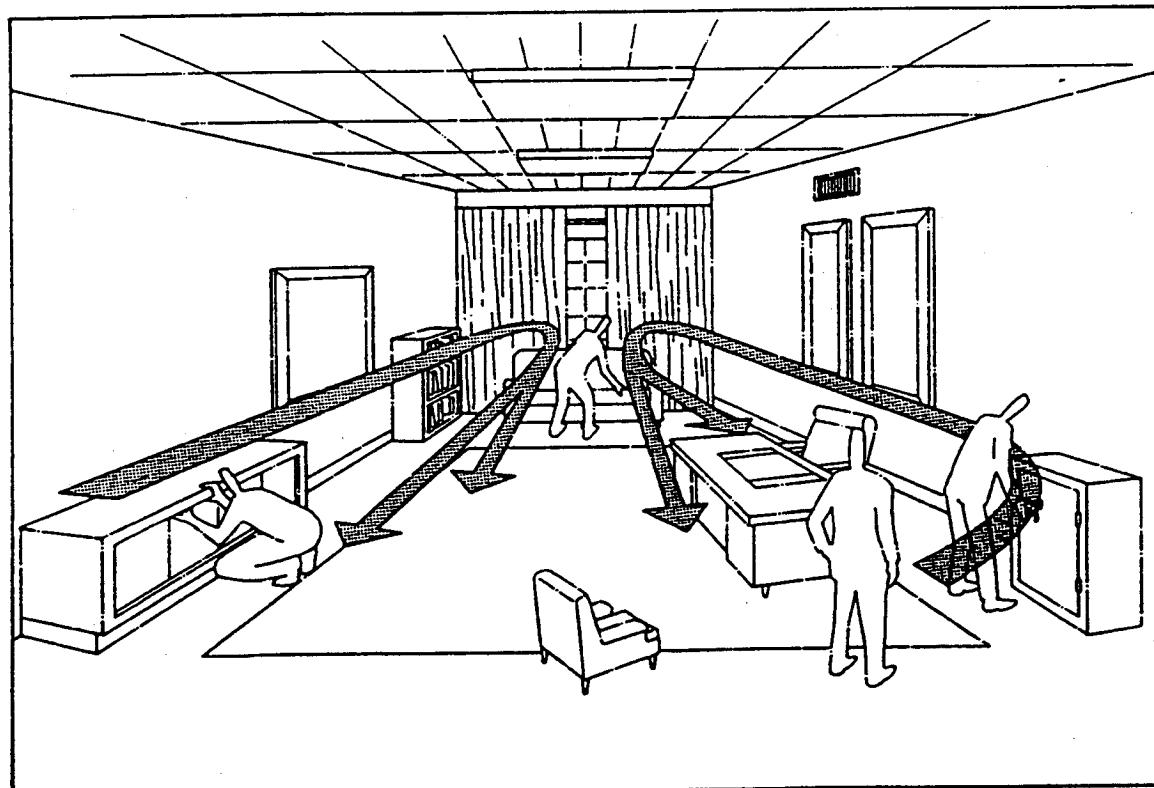
Summary

This pamphlet serves only as a guide and is not intended to be anything more. The ultimate determination of how to handle a bomb threat must be made by the individual responsible for the threatened facility.

Develop a bomb incident plan. Draw upon any expertise that is available to you from police departments, government agencies, and security specialists. Don't leave anything to chance. Be prepared!



#2 DIVIDE ROOM BY HEIGHT FOR SEARCH



#3 SEARCH ROOM BY HEIGHT & ASSIGNED AREA,
OVERLAP FOR BETTER COVERAGE

ATF BOMB THREAT CHECKLIST

Exact time of call _____

Exact words of caller _____

_____**QUESTIONS TO ASK**

1. When is bomb going to explode? _____
2. Where is the bomb? _____
3. What does it look like? _____
4. What kind of bomb is it? _____
5. What will cause it to explode? _____
6. Did you place the bomb? _____
7. Why? _____
8. Where are you calling from? _____
9. What is your address? _____
10. What is your name? _____

CALLER'S VOICE (circle)

Calm	Disguised	Nasal	Angry	Broken
Stutter	Slow	Sincere	Lisp	Rapid
Giggling	Deep	Crying	Squeaky	Excited
Stressed	Accent	Loud	Slurred	Normal

If voice is familiar, whom did it sound like? _____

Were there any background noises? _____

Remarks: _____

Person receiving call: _____

Telephone number call received at: _____

Date: _____

Report call immediately to: _____
(Refer to bomb incident plan)**ATF BOMB THREAT CHECKLIST**

Exact time of call _____

Exact words of caller _____

_____**QUESTIONS TO ASK**

1. When is bomb going to explode? _____
2. Where is the bomb? _____
3. What does it look like? _____
4. What kind of bomb is it? _____
5. What will cause it to explode? _____
6. Did you place the bomb? _____
7. Why? _____
8. Where are you calling from? _____
9. What is your address? _____
10. What is your name? _____

CALLER'S VOICE (circle)

Calm	Disguised	Nasal	Angry	Broken
Stutter	Slow	Sincere	Lisp	Rapid
Giggling	Deep	Crying	Squeaky	Excited
Stressed	Accent	Loud	Slurred	Normal

If voice is familiar, whom did it sound like? _____

Were there any background noises? _____

Remarks: _____

Person receiving call: _____

Telephone number call received at: _____

Date: _____

Report call immediately to: _____
(Refer to bomb incident plan)

PART 6
TECHNICAL STANDARDS
6.2 PROTECTIVE LIGHTING

6.2 PROTECTIVE LIGHTING

a. General

Protective (or security) lighting increases the effectiveness of Customs personnel performing their duties during hours of darkness. It has considerable value as a deterrent to thieves and vandals and increases the risk of uncertainty for other criminal activity.

As with ordinary sunlight during the day, protective lighting at night is useful for Customs personnel to use for their own safety and the security of their work site. A criminal will have to add the risk of being seen to all the other security measures that harden a facility.

The overall goal of protective lighting is to provide the proper environment to perform duties such as identification of badges and personnel at gates, inspection of vehicles, prevention of illegal entry, detection of intruders, and inspection of unusual or suspicious activities.

Requirements for protective lighting at a Customs facility will depend upon the situation and the areas to be protected. In the interest of finding the best possible mix between energy conservation and effective security, each situation must be carefully studied.

Professional assistance in the evaluation and recommendation in this area can be requested by contacting the Security Management Branch or the Regional Physical Security Specialist.

b. General Principles and Guidelines

The responsible official at a Customs facility will apply the following basic principles:

- (1) Provide adequate illumination or compensating measures to discourage or detect attempts to enter Restricted Areas and to reveal the presence of unauthorized personnel within such areas.
- (2) Avoid glare that handicaps security personnel or is objectionable to air, rail, highway or navigable water traffic or occupants of adjacent properties.
- (3) Locate light sources so that illumination is directed toward likely avenues of approach, and provides relative darkness for stationary posts.
- (4) Illuminate shadowed areas caused by structures within or adjacent to Restricted Areas.

- (5) Design the system to provide overlapping light distribution. Equipment selection should be designed to resist the effects of environmental conditions, and all components of the system should be located to provide maximum protection against intentional damage.
- (6) Meet requirements of blackout and coastal dim-out areas (as required).
- (7) During planning stages, consideration should be given to future requirements of closed circuit television (CCTV) and recognition factors involved in selection of the type of lighting to be installed.
- (8) Choose lights that illuminate the ground or water but not the air above. These lights must penetrate fog and rain.
- (9) When considering the above, do not overlook possible applications of on-demand infrared lighting, and/or infrared floodlights.
- (10) Lighting must not draw unwanted attention to the security area being protected.

c. Protective Lighting Measures

It is not the intent of this handbook to prescribe specific protective lighting requirements. The senior Customs official must decide what areas or assets to illuminate and how to do it. This decision must be based upon the following:

- (1) Relative value of items being protected.
- (2) Significance of the items being protected in relation to the mission of the Customs Service.
- (3) Availability of security personnel to observe illuminated areas.
- (4) Availability of areas that will make the intruder have no place to hide and must take the risk of being seen because of the light.
- (5) Availability of fiscal resources (procurement, installation, and maintenance costs).

d. Standard Exterior Lighting Configurations

Lighting may operate continuously or on a standby basis.

- (1) Continuous Lighting: Continuous lighting is the most common security lighting system. It consists of a series of fixed luminaries arranged to flood a given area continuously during the hours of darkness with

overlapping cones of light. The two primary methods of using continuous lighting are glare projection and controlled lighting.

- (2) Glare Lighting: Glare lighting uses luminaries slightly inside a security perimeter and directed outward. It is considered a deterrent to a potential intruder because it makes it difficult for him to see inside the area being protected. It also protects the guard by keeping him in comparative darkness and enabling him to observe intruders at considerable distance beyond the perimeter.
- (3) Controlled Lighting: Controlled lighting is used when it is necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways, railroads, navigable waters, or airports. In controlled lighting, the width of the lighted strip is controlled and adjusted to fit a particular need, such as illumination of a wide strip inside a fence and a narrow strip outside, or floodlighting a wall or roof. Unfortunately, this method of lighting often illuminates or silhouettes security personnel at their work area. Controlled lighting may provide direct or indirect illumination.
- (4) Standby Lighting: A standby lighting system is different from continuous lighting since its intent is to create an impression of activity. The luminaries are not continuously lighted but are either automatically or manually turned on intermittently or responsively when activity is detected or suspected by the security force or IDS. Lamps with short restrike times are essential if this technique is chosen. This technique may offer significant deterrent value while also offering economy in power consumption.
- (5) Intermittent Lighting: A lighting system can be developed to turn lights on at random times as a deterrent to some threats. It can use either direct or indirect illumination concepts. While an intermittent lighting system can involve a duty cycle of 10 to 50 percent, it may increase operational and maintenance costs, it may force the use of inefficient lamps, or reduce lamp life. Deterrence can actually be higher for such a system because of its appearance of activity. Luminaries may be controlled individually or as a group.
- (6) On-Demand Lighting: Rather than randomly activating the luminaries, an IDS sensor can be used to turn on the lights when an intruder is detected. This type of active lighting system provides maximum deterrent value at a low duty cycle. Such a responsive area system is subject to the same nuisance and false alarms as any sensor system.
- (7) Direct Illumination: This lighting concept involves directing light down to the ground. Its goal is to provide a specified intensity of illumination on

intruders, facilitating their detection by CCTV or security patrols.

- (8) Indirect Illumination: An alternative lighting concept involves backlighting the intruders against a facility. This may be done by placing lighting away from the building and directing it back toward the walls so shadows will be cast on the building by the threat. Such applications are most effective if the luminaries themselves are near ground level. This indirect concept is also aesthetically pleasing, illuminating the architecture during darkness.

e. Emergency Power

Restricted Areas provided with protective lighting will have an emergency power source located within the security area.

