U.S. Department
of Transportation

United States
Coast Guard

PHYSICAL SECURITY PROGRAM

COMDTINST M5530.1B

U.S. Department of Transportation

United States Coast Guard

Commandant
United States Coast Guard

2100 Second St., S.W.
Washington, DC 20593-0001
Staff Symbol: G-CFI
Phone: (202) 267-1990

COMDTINST M5530.1B
10 MARCH 1999

COMMANDANT INSTRUCTION M5530.1B

Subj: PHYSICAL SECURITY PROGRAM

1. PURPOSE. To provide internal guidance for implementing physical security policies, standards and procedures.

2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanding officers of headquarters units, assistant commandants for directorates, chief counsel and special staff offices at headquarters shall ensure compliance with the provisions of this directive.

3. DISCUSSION. This instruction is the basic Coast Guard directive governing the Physical Security Program. This manual constitutes a rewrite of the previous edition. It has been reformatted and includes substantive changes. Due to the comprehensive changes incorporated, units are encouraged to conduct a thorough review of the contents of this manual.

   a. Applicability to Persons. The provisions of this manual apply to all Coast Guard personnel (military and civilian) and personnel from other agencies when engaged in security activities responsible for the protection of Coast Guard property, information, personnel, and critical infrastructure. These provisions also apply to contractor personnel providing security services to Coast Guard facilities under Coast Guard contract. The physical security of arms, ammunition and explosives (AA&E), as outlined in Chapter 3, is extremely important and shall be given priority when implementing the requirements of this manual.

   b. Internal Use Only. This manual is not intended to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies or personnel, or any person.

   c. Policy Conflict. In cases of apparent conflict between this manual and provisions of statutes or regulations, the latter provisions shall be applied, and Commandant (G-CFI)

DISTRIBUTION – SDL No. 135

	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	5	5	3		3	5	1	5	1	1		1	1	1	1	1	1	1	1		2					
B		20	20	3	3	3		10	3	2	1	1	1	10	2	2	3	10	1	2	2	1	1	1	1	2
C	5	3	1	5	5	5	1		1	1	5	1	2		2	1	5	1	2	1	1	1	1	1	1	1
D	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		1	1
E	1	1					1	1		1	1	1		1	1		1		1	1		1	1	1		
F	1	1	2	1		1		1	1	2	1	1			1	1	1	1	1	1						
G	1	1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION: Small Arms Repair Facility (1), Department of Transportation (M-72) (1)

shall be advised of the apparent conflict at the earliest opportunity. In cases where there is an apparent conflict with current law enforcement practice, Commandant (G-CFI) shall be contacted for further resolution and guidance.

4. DIRECTIVES AFFECTED. Physical Security Manual, COMDTINST M5530.1A dated 15 October 1992, is cancelled (superseded).

5. CHANGES. Changes will be issued as Commandant Notices. Time sensitive amendments will be promulgated by ALDIST/ALCOAST, pending their inclusion in the next change to this manual.

6. REQUEST FOR CHANGES. Suggestions for improvement are welcome at any time. Units and individuals may recommend changes by submitting the Publication Change Request (PCR) form included with this manual. The PCR should be submitted through the local chain of command and cognizant Security Manager. PCRs submitted without your cognizant Security Manager's endorsement, will be returned for their review and comment before processing. The Coast Guard Physical Security Program Manager will assign a serial number to the request and will reply to the originator within 60 days of the request receipt date.

7. FORMS AVAILABILITY. Stock points and other requisition information for the forms identified for use in this manual may be obtained through the Catalog of Forms, COMDTINST M5213.6 (series). Forms include:

a.	SF 700	Security Container Information Form
b.	SF 701	Activity Security Checklist
c.	SF 702	Security Container Check Sheet
d.	CG 3308A	Certificate of Compliance - Private Motor Vehicle Registration
e.	CG 4801	Coast Guard Registration Decal (FUNDED REQUISITION)
f.	CG 5439	Coast Guard Security Identification Badge
g.	CG 5439E	Visitors Security Badge
h.	CG 5448	Coast Guard Security Badge Record

W. H. CAMPBELL
Director of Finance and Procurement

PUBLICATION CHANGE RECOMMENDATION (PCR)

USE THIS PAGE TO MAKE RECOMMENDATIONS FOR THIS PUBLICATION

1. Identify each section you comment on by page number, paragraph, section, or figure.
2. Clearly identify the problem with the publication.
3. State your suggested solution to the problem. Include suggested wording or drawings.
4. Mail to : **Commandant (G-CFI)**
   U.S. Coast Guard **Via: Cognizant Security Manager**
   2100 Second Street, SW
   Washington, D.C. 20593-0001
   ATTN: M5530.1
5. G-CFI will assign a PCR number to the recommendation and will reply to the originator by mail.

COMDTINST M5530.1(series), PHYSICAL SECURITY PROGRAM

PAGE	PARA.	PROBLEM OR REASON FOR CHANGE:

RECOMMENDED CHANGE: (BE SPECIFIC ON HOW YOU THINK IT SHOULD BE WORDED OR APPEAR)

(CONTINUE YOUR REMARKS ON 8.5”x 11 PAPER IF ADDITIONAL SPACE IS NEEDED)

ORIGINATING UNIT ADDRESS:
(INCLUDE UNIT POC , PHONE NO. & EMAIL)

SECURITY MANAGER ENDORSEMENT

[ ] **CONCUR**	[ ] **DO NOT CONCUR**

REMARKS:

DATE:	**TYPED NAME:**	**SIGNATURE:**

CGHQ PCR NO.: PSM-	**ACTION:**	**DATE:**

PLEASE CLOSE WITH TAPE – DO NOT STAPLE – THANK YOU

(FOLD HERE)

U.S. Department
Of Transportation
United States
Coast Guard
2100 Second St. SW
Washington, D.C. 20593-0001

ATTN: M5530.1 (PRC)
Commandant (G-CFI)
U.S. Coast Guard
2100 Second Street, SW
Washington, D.C. 20593-0001

(FOLD HERE)

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE ENTERED	ENTERED BY (Printed name and signature)

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION TO AND MANAGEMENT OF THE PHYSICAL SECURITY PROGRAM

A. General 1-1
B. Responsibilities 1-1
C. Qualifications and Assignment of Security Personnel 1-1
D. Duties and Responsibilities 1-2
1. Area & district security managers 1-2
2. Command security officers 1-4
E. Waivers and Exceptions 1-4
F. Physical Security Plans 1-6

CHAPTER 2 PHYSICAL PROTECTION MEASURES

A. General 2-1
B. Designation of Restricted Areas 2-1
1. Policy 2-1
2. Restricted Areas 2-2
a. General 2-2
b. Definitions 2-2
(1) Exclusion Area 2-2
(2) Limited Area 2-2
(3) Controlled Area 2-3
c. Types 2-3
d. Minimum Security Measures Required for Restricted Areas 2-4
(1) Exclusion Areas 2-4
(2) Limited Areas 2-5
(3) Controlled Areas 2-6
e. Inspections 2-6
3. Non-Restricted Areas 2-6
C. Physical Barriers 2-7
1. General 2-7
2. Purpose 2-7
3. Types 2-8
a. Natural 2-8
b. Structural 2-8
4. General Considerations 2-8
5. Fences 2-9
a. Chain Link Fencing 2-9
(1) Fabric 2-9
(2) Fabric Ties 2-9