Emergency power systems must be adequate to sustain security lighting, CCTV, communications requirements, and other essential services required within a restricted and/or secured area, for a period of no less than 4 hours from the time of power failure.

Emergency power systems will be tested quarterly to ensure the system will perform as needed and will be recorded.

Emergency power sources will start automatically. Battery powered lights and essential communications will be available at all times at key locations within a restricted and/or secured area, in the event of complete failure of both the primary and emergency sources of power.

f. Wiring System

Multiple circuits may be used as an advantage in protective lighting systems. The circuits will be so arranged that the failure of any one lamp will not darken a long section of a critical or vulnerable area. The security area protective lighting system will be independent of other lighting systems.

g. Lighting Energy Considerations

Since the energy shortage of 1973-74, virtually every lighting system has come under scrutiny to identify energy savings. Security lighting systems are no exception. This scrutiny is probably as much related to the conspicuousness of security lighting as to the amount of energy consumed.

While the only energy consumption statistics available on lighting pertain to the energy required to maintain street lighting systems, security lighting used considerably less energy. Recently, the direction of the security community to reduce energy costs in security lighting has resulted in replacing luminaries to increase source efficacy by changing to high-pressure sodium (HPS) lamps.

HPS lamps produce more lumens per watt than either mercury vapor or incandescent lamps. The latter two lamps are the least efficient, costly, and most widely used.

Rather than randomly activating the luminaries, an IDS sensor can be used to turn on the lights when an intruder is detected. This type of active lighting system provides maximum deterrent value at a low duty cycle. Such a responsive area system is subject to the same nuisance and false alarms as any sensor system.

PART 6

TECHNICAL STANDARDS

6.3 INTRUSION DETECTION SYSTEM (IDS) GUIDE

6.3 INTRUSION DETECTION SYSTEM (IDS) GUIDE

The purpose of an alarm system is to detect an intrusion or attempted intrusion and to notify appropriate personnel.

a. General Requirements:

- (1) Equipment shall be UL approved (or equivalent);
- (2) If the secure area has a false ceiling or floor that provides a means for surreptitious entry, then one of the below listed methods should be used to protect that area;
- (3) A separate zone on the IDS covering the area between the false and true ceiling or false and true floor;
- (4) Expanded metal (9-gauge) partition between the false floor or ceiling and the true floor or ceiling;
- (5) Balanced Magnetic Switches (BMSs) on all perimeter doors;
- (6) All windows should be protected by an alarm system, either adequately covered by volumetric sensors or be individually alarmed, e.g. glass break sensors;
- (7) All control units will be located within the area protected by the alarm system;
- (8) All systems will be tested quarterly, i.e. doors opened and volumetric sensors walk tested. A record of these tests must be maintained;
- (9) All components shall be installed in a manner to prevent access or removal from a location external to the protected zone;
- (10) All alarm systems shall be capable of operating from commercial AC power. In the event of commercial power failure, provisions will be made for automatic switchover to emergency power, and back to commercial power without causing an alarm. A signal will be presented to the monitoring location indicating when the system has lost power. When batteries are used for emergency power, they will be maintained at full charge by automatic circuits. Emergency power must be capable of operating the system for a minimum of four hours;
- (11) Volumetric sensors employed in the alarm system must be placed so that the most likely intruder motions are detected;

- (12) All perimeter sensors and control units will be equipped with tamper detection;
- (13) Depending on facility operations, a duress/panic alarm may be installed. If a duress/panic alarm is used it must be connected to a class A Central Monitoring Station;
- (14) All alarm wiring leaving the controlled area shall be equipped with electronic line supervision.

Classes of Electronic Line Supervision – Line supervision is the electronic monitoring of IDS wiring to prevent compromise of the system by interrupting the signal in the wiring. Class C supervision or better should be used.

- (a) Class A – Pseudo-Random digital and tone-wire transmitted preferred. Exceeds previous “High Line Security” Requirement.

These systems will transmit over wire a pseudo-random generated tone or tones or digital type modulation. These systems will use either an interrogation and reply scheme or a synchronization scheme. The signal between the protected premises and the monitor location shall not repeat itself within a six month period. A line supervision alarm signal shall cause a lock-in condition, which shall be transmitted to the monitor location in not more than 30 seconds. If the above conditions cannot be met, then a UL approved system with commercial Grade A service and Grade AA transmission will be acceptable. It shall not be possible to compromise Class A systems by the use of resistance, voltage or current substitution techniques.

- (b) Class B – Digital and tone-wire transmitted preferred (Formerly described as High Line Security).

The systems using digital or tone type modulation over transmission lines shall use an interrogation and reply scheme. The signal technique used for the interrogation shall be different than that of the reply. Each line supervision alarm shall cause a lock-in condition, which shall be transmitted to the annunciator in not more than 90 seconds. If the above conditions cannot be met then a UL approved system with Grade B commercial service and Grade A transmission will be acceptable. It shall not be possible to compromise Class B systems by the use of resistance, voltage, or current substitution techniques. The circuits and methods employed shall be highly immune to transmission line noise, such as cross talk, hum, transients, and the like.

- (c) Class C-AC and DC- Wire transmitted (Standard Line Security). The Class C circuit supervisor units shall provide an alarm response in the annunciator in not more than one second as a result of the following changes in normal transmission line current: Five percent or more in normal line signal when it consists of direct current from 0.5 milliamperes through 30 milliamperes. Ten percent or more in normal line signal when it consists of direct current from 10 microamperes to 0.5 milliamperes. Five percent or more of any component or components in a complex signal upon which the security integrity of the system is dependent. This tolerance will be applied for frequencies up to 100Hz. Component as used in this specification means AC or DC voltage or current, AC phase, or frequency duration. Fifteen percent or more of any component or components in a complex signal upon which the security integrity of the system is dependent. This tolerance will be applicable for all frequencies above 100Hz. Components as used in this specification mean an AC or DC voltage or current, AC phase, or frequency duration.
- (15) Volumetric Sensors – There are two types of volumetric sensors in general use: passive infrared and microwave. The sensing capabilities cover a space rather than a door, window, or wall.
- (a) Passive infrared sensors are used to detect temperature differences. Temperature stability in a covered area is necessary. Heat or air conditioning outlets may cause an installer to avoid a specific area that should be covered. These sensors can be highly directional with a very narrow detection field near the sensor. Detection capabilities are most sensitive for movement across the field, as opposed to strength toward or away from the sensor. An intruder wearing a ski mask, coat and gloves may not be detected by some passive infrared sensors, dependent upon relative orientation and sensitivity of the sensor. If the sensor is blocked there will be no detection capability beyond the blockage.
- (b) Microwave sensors operate on a “radar” principle similar to ultrasonic, although the higher frequency eliminates problems with air turbulence. Vibration of doors, exposed pipes, or fluorescent lights can trigger a false alarm. If not properly adjusted, microwave can penetrate walls, allowing movement outside the protected area to create a false alarm. Microwave can be blocked from areas where protection is desired or reflected by large metal objects.
- (16) Remote Monitoring-IDS's are designed to annunciate at a remote location, or to sound an alarm at the site. Remote monitoring increases the likelihood for capture of the intruder and provides greater assurance of a

response. Optimal monitoring locations would be Federal Protective Service where applicable, Local Police departments having appropriate jurisdiction, and commercial vendors. Commercial vendors must be UL listed as a Class A Central Monitoring Station.

Automatic telephone tape dialers, that automatically place a telephone call and play a recorded message when the IDS senses an intrusion, are not authorized. They are bypassed by cutting the telephone lines, which makes them too easy to defeat.

- (17) IDS Evaluation – A thorough demonstration of sensors proposed by a contractor, careful review of proposed placement, and careful testing following installation are required procedures in the acquisition of an adequate IDS.

THE ATTACHED CHART MAY BE USED AS A SELECTION GUIDE FOR INTRUSION DETECTION SYSTEM VOLUMETRIC SENSORS. ALTHOUGH THE CHART INCLUDES ULTRASONIC SENSORS, THEIR USE IS NOT PERMITTED IN CUSTOMS FACILITIES.

**Selection Guidance for
Intrusion Detection System Volumetric Sensors**

The following matrix is intended as a guide only and does not represent absolutes, but suggests areas for consideration.

Environmental and

Other variables

Ultrasonic

Passive Infrared

Microwave

Vibration	No Problem with balanced processing, some problem with unbalanced	Very few problems	Can be a major problem
Effect of temperature change on range	A Little	A lot	None
Effect of humidity change on range	Some	None	None
Reflection of area of coverage by large metal objects	Very little	None, unless metal is highly polished	Can be a major problem
Reduction of range by drapes, carpets	Some	None	None
Sensitivity to movement of overhead doors	Needs careful placement	Very few problems	Can be a major problem
Sensitivity to small animals	Problem if animal is close	Problem if animal is close, but beam can be aimed well above ground level	Problem if animal is close
Water movement in plastic storm drain pipes	No problem	No problem	Can be a problem if very close
Water noise from faulty valves	Can be a problem, very rare	No problem	No problem
Movement through thin walls or glass	No problem	No problem	Needs careful placement
Drafts, air movement	Needs careful placement	No problem	No problem
Sun, moving headlights, through windows	No problem	Needs careful placement	No problem
Ultrasonic noise	Bells, hissing, some inaudible noises can cause problems	No problem	No problem
Heaters	Problem only in extreme cases	Needs careful placement	No problem
Moving machinery, fan blades	Needs careful placement	Very little problem	Needs careful placement
Radio interference, AC line transients	Can be a problem in severe cases	Can be a problem in severe cases	Can be a problem in severe cases
"Piping" of detection field to unexpected areas by AC ducting	No problem	No problem	Occasional problem where beam is directed at duct outlet
Radar interference	Very few problems	Very few problems	Can be a problem when radar is close and sensor pointed at it
Cost per Sq. ft. – large open areas	In between	Most expensive	Least expensive
Cost per sq. ft. – divided areas/multiple rooms	Least expensive	Most expensive	In between
Range adjustment required	Yes	No	Yes
Current consumption (size of battery required for extended standby power)	In between	Smallest	Largest
Interference between two or more sensors	Must be crystal controlled and/or synchronized	No problem	Must be different frequencies

PART 6

TECHNICAL STANDARDS

6.4 ACCESS CONTROL SYSTEMS GUIDANCE

6.4 ACCESS CONTROL SYSTEMS GUIDANCE

The purpose of this guidance is to provide information concerning access control, with attention focused on card access control systems for those Customs facilities in need of such a system, and not to advocate installation of this system at every Customs facility.

a. Background

Alternative access control systems should be considered if key operated systems are inefficient for a facility. The most prominent are mechanical pushbutton locks, electrical locks (keypad systems), and card access control systems listed here in ascending cost. A keypad system or mechanical pushbutton could provide adequate security at considerably less cost than card readers. Dependent upon the number of personnel requiring access, either of the two could be more cost effective than a card reader system, due to the cost of supporting computer equipment, administration, and access cards needed for the system. Frequently changing the access code would optimize the security they provide.