(3) Height 2-9
(4) Fencing Posts, Supports and Hardware 2-9
(5) Reinforcement 2-9
(6) Ground Clearance 2-10
(7) Culverts and Openings 2-10
(8) Fence Placement 2-10
(9) Top Guards 2-10
(10) Barriers 2-10
b. Alternative Fencing 2-10
c. Other Fencing 2-10
6. Walls 2-11
7. Temporary Barriers 2-11
8. Clear Zones 2-11
9. Patrol Roads 2-12
10. Inspection of Barriers 2-12
11. Perimeter Openings 2-12
12. Gates 2-12
a. Number and Location 2-12
b. Inspection 2-12
c. Pedestrian Gates 2-13
d. Vehicular Gates 2-13
13. Doors, Windows, Skylights and Other Openings 2-13
14. Sewers, Culverts and Other Utility Openings 2-13
15. Utility Poles, Signboards and Trees 2-13
16. Signs and Posting of Boundaries 2-14
a. Classified Space Restricted Areas 2-14
b. Other Restricted Areas 2-14
c. Restricted Area Perimeters 2-14
d. Non-restricted Areas 2-15
e. Government Property Boundaries 2-15
D. Protective Lighting 2-16
1. General 2-16
2. Principles and Guidelines 2-16
3. Types 2-17
a. Continuous 2-17
(1) Glare Projection 2-17
(2) Controlled 2-17
b. Standby 2-17
c. Movable 2-17
d. Emergency 2-17
4. Lighting Concepts 2-18
a. Direct Illumination 2-18
b. Indirect Illumination 2-18
c. Intermittent Lighting 2-18
d. Responsive Area Illumination 2-18

5. Protective Lighting Parameters 2-18
6. Minimum Standards 2-19
7. Emergency Power 2-19
8. Additional Protection 2-19
a. Wiring System 2-19
b. Controls and Switches 2-20
E. Intrusion Detection Systems 2-20
1. General 2-20
2. Planning and Design Considerations 2-20
3. Characteristics 2-21
4. Security Standards 2-21
5. Principles of Operation 2-22
a. Breaking an Electrical Circuit 2-22
(1) General 2-22
(2) Advantages 2-22
(3) Disadvantages 2-22
b. Interruption of a Light Beam 2-23
(1) General 2-23
(2) Advantages 2-23
(3) Disadvantages 2-24
c. Detection of Sound 2-24
(1) General 2-24
(2) Advantages 2-24
(3) Disadvantages 2-24
d. Detection of Vibration 2-24
(1) General 2-24
(2) Advantages 2-25
(3) Disadvantages 2-25
e. Detection of Motion 2-25
(1) Ultrasonic Systems 2-25
(a) Advantages 2-25
(b) Disadvantages 2-26
(2) Microwave Systems 2-26
(a) Advantages 2-26
(b) Disadvantages 2-26
f. Detection of Change in Capacitance Due to Penetration of an Electrostatic Field 2-26
(1) General 2-26
(2) Advantages 2-27
(3) Disadvantages 2-27
6. Maintenance 2-27
7. Monitoring 2-28
8. Testing 2-29
(1) Motion Detection 2-30
(2) Door Switches 2-30

(3) Capacitance Alarm 2-30
(4) Vibration Detection 2-30
(5) Other 2-30
9. IDS Access Codes 2-31
F. Key and Lock Control 2-31
1. Purpose 2-31
2. General 2-31
3. Key Types 2-33
a. Control Keys 2-33
b. Grand Master Keys 2-33
c. Master Keys 2-33
d. Operating Keys 2-33
e. Special Keyed Alike 2-33
f. Special Keyed Different 2-33
g. Duplicate Keys 2-33
h. Reserve Locks and Keys 2-33
4. Security and Control Measures 2-34
5. Control of Grand Master, Master and Control Keys 2-35
6. Loss of Keys 2-36
G. Security Containers 2-36
H. Visitor Control 2-37

EXHIBIT 2-1 Excerpt from Title 18 U.S.C. 1382 2-39
2-2 Master Key Systems 2-40
2-3 Key Repository Index 2-42
2-4 Key Control Register 2-43

CHAPTER 3 PHYSICAL SECURITY OF ARMS, AMMUNITION AND EXPLOSIVES

A. Purpose 3-1
B. Discussion 3-1
C. Cost Reduction Measures 3-1
D. Waivers and Exceptions 3-2
E. Physical Security Objectives 3-2
F. Physical Security Planning 3-2
1. Background 3-2
2. Plans Documentation and Review 3-2
3. Coordination and Liaison 3-3
G. Security Risk Categories 3-3
1. Arms 3-3
a. Category I 3-3
b. Category II 3-3
c. Category III 3-4
d. Category IV 3-4
2. Ammunition and Explosives (A&E) 3-4

		a. Category I	3-4
		b. Category II	3-4
		c. Category III	3-5
		d. Category IV	3-5
H.	Accountability		3-5
I.	Access Control		3-6
J.	AA&E Key Control		3-6
K.	Intrusion Detection Systems		3-7
	1.	General	3-7
	2.	Security Telephone Systems	3-7
L.	Security and Police Forces		3-8
M.	Restricted Area Designation		3-8
	1.	Personnel and Vehicle Movement Control	3-8
	2.	Removal from Secure Storage	3-9
N.	Fencing		3-9
O.	Lighting		3-9
P.	Arms Storage Requirements		3-9
	1.	Policy	3-9
	2.	Containers	3-10
	3.	Arms Racks	3-10
	4.	Exception	3-10
	5.	Storage in Private Residences	3-11
Q.	Ammunition and Explosives (A&E) Storage Requirements		3-12
	1.	Policy	3-12
	2.	Security Standards	3-12
	3.	Exception	3-12
R.	Armory Construction Specifications		3-12
	1.	Walls	3-12
	2.	Ceilings and Roofs	3-13
	3.	Floors	3-13
	4.	Doors	3-13
	5.	Hinges	3-14
	6.	Windows and Other Openings	3-14
S.	Weapons Space Specifications		3-14
	1.	Walls	3-15
	2.	Ceilings and Floors	3-15
	3.	Doors	3-15
	4.	Locks	3-15
	5.	Hinges	3-15
	6.	Windows and Other Openings	3-15
	7.	Intrusion Detection System	3-15
T.	Shipboard Doors/Hatches		3-16
U.	Arms, Ammunition and Explosives Shipments		3-16

CHAPTER 4 TECHNICAL SECURITY COUNTERMEASURES (TSCM)

A. General 4-1
B. Purpose 4-1
C. Background 4-1
D. Policy 4-2
E. Discussion 4-2
1. Selection of Spaces Requiring Support 4-2
a. Qualifying Spaces/Facilities 4-2
b. Conferences 4-2
c. Flag Offices/Residences 4-3
d. New/Renovated Facilities 4-3
e. Ships/Aircraft 4-3
2. Recurring Support 4-3
3. Operational Security (OPSEC) 4-3
F. Finds 4-4
G. Support; (4. Survey Request Procedure) 4-4
H. Classification Guidance 4-6
I. TSCM Reports 4-6

CHAPTER 5 TERRORIST THREAT CONDITIONS (THREATCONS)

A. Purpose 5-1
B. Responsibilities 5-1
C. Threat Analysis and Assessment Factors 5-2
1. Existence 5-2
2. Capability 5-2
3. Intentions 5-3
4. History 5-3
5. Targeting 5-3
6. Security Environment 5-3
D. Levels of Threat 5-3
1. Negligible 5-3
2. Low 5-3
3. Medium 5-3
4. High 5-3
5. Critical 5-3
E. Threat Condition (THREATCON) Definitions 5-4
1. THREATCON NORMAL 5-4
2. THREATCON ALPHA 5-4
3. THREATCON BRAVO 5-4
4. THREATCON CHARLIE 5-4
5. THREATCON DELTA 5-4

F. Suggested Protective Measures 5-4
1. General 5-4
a. THREATCON ALPHA Measures 5-5
b. THREATCON BRAVO Measures 5-6
c. THREATCON CHARLIE Measures 5-7
d. THREATCON DELTA Measures 5-8
2. Shipboard Terrorist THREATCON Measures 5-9
(1) THREATCON ALPHA Measures 5-10
(2) THREATCON BRAVO Measures 5-12
(3) THREATCON CHARLIE Measures 5-16
(4) THREATCON DELTA Measures 5-18
3. Aviation Facility Terrorist THREATCON Measures 5-18
(1) THREATCON ALPHA/BRAVO Measures 5-20
(2) THREATCON CHARLIE Measures 5-21
(3) THREATCON DELTA Measures 5-22