There are no absolute rules on the number of personnel utilizing a facility before a card reader system can be installed, but, common sense should suggest that a facility with a static population of employees in a low threat environment, where a visible identification card is not required, should probably opt for a less cumbersome system. If a card reader system is needed, consideration should be given to selection of a system compatible with the system selected for Headquarters facilities. Additional information about the Headquarters system may be acquired from the Security Management Branch. Any system configured to use these proximity cards (cards which are merely passed within 4 to 6-inches of the reader to release the electrically (operated bolt) will be compatible. The first step in the procurement process is to contact the Security Management Branch (SMB), Office of Internal Affairs for concurrence that such a system is warranted. If it is determined to be appropriate, further guidance will be provided. Following review of the proposals by the SMB, the system should be procured according to routine procurement methods. Funding for these requisitions is normally the responsibility of the Customs entity occupying the space protected by the system.

A recommendation that it may be in the best interest of the Customs Service to provide for a standard access control system is currently under consideration. This system can be used in all Customs facilities where a card reader access control system is warranted by the level of security determined for a particular facility and the number of personnel expected to use the system.

- b. All vaults and permanent storage rooms (see Part 4.7 – 4.9) must have an approved access control system installed that can be queried to determine historical access to the vault/storage room. SMB should be consulted for

information regarding approved access systems.

c. **Responsibilities**

All Customs Service managers responsible for facility security must make a determination concerning the feasibility of the installation of any of these access control systems, based on the level of security desired and the cost of the system.

PART 6

TECHNICAL STANDARDS

6.5 THIS PART CONTAINS INFORMATION ON BALLISTIC RESISTANT MATERIALS AND A COPY OF THE NATIONAL INSTITUTE OF JUSTICE (NIJ) STANDARD 0108.01, THE INDUSTRY GUIDELINES FOR THESE MATERIALS IS INCLUDED

**6.5 BALLISTIC RESISTANT PROTECTIVE MATERIAL– NIJ STANDARD 0108.01
(SEE ATTACHED)**

All new construction requiring ballistic resistant material must meet or exceed Type III as described in the attached standard.

All Type III-A ballistic resistant material currently in use in Customs facilities is approved for continued use and does not need to be replaced.

If there is ballistic resistant material in use at a Customs facility that does not meet the specifications of Level III-A at a minimum, it must be replaced with Type III material.

National Institute
of Justice

*Technology Assessment
Program*

Ballistic Resistant Protective Materials

NIJ Standard 0108.01

National Institute of Justice

Technology Assessment Program

**Ballistic Resistant
Protective Materials**

NIJ Standard 0108.01

September 1985

ABOUT THE TECHNOLOGY ASSESSMENT PROGRAM

The Technology Assessment Program is sponsored by the Office of Development, Testing, and Dissemination of the National Institute of Justice (NIJ), U.S. Department of Justice. The program responds to the mandate of the Justice System Improvement Act of 1979, which created NIJ and directed it to encourage research and development to improve the criminal justice system and to disseminate the results to Federal, State, and local agencies.

The Technology Assessment Program is an applied research effort that determines the technological needs of justice system agencies, sets minimum performance standards for specific devices, tests commercially available equipment against those standards, and disseminates the standards and the test results to criminal justice agencies nationwide and internationally.

The program operates through:

The *Technology Assessment Program Advisory Council* (TAPAC) consisting of nationally recognized criminal justice practitioners from Federal, State, and local agencies, which assesses technological needs and sets priorities for research programs and items to be evaluated and tested.

The *Law Enforcement Standards Laboratory* (LESL) at the National Bureau of Standards, which develops voluntary national performance standards for compliance testing to ensure that individual items of equipment are suitable for use by criminal justice agencies. The standards are based upon laboratory testing and evaluation of representative samples of each item of equipment to determine the key attributes, develop test methods, and establish minimum performance requirements for each essential attribute. In addition to the highly technical standards, LESL also produces user guides that explain in nontechnical terms the capabilities of available equipment.

The *Technology Assessment Program Information Center* (TAPIC) operated by the International Association of Chiefs of Police (IACP), which supervises a national compliance testing program conducted by independent agencies. The standards developed by LESL serve as performance benchmarks against which commercial equipment is measured. The facilities, personnel, and testing capabilities of the independent laboratories are evaluated by LESL prior to testing each item of equipment, and LESL helps the Information Center staff review and analyze data. Test results are published in Consumer Product Reports designed to help justice system procurement officials make informed purchasing decisions.

Publications issued by the National Institute of Justice, including those of the Technology Assessment Program, are available from the National Criminal Justice Reference Service (NCJRS), which serves as a central information and reference source for the Nation's criminal justice community. For further information, or to register with NCJRS, write to the National Institute of Justice, National Criminal Justice Reference Service, Washington, DC 20531.

**James K. Stewart, Director
National Institute of Justice**

**U.S. DEPARTMENT OF JUSTICE
National Institute of Justice**

James K. Stewart, Director

ACKNOWLEDGMENTS

This standard was formulated by the Law Enforcement Standards Laboratory (LESL) of the National Bureau of Standards under the direction of Daniel E. Frank, Manager, Protective Equipment Program, and Lawrence K. Eliason, Chief of LESL. The technical research was performed by Nicholas J. Calvano of the Automated Production Technology Division. The standard has been reviewed and approved by the Technology Assessment Program Advisory Council and adopted by the International Association of Chiefs of Police (IACP) as an IACP standard.

FOREWORD

This document, NIJ Standard-0108.01, Ballistic Resistant Protective Materials, is an equipment standard developed by the Law Enforcement Standards Laboratory of the National Bureau of Standards. It is produced as part of the Technology Assessment Program of the National Institute of Justice. A brief description of the program appears on the inside front cover.

This standard is a technical document that specifies performance and other requirements equipment should meet to satisfy the needs of criminal justice agencies for high quality service. Purchasers can use the test methods described in this standard to determine whether a particular piece of equipment meets the essential requirements, or they may have the tests conducted on their behalf by a qualified testing laboratory. Procurement officials may also refer to this standard in their purchasing documents and require that equipment offered for purchase meet the requirements. Compliance with the requirements of the standard may be attested to by an independent laboratory or guaranteed by the vendor.

Because this NIJ standard is designed as a procurement aid, it is necessarily highly technical. For those who seek general guidance concerning the selection and application of law enforcement equipment, user guides have also been published. The guides explain in nontechnical language how to select equipment capable of the performance required by an agency.

NIJ standards are subjected to continuing review. Technical comments and recommended revisions are welcome. Please send suggestions to the Program Manager for Standards, National Institute of Justice, U.S. Department of Justice, Washington, DC 20531.

Before citing this or any other NIJ standard in a contract document, users should verify that the most recent edition of the standard is used. Write to: Chief, Law Enforcement Standards Laboratory, National Bureau of Standards, Gaithersburg, MD 20899.

Lester D. Shubin
Program Manager for Standards
National Institute of Justice

NIJ STANDARD FOR BALLISTIC RESISTANT PROTECTIVE MATERIALS

CONTENTS

	Page
Foreword.....	iii
1. Purpose	1
2. Scope and Classification.....	1
3. Definitions	2
4. Requirements	3
4.1 Acceptance Criteria.....	3
4.2 Workmanship	3
4.3 Labeling.....	4
4.4 Ballistic Resistance	5
5. Test Methods.....	5
5.1 Sampling	5
5.2 Test Equipment	6
5.3 Ballistic Resistance Test	6
Appendix A—References	8

COMMONLY USED SYMBOLS AND ABBREVIATIONS

A	ampere	H	henry	nm	nanometer
ac	alternating current	h	hour	No.	number
AM	amplitude modulation	hf	high frequency	o.d.	outside diameter
cd	candela	Hz	hertz (c/s)	Ω	ohm
cm	centimeter	i.d.	inside diameter	p.	page
CP	chemically pure	in	inch	Pa	pascal
c/s	cycle per second	ir	infrared	pe	probable error
d	day	J	joule	pp.	pages
dB	decibel	L	Lambert	ppm	part per million
dc	direct current	L	liter	qt	quart
°C	degree Celsius	lb	pound	rad	radian
°F	degree Fahrenheit	lbf	pound-force	rf	radio frequency
diam	diameter	lbf-in	pound-force inch	rh	relative humidity
emf	electromotive force	lm	lumen	s	second
eq	equation	ln	logarithm (natural)	SD	standard deviation
F	farad	log	logarithm (common)	sec.	section
fc	footcandle	M	molar	SWR	standing wave ratio
fig.	figure	m	meter	uhf	ultrahigh frequency
FM	frequency modulation	min	minute	uv	ultraviolet
ft	foot	mm	millimeter	V	volt
ft/s	foot per second	mph	mile per hour	vhf	very high frequency
g	acceleration	m/s	meter per second	W	watt
g	gram	N	newton	λ	wavelength
gr	grain	N·m	newton meter	wt	weight

area = unit² (e.g., ft², in², etc.); volume = unit³ (e.g., ft³, m³, etc.)

PREFIXES

d	deci (10^{-1})	da	deka (10^1)
c	centi (10^{-2})	h	hecto (10^2)
m	milli (10^{-3})	k	kilo (10^3)
μ	micro (10^{-6})	M	mega (10^6)
n	nano (10^{-9})	G	giga (10^9)
p	pico (10^{-12})	T	tera (10^{12})

COMMON CONVERSIONS

(See ASTM E380)

ft/s × 0.3048000 = m/s	lb × 0.453592 = kg
ft × 0.3048 = m	lbf × 4.448222 = N
ft-lbf × 1.355818 = J	lbf/ft × 14.59390 = N/m
gr × 0.06479891 = g	lbf-in × 0.1129848 = N·m
in × 2.54 = cm	lbf/in ² × 6894.757 = Pa
kWh × 3 600 000 = J	mph × 1.609344 = km/h
	qt × 0.946353 = L

$$\text{Temperature: } (T_{\text{F}} - 32) \times 5/9 = T_{\text{C}}$$

NIJ STANDARD FOR BALLISTIC RESISTANT PROTECTIVE MATERIALS

1. PURPOSE

The purpose of this standard is to establish minimum performance requirements and methods of test for ballistic resistant protective materials. This standard supersedes NIJ Standard-0108.00, Ballistic Resistant Protective Materials, dated December 1981. This revision adds threat level III-A and establishes threat level classifications that are consistent with other NIJ standards for ballistic protection.

2. SCOPE AND CLASSIFICATION

2.1 Scope

This standard is applicable to all ballistic resistant materials (armor) intended to provide protection against gunfire, with the exception of police body armor and ballistic helmets, which are the topic of individual NIJ performance standards [1,2]¹. Many different types of armor are now available that range in ballistic resistance from those designed to protect against small caliber handguns to those designed to protect against high-powered rifles. Ballistic resistant materials are used to fabricate portable ballistic shields, such as a ballistic clipboard for use by a police officer, to provide ballistic protection for fixed structures such as critical control rooms or guard stations, and to provide ballistic protection for the occupants of vehicles. The ballistic resistant materials used to fabricate armor include metals, ceramics, transparent glazing, fabric, and fabric-reinforced plastics; they are used separately or in combination, depending upon the intended threat protection.