CHAPTER 6 FUNDS FACILITIES AND STORAGE

A. Applicability 6-1
B. Responsibilities 6-1
1. Command 6-1
2. Area and District Security Managers 6-2
C. Consideration Factors for Funds Site Selection 6-2
D. Cost Reduction Measures 6-3
E. Funds Storage Containers 6-3
1. Storage Container Limitations 6-3
a. Under $2,000 6-4
b. $2,000 - $9,999 6-4
c. $10,000 - $49,999 6-4
d. $50,000 or More 6-4
2. Storage Container Categories 6-4
a. Burglary Resistant Safes 6-4
b. Security Containers 6-4
3. Storage Container Requirements 6-5
4. Storage Container Records 6-5
a. Standard Form 700 6-6
b. Standard Form 701 6-6
c. Standard Form 702 6-6
F. Money Packets (for ashore units) 6-6
G. Keys and Combinations 6-7
H. Protective Lighting 6-8
I. Intrusion Detection Systems 6-8
1. Requirements 6-8
2. Selection 6-8
3. Essential Characteristics 6-8

J. Escort Procedures 6-8
K. Penalty Postage Meters 6-9
1. Accounting Responsibilities 6-9
2. Custody of Meter Keys 6-10
3. Meter Security 6-10
L. Government Credit Cards 6-10
M. Travelers Checks 6-11
N. Robbery Prevention and Planning 6-11

CHAPTER 7 PRIVATE MOTOR VEHICLE ACCESS CONTROL PROGRAM

A. Purpose 7-1
B. General 7-1
C. Policy 7-1
D. Privately Owned Vehicle Access Registration 7-2
1. Objectives 7-2
2. Privileges 7-3
a. Personnel Eligibility 7-3
b. Vehicle Eligibility 7-4
3. Deviations 7-4
4. Requirements 7-5
5. Procedures for Completing CG-3308A 7-6
6. Distribution of CG-3308A 7-6
7. Transfer out of Issuing Authority's AOR 7-6
8. Temporary Access/Visitor Passes 7-6
9. Decal Display 7-7
10. Termination of Access 7-8
E. Motorcycle Access Registration Requirements 7-8
F. Security and Accountability 7-9
1. Accountability 7-9
2. Storage 7-9
3. Responsibilities 7-9
G. Availability of Forms 7-9
H. Decal and Tab Description 7-9
1. Basic Decal 7-10
2. Expiration Tab 7-10

EXHIBIT 7-1 Certificate of Compliance - Private Motor Vehicle Registration, CG-3308A 7-11
7-2 Coast Guard Registration Decal, CG-4801 7-12
7-3 List of Stock Numbers 7-13

CHAPTER 8 SECURITY IDENTIFICATION BADGE SYSTEM

A. Purpose 8-1

B. General 8-1
1. Information Security 8-1
2. Physical Security 8-1
C. Policy 8-1
D. Format/Characteristics 8-2
E. Procedures 8-2
F. Security and Accountability 8-3
1. Accountability 8-3
2. Storage 8-3
3. Responsibilities 8-3

EXHIBIT 8-1 Security Identification Badge Record, CG-5448 8-4
8-2 Privacy Act Statement 8-5
8-3 Security Identification Badge, CG-5439 (series) 8-6

CHAPTER 9 LOSS PREVENTION

A. Purpose 9-1
B. Property Management 9-1
C. Responsibilities 9-1
D. Loss Reporting Procedures 9-1
E. Pilferage 9-3
F. Personal Need or Desire 9-3
G. Inventory Control 9-3
H. Inspections 9-4

EXHIBIT 9-1 Sample Message Report of Loss of Government Property 9-5

CHAPTER 10 SECURITY AND POLICE FORCES

A. General 10-1
B. Purpose 10-1
C. Responsibilities 10-1
D. Categories 10-2
1. Security Guards 10-2
2. Police 10-2
3. Foreign Security and Police Forces 10-2
E. Establishment 10-2
F. Functions 10-3
G. Authority 10-4
H. Jurisdiction 10-6
1. General 10-6
2. Types 10-6
a. Exclusive Federal Jurisdiction 10-6
b. Concurrent Federal Jurisdiction 10-7

c. Proprietary Jurisdiction 10-7
3. Territorial 10-7
4. Assistance to Local Authorities 10-7
5. Posse Comitatus Act 10-8
I. Size 10-8
J. Security and Police Force Standing Orders 10-9
K. Personnel Selection 10-9
L. Personal Supervision 10-11
M. Indirect Supervision 10-11
1. Recorded Tour Systems 10-11
2. Portable Radios or Call-in Boxes 10-11
N. Determination of Posts 10-11
O. Types of Posts 10-12
1. Fixed 10-12
2. Mobile 10-12
3. Administrative 10-12
P. Post Requirements and Considerations 10-12
1. Gates 10-12
2. Perimeter 10-12
3. Area Posts 10-12
4. Motorized Patrols 10-13
5. Funds Escorts 10-13
6. Visitor Escorts
10-13
Q. Determination of Strength 10-13
R. Estimating Security and Police Force Strength Requirements 10-14
S. Emergency Planning and Auxiliary Security/Police Forces. 10-14
T. Security Investigations for Security and Police Forces. 10-15
U. Uniforms 10-15
1. General 10-15
2. Headgear 10-16
3. Footwear 10-16
4. Uniform Insignia 10-17
5. Outer Garments 10-17
6. Coveralls 10-17
7. Body Armor 10-17
8. Bicycle Patrols 10-18
V. Patches, Badges and Credentials 10-18
W. Training 10-19
X. Equipment 10-20
1. General 10-20
2. Carriage of Equipment 10-20
3. Handcuffs 10-21
4. Flashlights 10-21
5. Holsters 10-21

	Y.	Weapons		10-22
		1.	General	10-22
		2.	Reporting Requirements	10-22
		3.	Carriage of Weapons by USCG Police Forces	10-23
		4.	Impact Weapons	10-24
		5.	Chemical Irritants	10-24
		6.	Standard Service Weapons	10-25
			a. Qualifications for Carriage	10-25
			b. Standard Service Sidearm	10-25
			c. Shotguns	10-26
			d. M-16 and other Shoulder Fired Weapons	10-26
	Z.	Use of Force		10-26
	AA.	Searches of Persons		10-27
		1.	General	10-27
		2.	Pre-Arrest Body Search	10-28
			a. Frisk	10-28
			b. Other Body Searches	10-29
			c. Persons not Arrested, but Detained by USCG	10-29
		3.	Post-Arrest Body Search	10-30
			a. Field Search/Search Incident to Arrest	10-30
			b. Strip Search	10-31
			c. Body Cavity Search	10-32
		4.	Searches by Members of the Opposite Sex	10-33
	BB.	Patrol Vehicle Standards		10-33
	CC.	Emergency Vehicle Response		10-35
	DD.	Communications System		10-36
	EE.	Evidence Procedures		10-37
	FF.	Security and Police Force Records Management		10-38
		1.	General	10-38
		2.	Purpose	10-39
		3.	Retention Requirements/Limitations	10-39
			a. List of Records	10-39
			b. Extended Records Retention	10-43
EXHIBIT	10-1	Security Badge and Patch Design Specifications		10-45
	10-2	Security and Police Force Training		10-46
	10-3	Security and Police Force Use of Deadly Force Summary		10-48

CHAPTER 11 STORAGE OF CONTROLLED MEDICAL SUBSTANCES

A.	Purpose	11-1
B.	Storage Requirements	11-1

CHAPTER 12 BOMB THREATS AND INCIDENTS

	A.	Purpose	12-1
	B.	General	12-1
	C.	Bomb Threats and Physical Security Planning	12-1
		1. Bombs	12-1
		2. Bomb Threats	12-1
		a. Telephonic Bomb Threat	12-2
		b. Written Bomb Threat	12-2
		c. Letter/Package Bombs	12-2
		3. Why Prepare	12-2
		4. How to Prepare	12-3
		5. Security Against Bomb Incidents	12-4
	D.	Responding to Telephonic Bomb Threats	12-7
	E.	Countermeasures	12-9
	F.	Decision Time (Ignore/Search/Evacuate)	12-10
	G.	Conducting a Search	12-11
		1. General	12-11
		2. Search Teams	12-11
		3. Search Techniques	12-12
		(1) First Room-searching Sweep	12-13
		(2) Second Room-searching Sweep	12-13
		(3) Third Room-searching Sweep	12-13
		(4) Fourth Room-searching Sweep	12-14
		4. Vehicle Bomb Search	12-14
	H.	Suspicious Object Located	12-14
	I.	Evacuation Procedures	12-15
	J.	Handling the News Media	12-16
	K.	Training	12-16
	L.	Summary	12-17
EXHIBIT	12-1	Telephonic Bomb Threat Report	12-19
	12-2	Letter and Package Bomb Recognition	12-21
	12-3	Bomb Incident Plan	12-24
	12-4	Bomb Threat Command Center Plan	12-25
	12-5	Vehicle Bomb Search Procedure	12-26