The ballistic threat posed by a bullet depends, among other things, on its composition, shape, caliber, mass, and impact velocity. Because of the wide variety of cartridges available in a given caliber, and because of the existence of hand loads, armors that will defeat a standard test round may not defeat other loadings in the same caliber. For example, an armor that prevents penetration by a 357 Magnum test round may or may not defeat a 357 Magnum round with higher velocity. Similarly, for identical striking velocities, nondeforming or armor-piercing rounds pose a significantly greater penetration threat than an equivalent lead core round of the same caliber. The test ammunitions specified in this standard represent common threats to the law enforcement community.

2.2 Classification

Ballistic resistant protective materials covered by this standard are classified into five types, by level of performance.

2.2.1 Type 1 (22 LR; 38 Special)

This armor protects against the standard test rounds as defined in section 5.2.1. It also provides protection against lesser threats such as 12 gauge No. 4 lead shot and most handgun rounds in calibers 25 and 32.

2.2.2 Type II-A (Lower Velocity 357 Magnum; 9 mm)

This armor protects against the standard test rounds as defined in section 5.2.2. It also provides protection against lesser threats such as 12 gauge 00 buckshot, 45 Auto., 38 Special ±P and some other factory loads in caliber 357 Magnum and 9 mm, as well as the threats mentioned in section 2.2.1.

¹ Numbers in brackets refer to the references in appendix A.

2.2.3 Type II (Higher Velocity 357 Magnum; 9 mm)

This armor protects against the standard test rounds as defined in section 5.2.3. It also provides protection against most other factory loads in caliber 357 Magnum and 9 mm, as well as threats mentioned in section 2.2.1 and 2.2.2.

2.2.4 Type III-A (44 Magnum; Submachine Gun 9 mm)

This armor protects against the standard test rounds as defined in section 5.2.4. It also provides protection against most handgun threats as well as the threats mentioned in sections 2.2.1 through 2.2.3.

2.2.5 Type III (High-Powered Rifle)

This armor protects against the standard test round as defined in section 5.2.5. It also provides protection against most lesser threats such as 223 Remington (5.56 mm FMJ), 30 Carbine FMJ, and 12 gauge rifle slug, as well as the threats mentioned in sections 2.2.1 through 2.2.4.

2.2.6 Type IV (Armor-Piercing Rifle)

This armor protects against the standard test round as defined in section 5.2.6. It also provides at least single hit protection against the threats mentioned in sections 2.2.1 through 2.2.5.

2.2.7 Special Type

A purchaser having a special requirement for a level of protection other than one of the above standards should specify the exact test rounds to be used, and indicate that this standard shall govern in all other respects.

3. DEFINITIONS

3.1 Angle of Incidence

The angle between the line of flight of the bullet and the perpendicular to the plane tangent to the point of impact (see fig. 1). Also known as angle of obliquity.

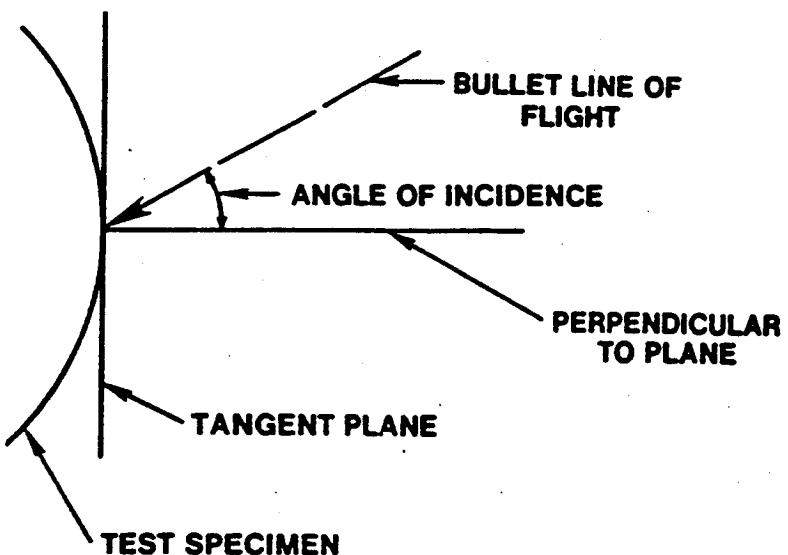


FIGURE 1. *Angle of incidence.*

3.2 Fair Hit

A hit that impacts the ballistic resistant protective material at an angle of incidence no greater than 5°, and is at least 5 cm (2 in) from a prior hit or the edge of the test specimen and at an acceptable velocity as defined in this standard. A bullet that impacts too close to the edge or a prior hit and/or at too high a velocity, but does not penetrate, shall be considered a fair hit for the determination of nonpenetration.

3.3 Full Metal Jacketed (FMJ) Bullet

A bullet made of lead completely covered, except for the base, with copper alloy (approximately 90 copper-10 zinc).

3.4 Jacketed Soft Point (JSP) Bullet

A bullet made of lead completely covered, except for the point, with copper alloy (approximately 90 copper-10 zinc).

3.5 Lead Bullet

A bullet made of lead alloyed with hardening agents.

3.6 Penetration

Perforation of a witness plate by any part of the test specimen or test bullet, as determined by passage of light when held up to a 60-W light bulb.

3.7 Strike Face

The surface of a ballistic resistant protective material designated by the manufacturer as the surface that should be exposed to (face) the weapon threat.

3.8 Semiwadcutter

A bullet shape characterized by a flat nose and a tapered section leading to a cylindrical bullet body with a sharp break where the taper meets the body.

3.9 Witness Plate

A thin sheet of aluminum alloy placed behind a test specimen to determine the potential for an incapacitating injury.

4. REQUIREMENTS

4.1 Acceptance Criteria

A ballistic material satisfies the requirements of this standard if the sample item (see sec. 5.1) meets the requirements of sections 4.2 through 4.4.

4.2 Workmanship

Ballistic resistant protective materials shall be free from dents, blisters, cracks, crazing, chipped or sharp corners, and other evidence of inferior workmanship.

4.3 Labeling

The sample item and each full size panel of ballistic resistance material shall be permanently and legibly labeled and shall include the following information.

- a) Name, designation, or logo of the manufacturer
- b) Type of material, according to section 2 of this standard
- c) Month and year of manufacture
- d) Lot number
- e) Strike face, if any
- f) Certification of compliance with this edition of this standard

Items c and d may be incorporated into a single number, e.g., a serial number.

4.4 Ballistic Resistance

The ballistic resistance of each test specimen of ballistic resistant protective material shall be determined in accordance with section 5.3. The test weapon and ammunition used during this test shall be those specified in table 1 in accordance with the type (threat level rating) specified by the manufacturer (sec. 4.3). Any penetration of the witness plate shall constitute failure.

The ballistic resistance test variables and test requirements are presented in table 1.

TABLE 1. Test summary.

Armor type	Test ammunition	Test variables		Performance requirements		
		Nominal bullet mass	Suggested barrel length	Required bullet velocity	Required fair hits per armor specimen	Permitted penetrations
I	22 LRHV Lead	2.6 g 40 gr	15 to 16.5 cm 6 to 6.5 in	320±12 m/s 1050±40 ft/s	5	0
	38 Special RN Lead	10.2 g 158 gr	15 to 16.5 cm 6 to 6.5 in	259±15 m/s 850±50 ft/s	5	0
II-A	357 Magnum JSP	10.2 g 158 gr	10 to 12 cm 4 to 4.75 in	381±15 m/s 1250±50 ft/s	5	0
	9 mm FMJ	8.0 g 124 gr	10 to 12 cm 4 to 4.75 in	332±12 m/s 1090±40 ft/s	5	0
II	357 Magnum JSP	10.2 g 158 gr	15 to 16.5 cm 6 to 6.5 in	425±15 m/s 1395±50 ft/s	5	0
	9 mm FMJ	8.0 g 124 gr	10 to 12 cm 4 to 4.75 in	358±12 m/s 1175±40 ft/s	5	0
III-A	44 Magnum Lead SWC Gas Checked	15.55 g 240 gr	14 to 16 cm 5.5 to 6.25 in	426±15 m/s 1400±50 ft/s	5	0
	9 mm FMJ	8.0 g 124 gr	24 to 26 cm 9.5 to 10.25 in	426±15 m/s 1400±50 ft/s	5	0
III	7.62 mm (308 Winchester) FMJ	9.7 g 150 gr	56 cm 22 in	838±15 m/s 2750±50 ft/s	5	0
	30-06 AP	10.8 g 166 gr	56 cm 22 in	868±15 m/s 2850±50 ft/s	1	0
Special requirement (see sec. 2.2.7)	*	*	*	*	*	0

*These items must be specified by the user. All of the items must be specified.

Abbreviations:

- AP - Armor Piercing
- FMJ - Full Metal Jacketed
- JSP - Jacketed Soft Point
- LRHV - Long Rifle High Velocity
- RN - Round Nose
- SWC - Semi-Wadcutter

5. TEST METHODS

5.1 Sampling

The test specimen shall be a current production sample of the ballistic resistant material at least 30.5×30.5 cm (12 \times 12 in).

5.2 Test Equipment

It should be noted that hand-loaded ammunition may be required to achieve some of the bullet velocities required in the following sections.

5.2.1 Type I Test Weapons and Ammunition

5.2.1.1 .22 LR

The test weapon may be a .22 caliber handgun or test barrel. The use of a handgun with a 15 to 16.5 cm (6 to 6.5 in) barrel is suggested. Test bullets shall be .22 Long Rifle High Velocity lead, with nominal masses of 2.6 g (40 gr) and measured velocities of 320 ± 12 m (1050 \pm 40 ft) per second.

5.2.1.2 .38 Special

The test weapon may be a .38 Special handgun or test barrel. The use of a handgun with a 15 to 16.5 cm (6 to 6.5 in) barrel is suggested. Test bullets shall be .38 Special round-nose lead, with nominal masses of 10.2 g (158 gr) and measured velocities of 259 ± 15 m (850 \pm 50 ft) per second.

5.2.2 Type II-A Test Weapons and Ammunition

5.2.2.1 Lower Velocity 357 Magnum

The test weapon may be a 357 Magnum handgun or test barrel. The use of a handgun with a 10 to 12 cm (4 to 4.75 in) barrel is suggested. Test bullets shall be 357 Magnum jacketed soft point, with nominal masses of 10.2 g (158 gr) and measured velocities of 381 ± 15 m (1250 \pm 50 ft) per second.

5.2.2.2 Lower Velocity 9 mm

The test weapon may be a 9 mm handgun or test barrel. The use of a handgun with a 10 to 12 cm (4 to 4.75 in) barrel is suggested. Test bullets shall be 9 mm full metal jacketed, with nominal masses of 8.0 g (124 gr) and measured velocities of 332 ± 12 m (1090 \pm 40 ft) per second.