ENCLOSURES

(1) Glossary of Terms and Acronyms
(2) Physical Security Plan
(3) Physical Security Checklist
(4) Preliminary Information for TSCM Security Review
(5) Approved Locking Devices for AA&E Storage

(6) Use of Force and General Weapons Policy for Coast Guard Security and Police Forces
(7) References

INDEX

Chapter 1 INTRODUCTION TO AND MANAGEMENT OF THE PHYSICAL SECURITY PROGRAM

A. General.

1. This chapter establishes policy and guidance for planning the physical security of individual units. Every individual in the Coast Guard is directly responsible for supporting the Coast Guard Physical Security Program.

2. For the purpose of this manual, commanding officer includes commanders and officers-in-charge. Cognizant security manager (SECMGR) includes area and district SECMGRs. Major units include Headquarters, groups, air stations, Marine Safety Offices (MSOs), area and district staffs, integrated support commands (ISCs), communications stations, and all cutters 180' and larger.

3. Recommendations for changes to this manual are encouraged and shall be forwarded to Commandant (G-CFI), the Physical Security Program Manager, via the cognizant Area or District Security Manager (SECMGR). Comments or proposed changes shall be specific and include justification or documentation necessary to ensure proper evaluation.

B. Responsibilities.

1. Commandant (G-CFI) serves as the Director of Coast Guard Security and manages the overall USCG Security Program; monitors and oversees all elements of the Coast Guard Security Program and the protection of the critical infrastructure of the Coast Guard; manages and evaluates Security and Counterintelligence operations; develops and transmits policy, procedures, standards, and guidelines for the Physical Security and Antiterrorism/Force Protection Programs; and provides programmatic guidance and direction.

2. The physical security requirements in this manual do not apply to Communications Security (COMSEC) Facilities which is covered by Communication Security Material System Policy and Procedures Manual (CMS-1) or Sensitive Compartmented Information Facilities (SCIF) which is covered by Director of Central Intelligence Directive 1/21 (DCID 1/21).

C. Qualifications and Assignment of Security Personnel.

1. The Area SECMGR shall provide support to area and maintenance and logistics command (MLC) units, and the District SECMGR shall provide support to district units and headquarters units geographically located within a district. The Area or District SECMGR shall also monitor and oversee all elements of the Coast Guard Security Program.

a. The Area or District SECMGR shall be a commissioned officer, chief warrant officer, or a civilian employee (GS-13 or above).

b. The Area or District SECMGR shall be the subject of a Single Scope Background Investigation (SSBI) and possess a final TOP SECRET (TS) clearance.

c. The Area or District SECMGR shall be certified by the issuance of credentials by Commandant (G-CFI).

2. Commanding Officers of major units shall designate a Command Security Officer (CSO) to manage the unit security program and to provide unit or staff level security support.

a. The CSO shall be a commissioned officer, chief warrant officer or civilian employee (GS-9 or above), be the subject of a favorable NAC, and possess a final SECRET clearance, (SSBI if TS clearance is required).

b. The designation of CSO shall be made by the unit in writing to the cognizant SECMGR.

c. Loran-C Regional Managers shall serve as the CSO for Loran Stations under their control, and obtain assistance from the cognizant SECMGR.

d. Units which are not under the administrative control of a major unit, e.g., group, shall designate their own CSO and obtain assistance from the cognizant SECMGR.

3. Classified Material Control Officers (CMCO) are required at any unit which initiates, receives or processes classified material. Classified Information Management Program, COMDTINST M5510.23 (series), contains specific policy and guidance for CMCOs.

4. Automated Information Systems (AIS) Security Manual, COMDTINST M5500.13 (series), contains information on qualifications, assignment and responsibilities of the Automated Data Processing Security Officer (ADPSO).

D. Duties and Responsibilities.

1. Area and district security managers (SECMGR). Due to the oversight responsibilities of the Area and District SECMGRs, they shall not be assigned duties or responsibilities of the CSO, CMCO, Top Secret Control Officer (TSCO), Special Security Officer (SSO) (or Assistant), Communications Security (COMSEC) Inspector, ADPSO, Automated Data Processing Systems Security Officer (ADPSSO), Network Security Officer (NSO), or any duties involving

control or accounting of classified or sensitive material. The assignment of non-security related duties and responsibilities which interfere with the area or district SECMGRs ability to perform the duties and responsibilities stated below, are also prohibited. The Area and District SECMGR shall:

a. Monitor and oversee the implementation of security programs, plans, policies, procedures and security and police force operations, as contained in internal security related instructions, for all area or district commands and units, district SECMGRs will monitor and oversee headquarters units geographically located within their district, and provide advice and guidance when required, to ensure the critical infrastructure of the Coast Guard is adequately protected. Maintain liaison with the cognizant ADPSO and CSO and provide assistance when appropriate.

b. Conduct a biennial evaluation of major commands and units (SECMGRs will evaluate all units geographically located within their AOR), and forward a copy of the written evaluation to Commandant (G-CFI).

c. Serve as the security advisor to the Area or District Commander.

d. Ensure that an active, comprehensive security awareness, training and education program for the protection of classified information, assets and personnel is in place throughout the area or district, and exercise oversight of this program.

e. Develop and promulgate additional guidance and procedures for the protection of classified information, Coast Guard assets and personnel throughout the area or district.

f. Maintain liaison with the Area or District Public Affairs Officer to ensure that proposed public releases that could possibly contain classified or sensitive information are referred for review.

g. Review instances of administrative security discrepancies; review and close cases of possible compromises of classified information , government property losses, and missing controlled substances. Ensure they are recorded and when necessary, direct that they are thoroughly investigated by the responsible unit or conduct their own security investigation.

h. Grant waivers and endorse exceptions from security requirements in accordance with paragraph E of this chapter.

i. Exercise the physical security and force protection plan and terrorism incident response plan to determine their ability to protect personnel and

assets against terrorist attack and the consequences of a successful terrorist attack.

2. Command Security Officers (CSO). The CSO shall:

a. Become familiar with the requirements of all security related Commandant, Area, and District instructions and be responsible for all subordinate units under their cognizance.

b. Promulgate and implement security programs, policies, plans and procedures, as required by all applicable security instructions, and assist their subordinate units with administrative tasking.

c. Ensure that all persons who handle classified information are appropriately cleared, and have received the proper briefings. The clearance/access status of all individuals shall be recorded and be made available for verification.

d. Promulgate and implement additional security measures for the protection of Coast Guard personnel, assets, and information throughout the unit.

e. Ensure that an effective classified material control system is in place and properly managed by the CMCO.

f. Serve as the unit's security advisor and point-of-contact for classified visit requests, counterintelligence and other security related matters.

g. Maintain liaison with the unit Public Affairs Officer to ensure that proposed public releases which could possibly contain classified information, are reviewed prior to release.

h. Ensure their subordinate units are evaluated biennially. Enclosure (3) may be used for this purpose.

i. Monitor security and police force services.

3. In addition to the above CSO duties and responsibilities, the Headquarters CSO is authorized to grant waivers to the rank requirements for CMCOs and Document Station Control Officer's (DSCO) on the Headquarters staff.

E. Waivers and Exceptions. This section does not apply to waivers and exceptions from COMSEC requirements. Such requests are handled by Commander, TISCOM (ops-4) and the Director, COMSEC Material System.

1. Blanket waivers from physical security requirements are not authorized. Requests for waivers and exceptions shall be considered on an individual basis.

2. Requests for waivers shall be sent in writing to the cognizant SECMGR for action. Action shall be taken within 60 days. The cognizant SECMGR shall forward a copy of all correspondence pertaining to approved requests to Commandant (G-CFI). The cognizant SECMGR will numerically identify each waiver as follows:

   a. The first group of digits represent the area or district of the unit initiating the request.

   b. The next 4 digits will be the Standard Subject Identification Code (SSIC) (5530) of the request.

   c. The next digit represents "W" for waiver.

   d. The next two digits represent the serial number (sequentially), beginning annually on 1 January with 01.

   e. The last two digits represent the calendar year.

   f. Examples: D1-5530-W-01-94, PAC-5530-W-01-94

3. Requests for waiver extensions or for exceptions shall be sent in writing via the cognizant SECMGR to Commandant (G-CFI) for action.

4. Waivers shall be granted for a period of 1 year or less. They may be extended by Commandant (G-CFI) beyond 1 year only after a review of the circumstances described in the request for the extension. These requests shall be submitted to the cognizant SECMGR no later than 60 days prior to the expiration date. Each extension shall identify any previous extensions granted for the same item.

5. Requests for waivers and exceptions shall identify compensatory security measures currently in effect or planned.

6. Deficiencies which units can correct within 60 days will not require waivers; however, compensatory security measures shall be taken until the correction is made.

7. The cognizant SECMGR shall be notified in writing whenever a deficiency for which a waiver has been granted is corrected.

8. Exceptions shall be granted only when correction of a deficiency is not feasible or when the security being provided is equivalent to or better than that required by

this manual. Requests for exceptions shall cite better or equivalent protection being provided or explain why it is not feasible.

9. Requests for waivers and exceptions shall be thoroughly reviewed before forwarding to the cognizant SECMGR to ensure that all avenues for compliance have been exhausted. The approval of specific waivers and exceptions does not relieve commanding officers of the responsibility for maintaining security per all other provisions of this manual.

10. Each waiver or exception request shall be identified by the subject, the name of the unit initiating the request, the date, and shall include the following:

    a. Statement of the waiver or exception requirement and reference to the specific paragraph in this manual which cites the standards that cannot be met.

    b. Specific description of the conditions that caused the need for the waiver or exception and reasons why the standards in this manual cannot be met.

    c. Measures which are in effect to compensate for noncompliance with required standards of protection.

    d. Actions initiated or planned to eliminate the deficient condition(s) and estimated time of completion.

    e. Resources e.g., cost, manpower, required to eliminate the deficient condition(s).

    f. Impact on mission and any problem(s) that will interfere with operating requirements.

F. Physical Security Plans. In order to achieve adequate protection for a unit, a written physical security plan shall be developed. A physical security plan enables a unit to obtain a clear, comprehensive representation of the current physical security posture. A plan may also help identify means to use available resources more efficiently, prioritize security improvement projects, or provide justification for needed improvements. The effectiveness of plans are dependent on the alertness and response time of the security force, reliability and capability of intrusion detection equipment and penetration resistance of physical barrier(s). The most cost-effective security plans must take into account the interrelationship among these factors. It should be realized that barriers and locks are only delay devices and do not provide complete security, unless supported by means to detect, assess and respond to intrusions in a timely manner. Planning must be a continuing process. Changes in mission and activities of a unit require that adjustments be made in security plans. Planned security measures shall be employed so that they complement and supplement each other. Plans shall be tailored to specific security needs. Enclosure (2)

provides suggested format and essential elements of the plan. However, the plan may be a compilation of instructions or standard operating procedures. Plans shall be reviewed and updated at least annually and a copy forwarded to the cognizant SECMGR. The following factors should be taken into consideration when developing a plan:

1. Overall importance/criticality of the unit.

    a. Mission and sensitivity of the unit.

    b. Importance of the unit to the continuity of essential operations.

2. Definition and analysis of the area to be protected; for example, storage of classified information; number of personnel involved; monetary or strategic value of material; and problems such as existing hazards, either natural or man-made.

3. Criticality and vulnerability of information, equipment or material to compromise, damage, theft or pilferage.

4. Opportunity for and vulnerability to acts of terrorism.

5. Operational, maintenance and other unit requirements which must be integrated into the plan.

6. Political and economical environment, legal considerations, terrain and climate.

7. Cost of material and equipment to be installed, as well as the availability of funds to provide minimum protection for restricted areas.

8. Possible future expansion, relocation and other changes.

9. Natural Disasters IE: Hurricanes, floods, tornado’s, earthquakes etc.

This page intentionally left blank

Chapter 2 PHYSICAL PROTECTION MEASURES

A. General.

1. Good security planning works from the inside out,

   a. Start at the point where the highest value items are stored or where the highest level of protection is required. In a classified space, this point is the container where the National Security Information is stored. In a funds facility, this point is the vault, safe, or small cashier's cage.

   b. Next in importance is protecting the area around these points. This may be the room in which the safe is located, or the entire workshop where high value items are processed, or the executive offices of a major command.

   c. Finally, the perimeter of the building, complex or entire facility is secured. Gates, doors, windows, any opening that may permit someone to enter, should be protected with the appropriate locking devices and alarms..

   d. Securing the points, areas and perimeter can be accomplished in many ways and to many degrees of sophistication and reliability. The simplest way is to assign guards to all accesses to the facility, and place additional guards inside the building or area and around the safe itself. This plan would produce a high level of security. It would also generate an expense that few commands would find acceptable. To reduce costs, alarm systems are employed to take the place of all or some of the guards on the premises, especially during off-work hours.

2. The bulk of this chapter discusses those measures designed to provide protection for the high value points and areas. The application of large fences and barbed wire may not be applicable to the establishment of a simple perimeter boundary or demarcation of non-restricted areas. Many Coast Guard units are located in areas where the appearance of an armed encampment would be detrimental to their ability to work cooperatively with the public. In such situations, the Commanding Officer must understand the vulnerabilities and risks assumed by a lower security posture.

B. Designation of Restricted Areas.

1. Policy.

   a. Different areas and tasks involve different degrees of security depending upon the purpose, nature of the work performed within, and information and/or materials concerned. For similar reasons, different areas within a unit may have varying degrees of security importance. To address these

situations and at the same time facilitate operations and simplify the security system, a careful application of restrictions, controls and protective measures commensurate with these varying degrees or levels of security importance is essential. In some cases, the entire area of a unit may have a uniform degree of importance requiring only one level of restriction and control. In others, differences in the degree of security importance will require further segregation of certain security interests.

b. Cognizant Security Managers (SECMGR) shall designate restricted areas (in writing) for the purpose of protecting or safeguarding the property or material for which he/she is responsible. Such designations shall be coordinated with the Command Security Officer (CSO). Authorization for designation of such areas is derived from Title 18 U.S.C. 1382 (see Exhibit 2-1). Specific controls shall be established to meet different levels of security sensitivity and to provide an effective and practical basis for varying degrees of restricting access. These controls will depend upon the nature, sensitivity or importance of the security interest involved.

2. Restricted Areas.

a. General. Three types of restricted areas are established in descending order of protection afforded: exclusion area, limited area and controlled area. All restricted areas shall be posted as "Restricted Areas", per sign provisions of this chapter, so as not to single out or draw attention to the importance or criticality of an area. Although restricted areas frequently pertain to the safeguarding of classified information, the term's exclusion, limited and controlled are administrative only and are not synonymous with Top Secret, Secret or Confidential levels.

b. Definitions. Restricted areas are defined as follows:

(1) Exclusion Area. An exclusion area is the most secure type of restricted area. It may be within less secure types of restricted areas. It contains a security interest which if lost, stolen, compromised or sabotaged would cause grave damage to the unit mission or national security. Access to the exclusion area constitutes, or is considered to constitute, actual access to the security interest or asset.

(2) Limited Area. A limited area is the second most secure type of restricted area. It may be inside a controlled area, but is never inside an exclusion area. It contains a security interest which if lost, stolen, compromised, or sabotaged would cause serious damage to the unit mission or national security. Uncontrolled or unescorted movement could permit access to the security interest or asset.