5.2.3 Type II Test Weapons and Ammunition

5.2.3.1 Higher Velocity 357 Magnum

The test weapon may be a 357 Magnum handgun or test barrel. The use of a handgun with a 15 to 16.5 cm (6 to 6.5 in) barrel is suggested. Test bullets shall be 357 Magnum jacketed soft point, with nominal masses of 10.2 g (158 gr) and measured velocities of 425 ± 15 m (1395 \pm 50 ft) per second.

5.2.3.2 Higher Velocity 9 mm

The test weapon may be a 9 mm handgun or test barrel. The use of a handgun with a 10 to 12 cm (4 to 4.75 in) barrel is suggested. Test bullets shall be 9 mm full metal jacketed, with nominal masses of 8.0 g (124 gr) and measured velocities of 358 ± 12 m (1175 \pm 40 ft) per second.

5.2.4 Type III-A Test Weapons and Ammunition

5.2.4.1 .44 Magnum

The test weapon may be a .44 Magnum handgun or test barrel. The use of a handgun with a 14 to 16 cm (5.5 to 6.25 in) barrel is suggested. Test bullets shall be .44 Magnum, lead semiwadcutter with gas checks, nominal masses of 15.55 g (240 gr), and measured velocities of 426 ± 15 m (1400 \pm 50 ft) per second.

5.2.4.2 Submachine Gun (SMG) 9 mm

The test weapon may be a 9 mm SMG or test barrel. The use of a test barrel with a 24 to 26 cm (9.5 to 10.25 in) barrel is suggested. Test bullets shall be 9 mm full metal jacketed, with nominal masses of 8.0 g (124 gr) and measured velocities of 426 ± 15 m (1400±50 ft) per second.

5.2.5 Type III Test Weapon and Ammunition

The test weapon may be a rifle or a test barrel chambered for 7.62 mm (308 Winchester) ammunition. The use of a rifle with a barrel length of 56 cm (22 in) is suggested. Test bullets shall be 7.62 mm full metal jacketed (U.S. military designation M80), with nominal masses of 9.7 g (150 gr) and measured velocities of 838 ± 15 m (2750±50 ft) per second.

5.2.6 Type IV Test Weapon and Ammunition

The test weapon may be a rifle or a test barrel chambered for 30-06 ammunition. The use of a rifle with a barrel length of 56 cm (22 in) is suggested. Test bullets shall be 30 caliber armor piercing (U.S. military designation APM2), with nominal masses of 10.8 g (166 gr) and measured velocities of 868 ± 15 m (2850±50 ft) per second.

5.2.7 Special Type Test Weapon and Ammunition

The test weapon, cartridge type, bullet construction, bullet caliber, bullet mass, and bullet striking velocity must all be specified by the user.

5.2.8 Chronograph

The chronograph shall have a precision of $1 \mu\text{s}$ and an accuracy of $2 \mu\text{s}$. Its triggering devices shall be of either the photoelectric or conductive screen type.

5.2.9 Support Fixture

The test specimen shall be supported by a fixture that permits its position and attitude to be readily adjusted so that it is perpendicular to the line of flight of the bullet at the point of impact.

5.2.10 Witness Plate

The witness plate shall be a 0.5 mm (0.020 in) thick sheet of 2024-T3 or 2024-T4 aluminum alloy and shall be placed and rigidly affixed perpendicular to the line of flight of the bullet and 15 cm (6 in) beyond the armor under test.

5.3 Ballistic Resistance Test

Condition the test specimen at a temperature of 20 to 28 °C (68 to 82 °F) for at least 24 h prior to test.

Place the triggering devices 2 and 3 m (6.6 and 9.8 ft), respectively, from the muzzle of the test weapon as shown in fig. 2, and arrange them so that they define planes perpendicular to the line of flight of the bullet. Measure the distance between them with an accuracy of 1.0 mm (0.04 in). Use the time of flight and distance measurements to calculate the velocity of each test round.

After the specified test weapon has been supported, leveled, and positioned, fire one or more pretest rounds (as needed) through a witness plate to determine the point of impact.

Place the test specimen in the support fixture and position it 5 m (16 ft) from the muzzle of the test weapon. Then position an unperforated witness plate 15 cm (6 in) beyond the test specimen. Fire a test round and record the velocity of the bullet as measured by the chronograph. Examine the witness plate to determine penetration, and examine the specimen to see if the bullet made a fair hit.

If no penetration occurred, reposition the test specimen and repeat the procedure with additional test rounds until the test is completed. Space the hits as evenly as possible so that every portion of the test specimen is subject to test.

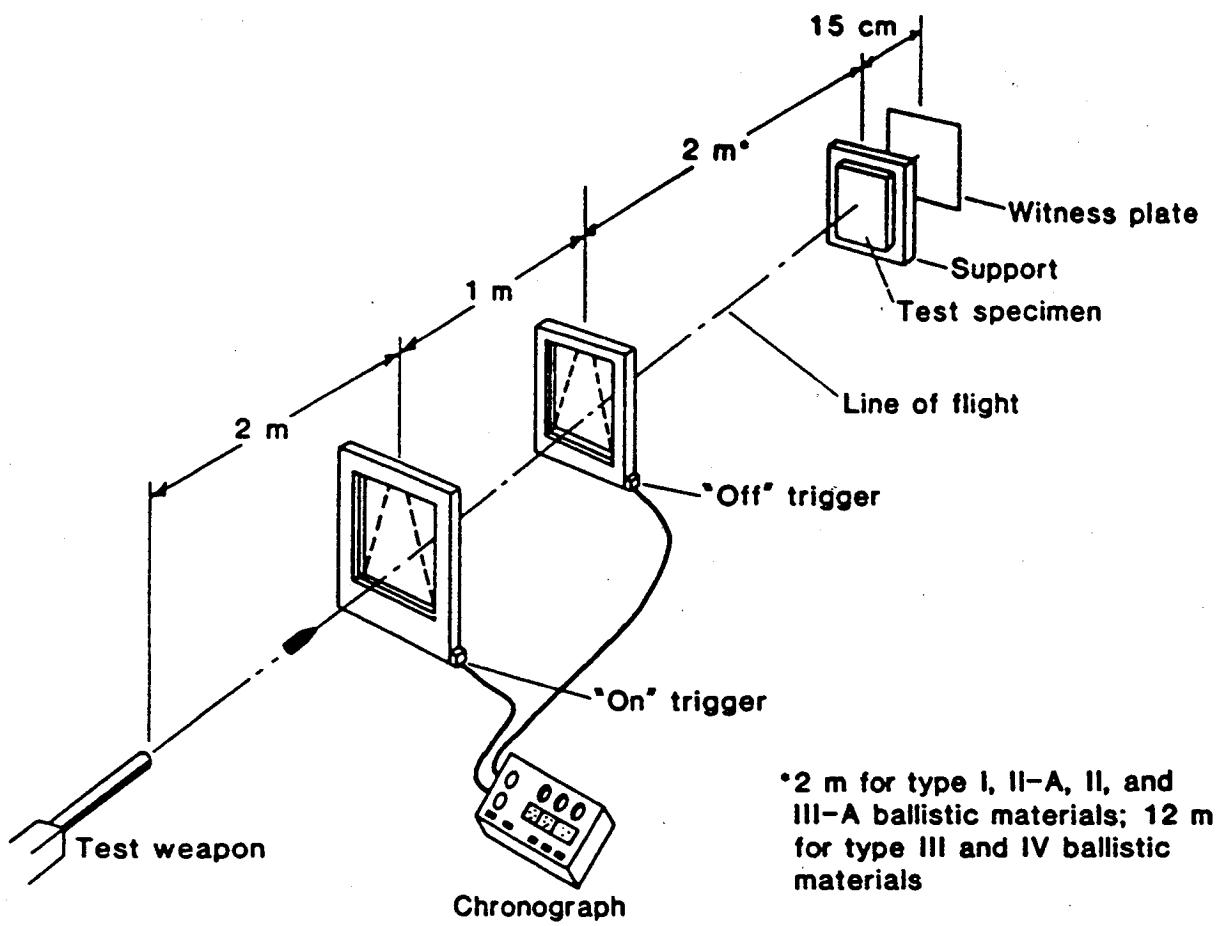


FIGURE 2. *Ballistic test setup.*

APPENDIX A—REFERENCES

- [1] Ballistic resistance of police body armor. NIJ Standard-0101.02. National Institute of Justice, U.S. Department of Justice, Washington, DC 20531.
- [2] Ballistic helmets. NIJ Standard-0106.01. National Institute of Justice, U.S. Department of Justice, Washington, DC 20531; 1981 December.

PART 6
TECHNICAL STANDARDS
6.6 FENCES

6.6 FENCES

a. General

Security fencing is used to economize on the use of security personnel and provides a visible legal statement that entry is not permitted. Fences permit increased protection to a security area and assist in deterring intruders who may be seen attempting to climbing over, under, or cutting through the fence. There are Customs areas that require protective covering materials (e.g. permahedge) to be laced or connected to the fence to limit the visibility of the secured area to perform certain duties on Customs property. Typically, however, perimeter fencing is not laced and provides a clear view of personnel, vehicles, or material in the vicinity of the fence line.

In general, fences (both with and without enhancements) offer delays of less than one minute against intruders. Trained and dedicated intruders can take as little as three to eight seconds to climb over a fence. The height of the fence, or the degree of enhancements used make little difference on this time. Fence material can be easily cut, or climbed over. This includes barbed wire which can be easily be climbed over with the aid of blankets, etc. However, fences do offer some advantage in limiting the amount of tools, contraband, etc., the intruder can readily carry into the secured area.

A simple fence without enhancements will be adequate in most cases to define the site boundary, deter the casual intruder, or support an exterior IDS system. The use of fence enhancements offers the increased appearance of impregnability, but this should be weighted in terms of the increased material and maintenance costs.

b. Chain Link Fencing

- (1) Chain link fencing is the type of structural barrier most commonly used and recommended for security purposes and must enclose all restricted areas. The following fence standards apply:
- (2) Fabric: The standard fence fabric will be coated 9-gauge steel wire mesh chain link. The coating may be zinc or aluminum, or polyvinyl chloride (PVC) over zinc or aluminum. The mesh openings will not be larger than two inches per side and there will be a twisted and barbed selvage at the top and bottom. **The only exception to this specification is fabric used around exterior, stand alone vaults. Fabric used around exterior, stand-alone vaults must be SS RR-F-191/1, Type 1,0135-inch core steel wire with aluminum coating per ASTM A 491. This fabric shall be 10-gauge woven in 3/8-inch diamond mesh.**
- (3) Fabric ties: Only 9-gauge ties with coating compatible with the fabric will

be used.