(3) Controlled Area. A controlled area is the least secure type of restricted area. It contains a security interest which if lost, stolen, compromised, or sabotaged would cause identifiable damage to the unit mission or national security. It may also serve as a buffer zone for exclusion and limited areas, thus providing administrative control and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement may or may not permit access to the security interest or asset.

c. Types. Classification as exclusion, limited or controlled area is dictated by unit mission and the above restricted area definitions. Arms, Ammunition and Explosives (AA&E) storage areas, and classified spaces shall be designated as restricted areas; funds storage and handling areas, and controlled medical substance storage and handling areas should be designated restricted areas.

NOTE: The mere existence of a security container does not automatically require the location it is in to be a restricted area. For example, a room with a container that only stores funds may not need restricted area controls, whereas a room with a container and where money transactions and handling regularly occur would require restricted area controls. Areas where transactions only occur on an occasional basis would require the extra controls only during the transactions or handling and not at other times. Cognizant Security Managers should be consulted and compensatory measures established for proper control during all planned levels of activity.

The following are examples of areas which may be designated as restricted areas:

(1) Aircraft hangars, ramps, flight lines and runways.
(2) Aircraft rework areas.
(3) Piers and wharves.
(4) Fuel depots and bulk storage tanks, fuel issue points.
(5) Communication facilities, radio relay facilities, telephone exchange spaces.
(6) Antennas and antenna fields.
(7) Broadcasting facilities.
(8) Storage warehouses.
(9) Power stations, transformers, master valve and switch spaces.
(10) Water tank areas, water purification facilities, pumping stations.
(11) Open storage areas and yards.
(12) Intrusion detection system monitoring spaces.
(13) Central storage spaces for keys.

(14) Computer facilities and data storage areas.

NOTE: There is certainly a difference in the level of "control" needed for the security of restricted areas when they are "operational" as compared to when they are "closed down." An example of this might be Combat/Radio on a cutter where in-port, all systems are de-energized and all classified material is properly secured. While the area remains "restricted," the level of administrative control, in this example, goes from a high of "exclusion" (underway) to a low of "controlled" (in-port). Cognizant Security Managers should be consulted and compensatory measures established for proper control during all planned levels of activity.

d. Minimum Security Measures Required for Restricted Areas.

(1) The following minimum security measures are required for all exclusion areas:

(a) A clearly defined protected perimeter. The perimeter may be a fence, the exterior walls of a building/structure or the outside walls of a space within a building, structure, vessel hull or superstructure. If the perimeter is a fence, it shall be posted per the sign provisions of this chapter, at 100-foot intervals along the perimeter. If the perimeter is a wall or bulkhead, it shall be posted at the points of entry/exit.

(b) A personnel identification and control system, including an entry/departure log and an access list posted inside the area. Visitors shall be logged in/out during normal duty hours. After normal duty hours, all personnel accessing the exclusion area shall be logged in/out. An electronic system, with the capability of recording entry/exit, may be used to accomplish this.

(c) Entry and exit controlled by guards or appropriately trained and cleared personnel within the area. When secured, access to the area shall be controlled by an Intrusion Detection System (IDS) or security personnel.

(d) Admission only to persons whose duties require access and who have been granted appropriate authorization. Persons who have not been cleared for access to the security interest contained within an exclusion area may, with appropriate approval, be admitted to such area, but they shall be controlled by a cleared escort and the security interest protected from compromise.

(e) Periodic security checks (as determined by the commanding officer). The security force shall check for signs of attempted or successful unauthorized entry, and other activity which threatens to degrade the security of the exclusion area.

(2) The following minimum security measures are required for all limited areas:

(a) A clearly defined protected perimeter. The perimeter may be a fence, the exterior walls of a building/structure or the outside walls of a space within a building, structure, vessel hull or superstructure. If the perimeter is a fence, it shall be posted per the sign provisions of this chapter, at 100 foot intervals along the perimeter. If the perimeter is a wall or bulkhead, it shall be posted at the points of entry/exit.

(b) A personnel identification and control system, including an access list posted inside the area. An entry/departure log is suggested, but not required. After normal duty hours, all personnel accessing the limited area shall be logged in/out. An electronic control system, with the capability of recording entry/exit, may be used to accomplish this.

(c) Entry and exit controlled by guards or appropriately trained and cleared personnel within the area.

(d) Admission only to persons whose duties require access and who have been granted appropriate authorization. Persons who have not been cleared for access to the security interest contained within a limited area may, with appropriate approval, be admitted to such area, but they shall be controlled by a cleared escort, and the security interest protected from compromise.

(e) Periodic security checks (as determined by the commanding officer). The security force shall check for signs of attempted or successful unauthorized entry, and other activity which threatens to degrade the security of the limited area.

(3) The following minimum security measures are required for all controlled areas:

(a) A clearly defined protected perimeter. The perimeter may be a fence, the exterior walls of a building/structure or the outside walls of a space within a building, structure, vessel hull or superstructure. If the perimeter is a fence, it shall be posted per the sign provisions of this chapter, at 100-foot intervals along the perimeter. If the perimeter is a wall or bulkhead, it shall be posted at the points of entry/exit.

(b) A personnel identification and control system. During normal duty hours, use of an access list and an entry/departure log is suggested, but not required. After normal duty hours, all personnel accessing the controlled area shall be logged in/out. An electronic system, with the capability of recording entry/exit, may be used to accomplish this or the entry/exit shall be controlled by guards or appropriately trained and cleared personnel within the area.

(c) Controlled admission of individuals who require access for reasons of employment/official business, individuals who render a service, or dependents/retired military, etc. Individuals without adequate identification as determined by the commanding officer shall be logged in/out.

e. Inspections. Unit physical security plans shall include procedures for conducting inspections of persons and vehicles entering and leaving restricted areas. The purpose is to detect and prevent the introduction of prohibited items (firearms, explosives, drugs, etc.) and to detect and prevent the unauthorized removal of COMSEC material, classified information and government property. To be effective, administrative inspections should be conducted on a random basis (as determined by the commanding officer). Procedures should be approved by the cognizant legal authority.

3. Non-Restricted Areas.

a. A non-restricted area is an area which is under the jurisdiction of a unit, but to which access is either minimally controlled or uncontrolled. Such an area may be fenced, but may be open to the uncontrolled movement of the general public at various times. An example of a non-restricted area is a visitor or employee parking lot open and unattended by security during business hours. After business hours it may be closed, patrolled and converted to a restricted area. Another example is a personnel office to which the general public is permitted access during business hours without being required to check in or register with security. A non-restricted area

could be an area closed by a fence or other barrier, to which access would be minimally controlled by a check point which would only ensure that the visit or access was for official business or other authorized purposes. A housing area, exterior to the unit, would normally be designated as a non-restricted area. Non-restricted areas shall not be located inside restricted areas.

b. Many units have areas containing a number of functions to which members of the armed forces and their dependents, as well as civilian employees and their families, are permitted access by displaying vehicle decals or by presenting appropriate identification cards (not issued on the basis of security clearance or similar screening, but by virtue of employment or status). These functions include exchanges, commissaries, administrative offices, dispensaries, clubs, recreational facilities, etc. Areas containing these functions will not normally be restricted areas. However, it is possible these areas may have internal spaces that are designated as restricted areas.

C. Physical Barriers.

1. General. A clearly defined perimeter should be established around all units and posted to establish a legal boundary. This provides a buffer zone, facilitates control, makes accidental intrusion unlikely, and identifies government property boundaries for prosecution purposes. Examples are building exteriors, fences, ropes, chains, etc. Natural barriers, appropriately posted, can also define a perimeter. It is important that consultation be made with local authorities to ensure that posting of barriers in areas of concurrent or proprietary jurisdiction complies with local or state trespass laws.

2. Purpose. Physical barriers control, deny, impede, delay and discourage access to restricted and non-restricted areas by unauthorized persons. They accomplish this by:

a. Defining the perimeter boundaries of government-owned property.

b. Defining the perimeter of restricted areas.

c. Establishing a physical and psychological deterrent to entry as well as providing notice that entry is not permitted.

d. Optimizing use of security forces.

e. Enhancing detection and apprehension opportunities by authorized personnel in restricted and non-restricted areas.

f. Directing and channeling the flow of personnel and vehicles through designated portals in a manner which permits efficient operation of the personnel identification and control system.

3. Types. Two general types of physical barriers are:

a. Natural: mountains, swamps, thick vegetation, rivers, bays, cliffs, etc.

b. Structural: fences, walls, doors, gates, roadblocks, vessel hull, superstructures, bulkheads.

4. General Considerations. Physical barriers delay but rarely can be depended upon to stop a determined intruder. Therefore, to be effective, such barriers must be augmented by security force personnel or other means of protection.

a. Physical barriers shall be established around all restricted areas. The barrier or combination of barriers used must afford an equal degree of continuous protection along the entire perimeter of the restricted area.

b. In cases of a high degree of relative criticality and vulnerability, it may be necessary to establish two lines of physical barriers at the restricted area perimeter. Such barriers should be separated by not less than 30 feet for optimum protection and control. Two lines of barriers shall only be used in conjunction with an IDS between the fences (or on the inside fence) and a security force capable of immediate response. The use of two barriers alone provides little extra protection beyond a few seconds of delay to a determined intruder and may actually be counter-productive by identifying the location of high-risk items.

c. In establishing any perimeter or barrier, especially a building or room, consideration must be given to providing emergency entrances and exits in case of fire; however, openings shall be kept to a minimum consistent with the efficient and safe operation of the unit without degradation of minimum security standards.

d. Water boundaries present special security problems. Such areas should be protected by structural barriers or an IDS and posted. In addition to barriers, patrol craft are recommended at units whose waterfronts contain critical assets, restricted areas, or other mission essential elements. In inclement weather, when patrols cannot provide an adequate degree of protection, security may be supplemented by additional patrols (e.g., foot/vehicular), Closed Circuit Television (CCTV), watch towers, sentry dogs, etc.

e. Construction of new security barriers and removal of existing barriers and related work shall be approved by the cognizant SECMGR.

5. Fences.

a. Chain Link Fencing. Chain link fencing is the type of structural barrier most commonly used and recommended for security purposes. Chain link fencing must be used to enclose restricted areas where fencing is required. The following standards apply:

(1) Fabric. The standard fence fabric shall be at least nine-gauge zinc or aluminum coated steel wire chain link with mesh openings not larger than 2 inches per side and a twisted and barbed selvage at top and bottom.

(2) Fabric Ties. Only nine gauge steel ties shall be used. If the ties are coated or plated, the coating or plating shall be electrolytically compatible with the fence fabric to inhibit corrosion.

(3) Height. The standard height for restricted area fencing is 8 feet. This includes a fabric height of 7 feet, plus a top guard.

(4) Fencing Posts, Supports and Hardware. All posts, supports, and hardware for security fencing shall meet the requirements of Federal Specification RR-F-191K/GEN of 14 May 1990, or latest version. All fastening and hinge hardware shall 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 shall be located on the inner side of the fencing. Posts shall be positively secured into the soil to prevent shifting, sagging or collapse.

(5) Reinforcement. Taut reinforcing wires shall be installed and interwoven or affixed with fabric ties along the top and bottom of the fence for stabilization of the fence fabric. Top rails shall not be installed on restricted area fencing. Top rails are permitted on non-restricted area fences. The vulnerability introduced is that these rigid top rails provide a stable structure to place climbing aids against.

(6) Ground Clearance. The bottom of the fence fabric shall be within 2 inches of firm soil or buried sufficiently in soft soil to compensate for shifting soil.

(7) Culverts and Openings. Culverts under or through a fence shall be of 10-inch pipe, or of clusters of such pipe or equivalent. Openings under or through a fence shall be secured with material equal or greater in strength than the overall barrier.

(8) 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.

(9) Top Guards. A top guard shall be constructed on all restricted area perimeter fences and may be added on interior enclosures for additional protection. A top guard is an overhang of barbed wire or barbed tape along the top of a fence, facing outward (away from protected site) and upward at approximately a 45 degree angle. Top guard supporting arms shall 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, equally spaced, shall be installed on the supporting arms. The top guard of fencing adjoining gates may rise to a vertical height of 18 inches and extend to the normal 45-degree outward direction. Top guard must be installed in a manner that will not interfere with gate operation.

(10) Barriers. Buildings, structures, waterfronts and other barriers used instead of, or as a part of, a fence line shall provide equivalent protection to the fencing required for that area. Therefore, all windows, doors and other openings shall be properly secured.

b. Alternative Fencing. Where a restricted area perimeter boundary passes through an isolated area (forest, jungle, swamp) that is unpatrolled and where vehicular passage is impossible, the boundaries may be defined with a three or four strand 12 gauge barbed wire fence approximately 4 feet high. It shall be posted with appropriate signs, approximately 1 foot from the top.

c. Other Fencing: For non-restricted areas where no fence is required, but is desired to establish and mark property boundaries, any suitable commercial fencing may be used. The Cognizant Security Manager should be consulted before purchase or installation to ensure it will be appropriate for its intended use. Some areas of the country are further restricted by the Historical Society. While the Coast Guard has the right to provide appropriate protection for government property, we must also work with the local communities to be a good neighbor

6. Walls. Walls may be used as barriers in lieu of fences for reasons of historical or ceremonial significance. The protection afforded by walls shall be equivalent to that provided by chain link fencing. This may be accomplished by barbed wire, IDS, etc., as determined by the cognizant SECMGR. Walls, floors, and roofs of buildings may also serve as perimeter barriers.

7. Temporary Barriers. In some instances, the temporary nature of a restricted area does not justify the construction of permanent perimeter barriers. The resulting lack of security shall be compensated for by additional security forces, patrols and other temporary security measures during the period of use.

8. Clear Zones.

   a. An unobstructed area or clear zone shall be maintained on both sides of and between permanent physical barriers of restricted and non-restricted areas. Vegetation inside clear zones shall not exceed 8 inches in height.

   b. An inside clear zone shall be at least 30 feet. Where possible, a larger clear zone should be provided to preclude or minimize damage from thrown objects such as incendiaries or bombs.

   c. The outside clear zone shall be 20 feet or greater between the perimeter barrier and any exterior structures, vegetation or any obstruction to visibility. Construction of any new fence enclosing a restricted area having a smaller clear zone shall be approved by an exception granted as set forth in Chapter 1.

   d. In those units where space on government land is available, but the fence does not meet clear zone requirements in its present location, relocating the fence to obtain a clear zone may not be feasible or cost effective. Some alternatives to extending the clear zone would be increasing the height of the perimeter fence, extending outriggers, installing double outriggers and in some cases installing concertina or general purpose barbed tape to compensate for the proximity of aids to concealment or access. Where property owners do not object, the area just outside the fence should be cleared to preclude concealment of a person. All fencing shall be kept clear of visual obstructions such as vines, shrubs, tree limbs, etc., which could provide concealment for a possible intruder.

   e. Inspections of clear zones shall be incorporated with inspections of perimeter barriers to ensure an unrestricted view of the barrier and adjacent ground.

9. Patrol Roads. When the patrolled perimeter barrier encloses a large area (1 square mile or greater), an interior perimeter road in all areas not affected by impassable terrain features shall be provided for use of security patrols.

10. Inspection of Barriers. Security and/or Police personnel shall check security barriers at least monthly for defects that would facilitate unauthorized entry and report them to supervisory personnel. Personnel must be alert to detect the following:

    a. Damaged areas (cuts in fabric, broken posts).

    b. Deterioration (corrosion).

    c. Erosion of soil beneath the barrier/shifting of land.

    d. Loose fittings (barbed wire, outriggers, and fabric fasteners).

    e. Growth in the clear zones that would afford cover for possible intruders.

    f. Obstructions at or on the fence which would afford concealment or aid entry/exit for an intruder.

    g. Evidence of intrusion or attempted intrusion.

11. Perimeter Openings. Openings in the perimeter barriers shall be kept to the minimum necessary for the efficient operation of the unit.