- (4) Height: The standard height of a security fence is 8-feet. This includes a fabric height of 7-feet, plus a topguard.
- (5) Fencing posts, supports and hardware: All posts, supports, and hardware for security fencing will meet the requirements of Federal Specification RR-F-191J/GEN of 22 July 1981 (see Table 6 attached to this part). A copy of this specification is available from the SMB. All fastening and hinge hardware will be secured in place by peening or welding to allow proper operation of components, but prevent disassembly of fencing or removal of gates. All posts and structural supports will be located on the inner side of the fencing. Posts will be secured into the soil to prevent shifting, sagging or collapse.
- (6) Reinforcement: Taut-reinforcing wires will be woven through the fabric along the top and bottom of the fence for stabilization of the fence fabric.
- (7) Ground clearance: The bottom of the fence fabric must be within two 2-inches of firm soil or buried sufficiently (concrete footings or gravel may be used) in soft soil to compensate for shifting soil.
- (8) Culverts and openings: Culverts under or through a fence will be ten 10-inch pipe, or of clusters of such pipe or equivalent. Openings under or through a fence will be secured with material equal or greater in strength than the overall barrier.
- (9) Fence placement: No fence will be located so that the features of the land (its topography) or structures (buildings, utility tunnels, light and telephone poles, fire escapes, ladders, etc.) defeat its purpose by allowing passage over, around or under the fence. At no time shall U.S. Customs facilities, containing a secured area, use any of the existing perimeter walls of the facility, as a substitute for a complete perimeter fence.
- (10) Topguards: A top guard should be constructed on all perimeter fences and may be added on interior enclosures for additional protection. A top guard is an overhang made of metal. The metal overhang may be constructed of 12-gauge metal posts, barbed wire, or barbed tape, along the top of a fence. The topguard will face outward and upward at approximately a 45-degree angle. Top guard supporting arms will be permanently affixed to the top of fence posts to increase the overall height of the fence at least 1-foot. Three strands of 12-gauge barbed wire, spaced 6 inches apart, may be installed on the supporting arms. The top guard of fencing adjoining gates may range from a vertical height of 18-inches to the normal 45-degree outward protection, but only for sufficient distance along the fence to open the gates adequately.

MIL-HDBK-1013/1A

Table 6
Common Chain Link Fence Materials (MIL-HDBK-1013/10)

COMPONENT	OPTIONS
Specification	Federal Specifications RR-F-191.
Gauge/Material	9-Gauge (3.8-mm) Steel Wire Mesh
Mesh	Less than 2 inches (50-mm) per side
Coating	Zinc coated, aluminum coated, or polyvinyl chloride (PVC) over zinc or aluminum coating
Tension wires	Wire, rail, cable (attached at top or bottom).
Support Posts	Steel pipe formed sections, H-sections, square sections (see Federal Specs RR-F-191/3).
Height with outriggers	8 feet (2.4-m). 7 feet (2.1-m) for AA&E (Arms ammunition and explosives) storage sites only.
Fabric tie-downs	Buried, 2-inch (50-mm) minimum encased in concrete or staked.
Pole Reinforcement	Buried, encased in concrete
Gate Opening	Single and double swing, cantilevered, wheel or overhead-supported.

PART 6

TECHNICAL STANDARDS

6.7 CLOSED CIRCUIT TELEVISION (CCTV)

6.7 CLOSED CIRCUIT TELEVISION (CCTV)

The purpose of CCTV is to provide an additional level of protection against loss, theft or destruction of Customs property.

a. Scope

For the purpose of this part, the scope of CCTV options available at different Customs locations are so vast, and of such a technical nature, that they will not be listed here. All determinations to incorporate the use of CCTV at a Customs facility will be made on a case by case basis. The determination to use CCTV in any construction after the issuance of this handbook, will be made by the physical security specialists at the Security Management Branch, Office of Internal Affairs. Upgrade specifications to current facilities, requiring the use of CCTV, will be the responsibility of the senior Customs official at that facility. The installing vendor can assist in the design/configuration of the CCTV plan. The senior Customs official on site will be responsible to incorporate all of the security requirements outlined in this handbook.

b. Minimum Requirements

Recorded videotapes associated with CCTV systems will be kept for file footage for a period of at least 30 days. A supply of 40 SVHS tapes should be sufficient for this purpose. It is the responsibility of the senior Customs official on site to ensure that the videotapes are changed and to administer to the CCTV system.

PART 6

TECHNICAL STANDARDS

6.8 ACOUSTICAL CONTROL AND SOUND MASKING TECHNIQUES

6.8 ACOUSTICAL CONTROL AND SOUND MASKING TECHNIQUES

a. General

Acoustical protection measures and sound masking systems are designed to protect against being overheard by the casual passerby, not to protect against deliberate interception of audio. The ability of a structure to retain sound within the perimeter is rated using a descriptive value, the Sound Transmission Class (STC).

- (1) The STC rating is a single number rating used to determine the sound barrier performance of walls, ceilings, floors, windows, and doors.
- (2) There are four established Sound Groups, one through four, of which Groups three and four are considered adequate for specific acoustical security requirements for construction.
 - a. Sound Group One - STC of 30 or better. Loud speech can be understood fairly well. Normal speech cannot be easily understood.
 - b. Sound Group Two - STC of 40 or better. Loud speech can be heard, but is hardly intelligible. Normal speech can be heard only faintly, if at all.
 - c. Sound Group Three - STC of 45 or better. Loud speech can be faintly heard, but not understood. Normal speech is unintelligible.
 - d. Sound Group Four - STC of 50 or better. Very loud sounds, such as loud singing, brass musical instruments, or a radio at full volume, can be heard only faintly or not at all.

PART 6
TECHNICAL STANDARDS

6.9 INSPECTIONS AND REPORTS

6.9 INSPECTIONS AND REPORTS

a. Inspections

Headquarters and/or field physical security specialists will make a periodic inspection of all U.S. Customs facilities at least once every three years, to ensure that security is adequate within his or her area of responsibility.

The Office of Internal Affairs shall conduct such inspections as deemed necessary for the purposes of oversight and as requested by management, consistent with operational commitments. Inspections can be announced or unannounced. As it relates to announced inspections, appropriate notification will be made to the facility.

b. Reports

Original inspection reports will be forwarded to the SMB for review and approval. The Assistant Commissioner (Internal Affairs) will issue all reports to the appropriate Assistant Commissioner or other executive. The field physical security specialist will keep a copy of the report in a separate file folder for each facility in his or her region. This copy will be maintained for a period of six years from the date of the last inspection.

c. Physical security inspection report format

The physical security inspection report format will be in Redbook form. There will be a title page under the front cover that will indicate the facility in question, and the U.S. Customs entity in charge of the facility. There will be seven standard paragraphs in every report. The length and scope of the report will vary with every facility, however the standard paragraphs will always be present. They are:

- I. LOCATION**
- II. PERSONNEL CONDUCTING INSPECTION**
- III. DATE OF INSPECTION**
- IV. FACILITY DESCRIPTION**
 - A. MISSION OF FACILITY**
 - B. GENERAL CONSTRUCTION**
 - C. SECURITY LEVEL**
- V. DESCRIPTION OF SECURITY SYSTEMS**
- VI. FINDINGS AND RECOMMENDATIONS**

VII. CONCLUSIONS

PARAGRAPH VII WILL BE FOLLOWED BY AN EXHIBIT SECTION

There will always be exhibits attached to this report. These exhibits may include blue prints, digital pictures of the facility, list of interviewees, access control systems guide/intrusion detection systems guide, or any other pertinent attachments.

In the event of significant deficiencies in existing security protocols, the report will stipulate specific time frames for the implementation of security enhancements necessary to adequately secure the facility. It will be the responsibility of the senior U.S. Customs official to respond in writing, to the recommendations in the report. This written response must be made within 30 days of the receipt of the report, and forwarded via certified return receipt mail to:

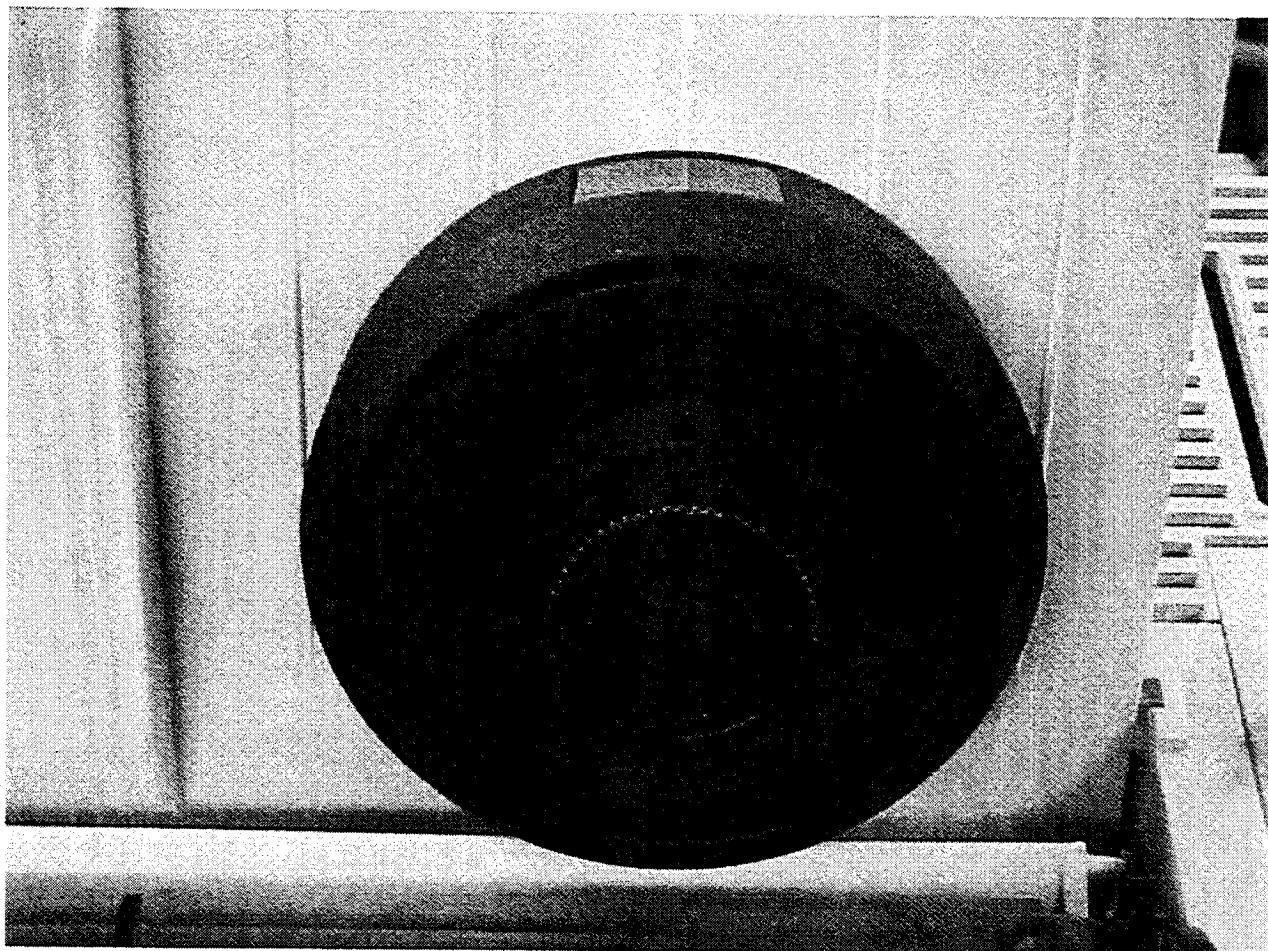
Assistant Commissioner
Office of Internal Affairs
1300 Pennsylvania Avenue, NW
Room 8.3-A
Washington, D.C. 20229

PART 7

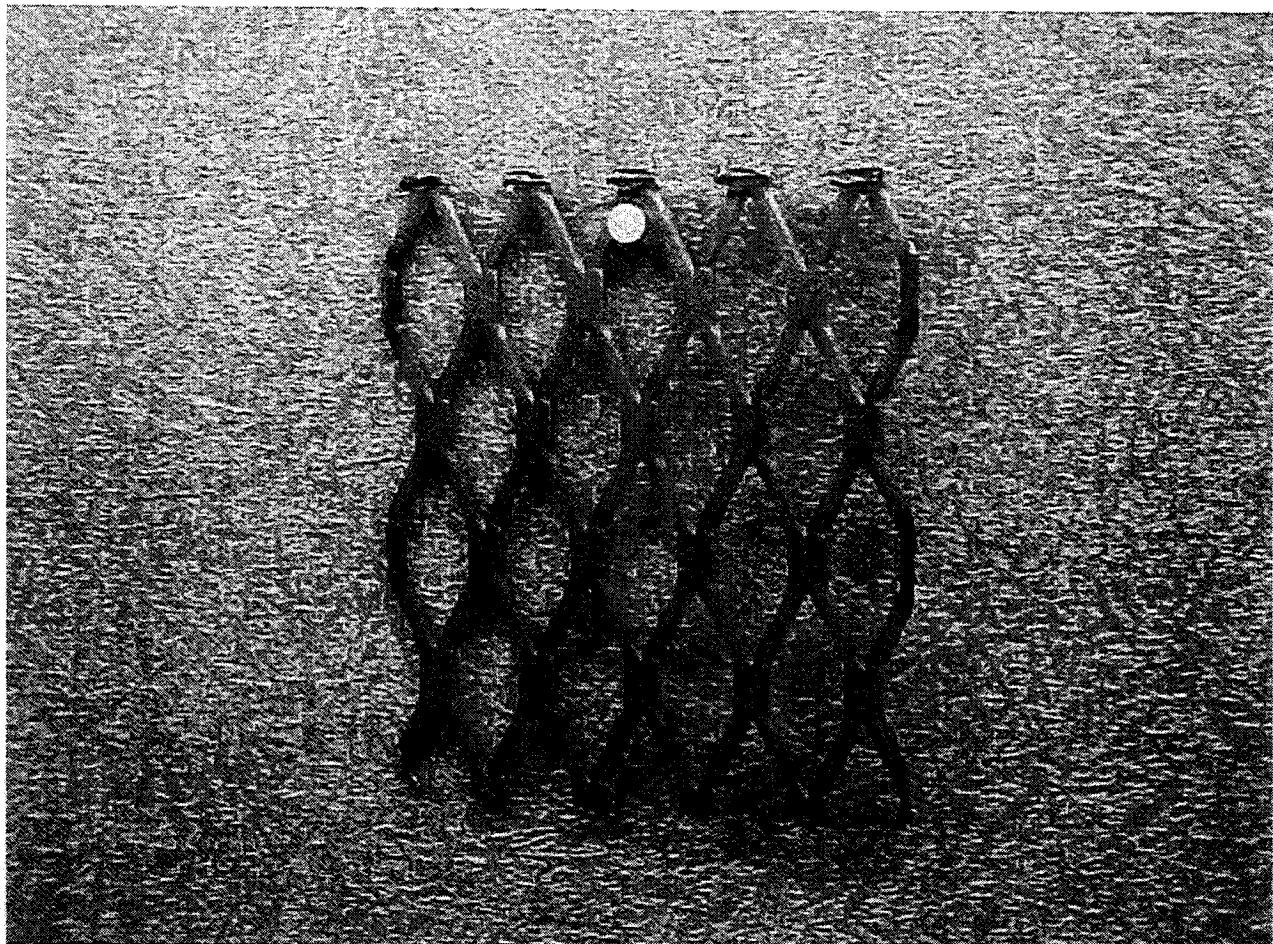
EXHIBITS

- 7.1 MAS – HAMILTON X07 LOCK**
- 7.2 9-GAUGE EXPANDED METAL**
- 7.3 GSA APPROVED CLASS V SECURITY CONTAINER (SAFE)**
- 7.4 GSA APPROVED CLASS VI SECURITY CONTAINER (5 DRAWER SAFE)**
- 7.5 PUSH TO EXIT BUTTON FOR ACCESS CONTROL SYSTEM**
- 7.6 ELECTRIC STRIKE FOR ACCESS CONTROL SYSTEM**
- 7.7 PROXIMITY CARD READER FOR ACCESS CONTROL SYSTEM**
- 7.8 SAMPLE PROXIMITY CARDS**

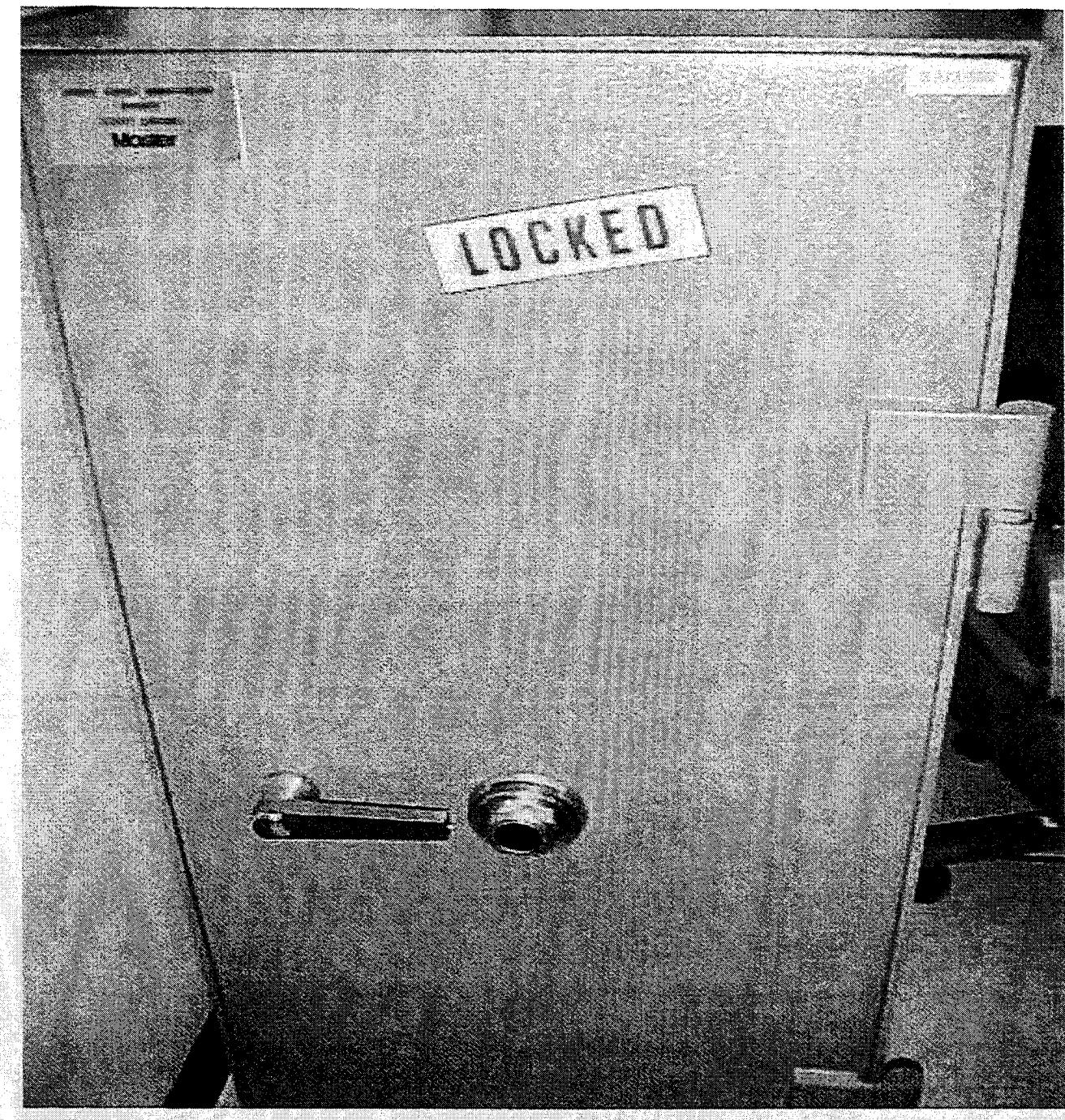
7.1 MAS HAMILTON X07 LOCK



7.2 9-GAUGE EXPANDED METAL



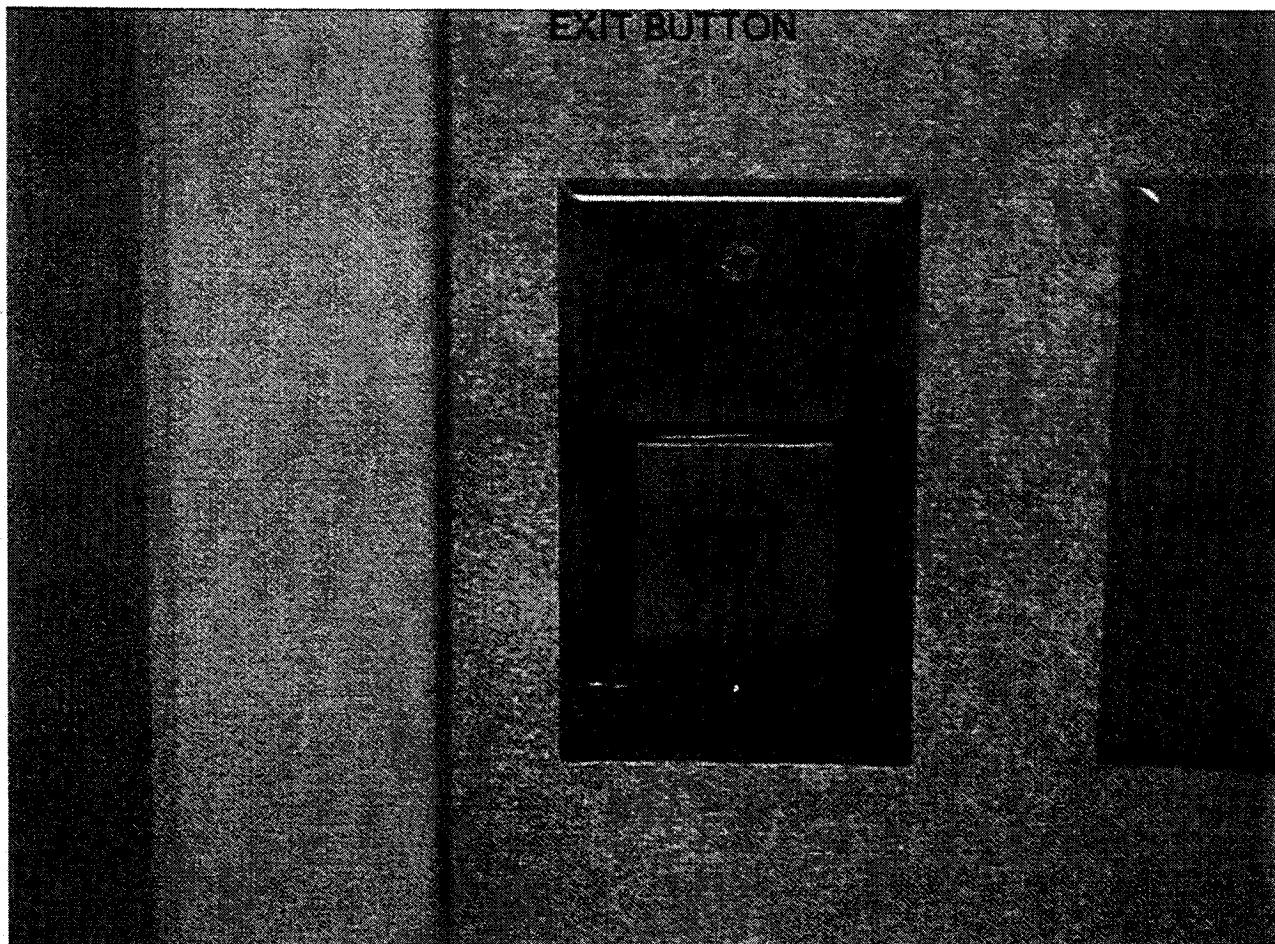
7.3 GSA APPROVED CLASS V SECURITY CONTAINER (SAFE)



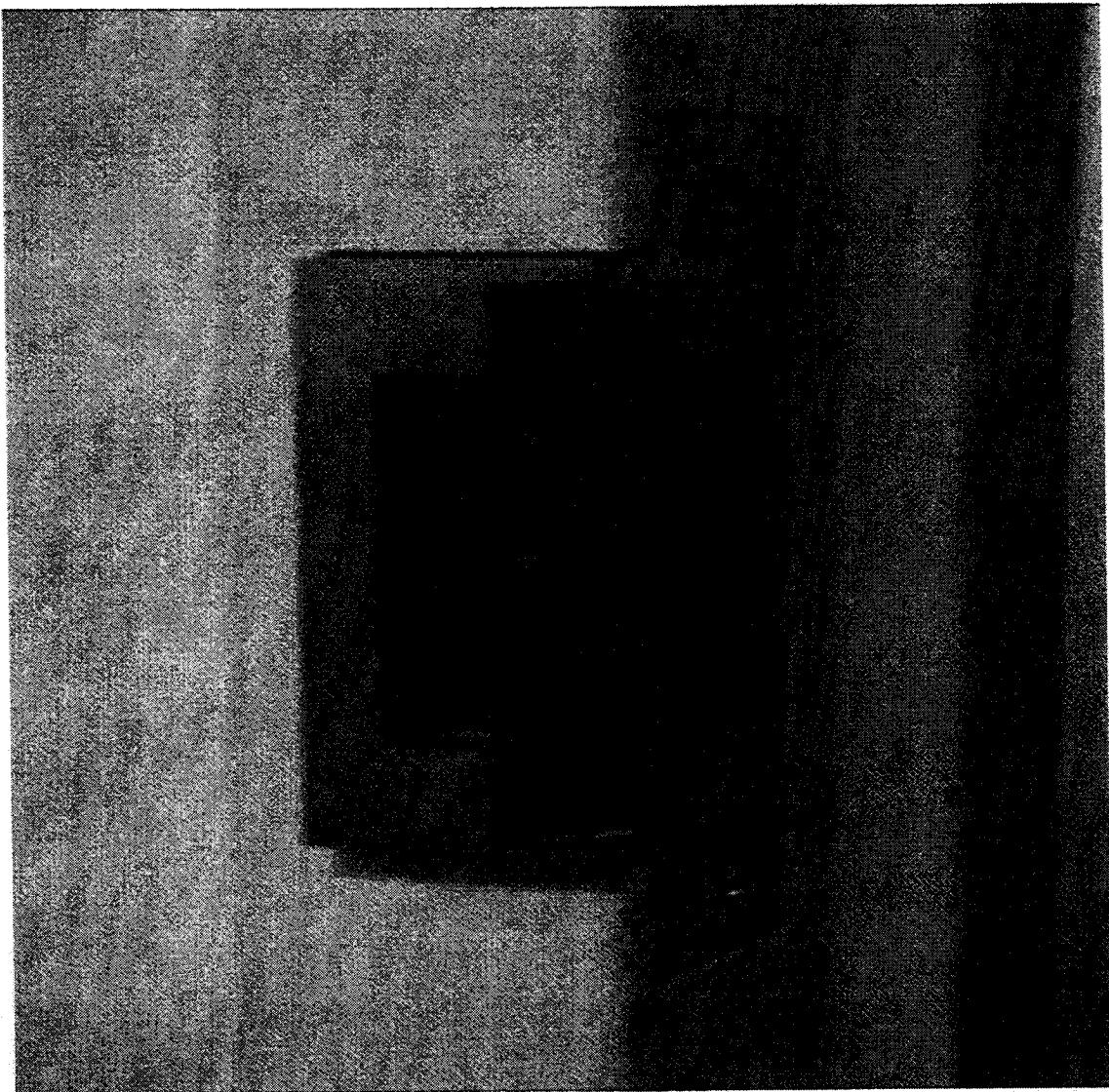
7.4 GSA APPROVED CLASS VI SECURITY CONTAINER (5 DRAWER SAFE)



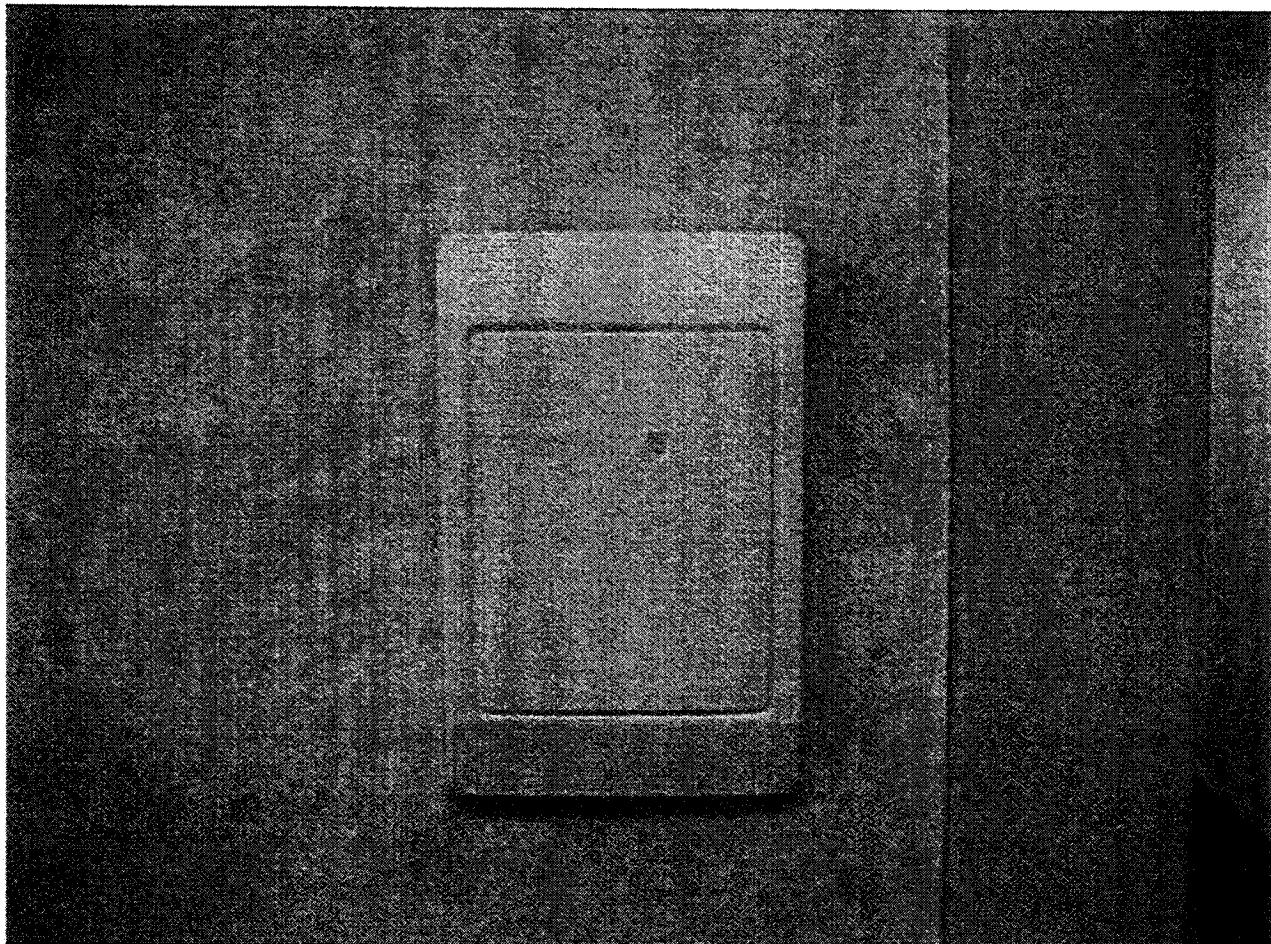
7.5 PUSH TO EXIT BUTTON FOR ACCESS CONTROL SYSTEM



7.6 ELECTRIC STRIKE FOR ACCESS CONTROL SYSTEM



7.7 PROXIMITY CARD READER FOR ACCESS CONTROL SYSTEM



7.8 SAMPLE PROXIMITY CARDS



PART 8
ACRONYMS

8 ACRONYMS

ANSI	American National Standards Institute
ANSI/UL	American National Standards Institute/Underwriters Laboratories
BMSs	Balanced Magnetic Switches
CCTV	Closed Circuit Television
CCD	Charged Coupled Device
GSA	General Services Administration
IDS	Intrusion Detection System
PIR	Passive Infrared (Motion detector)
SCIF	Sensitive Compartmentalized Information Facility
SMB	Security Management Branch
STC	Sound Transmission Class