12. Gates. Gates facilitate the entrance and exit of authorized traffic and control its flow.

    a. Number and Location. Gates shall be limited to the number consistent with efficient operations. Such factors as the centers of activity and personnel/vehicular traffic flow inside and outside the area shall be considered in locating gates. Alternative gates, which are closed except during peak movement hours, may be provided so that heavy traffic flow can be expedited. When open or operating, all gates should be under security force control. Gates shall provide protection equivalent to the outer fences or barriers of which they are a part when not in use. These gates shall be locked to form an integral part of the fence when closed.

    b. Inspection. When not in active use and controlled, gates, turnstiles and doors in the perimeter barrier shall be locked and frequently inspected by security patrols. Locks shall be rotated or re-keyed at least annually.

c. Pedestrian Gates. Pedestrian gates and turnstiles shall be designed so that only one person entering or departing may approach the guard at a time. Some channels may be closed between rush hours. Where possible, pedestrian and vehicular gates shall be clearly separated.

d. Vehicular Gates. Vehicular gates shall be set well back from any public highway in order that temporary delays caused by identification checks at the gate will not cause traffic hazards extending out onto a public highway. There shall also be sufficient space at the gate to allow for spot checks, inspections, searches and temporary parking of vehicles so as not to impede the flow of traffic.

13. Doors, Windows, Skylights and Other Openings. Building exit doors on the restricted area perimeter shall provide the protection commensurate with the requirement for proper protection of the assets accessible through those doors. Hinges shall be located on the inside of the door, or hinge pins shall be peened or welded to prevent removal. Windows, skylights and other openings, which penetrate the restricted area perimeter barrier, that are of 90 square inches or greater, shall be protected by securely fastened nine gauge wire mesh (not larger than 2 inch openings), framed and permanently bolted to the structure. Such openings are considered inaccessible to personnel when they are 18 feet or more above ground level or any horizontal surface large enough to place a climbing aid upon and 14 feet or more distant from other buildings, structures, etc., outside the perimeter. Protective screens, hardened steel bars, or glazing have an additional value of preventing missiles such as hand grenades, bombs and incendiary devices from being hurled through the windows from outside the perimeter.

14. Sewers, Culverts and Other Utility Openings. Sewers, air intakes, exhaust tunnels and other utility openings which penetrate the perimeter or restricted area barrier and have a cross section area of 90 square inches or greater, shall be protected by securely fastened grills (not larger than 2 inch openings), locked manhole covers or other equivalent means which provide security commensurate to that of the perimeter or restricted area barrier. Bars and grills across culverts, sewers, etc., are a hazard when susceptible to clogging. This hazard must be considered during planned construction of such bars and grills. All such installations shall be designed to permit rapid clearing or removal of grating when conditions require such action. Removable grates shall normally be locked in place.

15. Utility Poles, Signboards and Trees. Utility poles, signboards, trees, etc., located within 14 feet of the perimeter barrier of the unit, present a possible means of illegal entry. To reduce this possibility, the perimeter barrier shall be staggered to increase the distance to more than 14 feet and may be heightened to the extent necessary to prevent entry. Should these utility poles, signboards, trees, etc., also obstruct the visibility of security patrols, they shall be at least 20 feet outside the perimeter barriers.

16. Signs and Posting of Boundaries.

a. Restricted areas, that are also classified spaces, shall be posted at all external points of entry with signs approximately 2 feet by 2 feet in size with appropriate lettering. Signs shall read:

WARNING

RESTRICTED AREA

THIS AREA HAS BEEN DECLARED A RESTRICTED AREA IN ACCORDANCE WITH TITLE 18 U.S.C. 1382. UNAUTHORIZED ENTRY IS PROHIBITED. ALL PERSONS ENTERING HEREON ARE SUBJECT TO SEARCH. PHOTOGRAPHING OR MAKING NOTES, MAPS, DRAWINGS OR GRAPHIC REPRESENTATIONS OF THIS AREA OR ITS ACTIVITIES IS PROHIBITED UNLESS SPECIFICALLY AUTHORIZED BY THE COMMANDING OFFICER. ANY SUCH MATERIAL FOUND IN THE POSSESSION OF UNAUTHORIZED PERSONS SHALL BE CONFISCATED.

b. Other restricted areas shall be posted at all external points of entry with signs approximately 2 feet by 2 feet in size with appropriate lettering. Adjustments to the size of the sign to facilitate placement on magazine doors is authorized, as long as the required wording remains unchanged and legible. Size should not be adjusted any smaller than is minimally necessary and the wording must remain clearly readable from a distance. Signs shall read:

WARNING

RESTRICTED AREA
KEEP OUT

AUTHORIZED PERSONNEL ONLY
AUTHORIZED ENTRY INTO THIS RESTRICTED AREA CONSTITUTES CONSENT TO SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL.

TITLE 18 U.S.C. 1382

c. All restricted area perimeters, e.g. fence, shall be posted at 100-foot intervals, approximately 3 feet from the top (eye level), with signs measuring approximately 12 inches by 18 inches in size with appropriate lettering. Signs shall read:

WARNING

RESTRICTED AREA
KEEP OUT

AUTHORIZED PERSONNEL ONLY

d. Non-restricted areas shall be posted at all external points of entry with signs approximately 2 feet by 2 feet in size with appropriate lettering. Signs shall read:

WARNING

U.S. COAST GUARD PROPERTY

AUTHORIZED PERSONNEL ONLY
AUTHORIZED ENTRY INTO THIS AREA CONSTITUTES CONSENT TO SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL.
TITLE 18 U.S.C. 1382

e. Government property boundaries and non-restricted area perimeters, e.g. fence, shall be posted at 200 foot intervals, with signs at eye level, measuring approximately 11 inches by 12 inches in size with appropriate lettering. Signs shall read:

U.S. GOVERNMENT PROPERTY

NO TRESPASSING

Red, white and blue plastic signs in the form of a shield may be used for this purpose. NSN is 9905-00-559-2971.

f. Where a language other than English is prevalent, signs shall be posted in both English and the other language.

g. Barrier signs shall not obscure the necessary lines of vision for security force personnel.

h. Exterior signs shall be fabricated of metal with black lettering on a white background, except that the word "WARNING" shall be in red. Exterior signs shall be fabricated to provide legibility from a distance of at least 50

feet during daylight under normal conditions. Existing signs do not need to be replaced provided the signs are in good repair, the lettering is legible, and the wording is similar to the above requirements.

i. Interior signs may be fabricated of wood, metal, plastic or cardboard. Existing signs do not need be replaced provided the signs are in good repair, the lettering is legible, and the wording is similar to the above requirements.

D. Protective Lighting.

1. General. Protective lighting, during hours of darkness, provides a continuing degree of protection similar to that maintained during daylight hours. It increases the effectiveness of security forces performing their duties, has considerable value as a deterrent to thieves and vandals, and may make the job of the saboteur or terrorist more difficult.

2. Principles and Guidelines. When protective lighting is installed and used, the following basic principles should be applied to help ensure its effectiveness:

a. Provide adequate illumination or compensatory measures to discourage or detect illegal attempts to enter restricted areas and to reveal the presence of unauthorized persons within such areas.

b. Avoid glare which handicaps security force personnel or is objectionable to air, rail, highway or navigable water traffic or occupants of adjacent properties.

c. Locate light sources so that illumination is directed toward likely intruder avenues of approach and provides relative darkness for patrol roads, paths and posts. To minimize exposure of security force personnel, lighting at entry points shall be directed at the gate and the guard shall be in the shadows. This type of lighting technique is often called "glare projection".

d. Illuminate shadowed areas caused by structures within or adjacent to restricted areas.

e. Design the system to provide overlapping light distribution. Equipment selection shall be designed to resist the effects of environmental conditions, and all components of the system shall be located to provide maximum protection against intentional damage.

f. Avoid drawing unwanted attention to security areas.

g. During planning stages, considerations shall be given to future requirements of CCTV and recognition factors involved in selection of the type of lighting to be installed.

3. Types.

a. Continuous. This is the most common protective lighting system. It consists of a series of fixed lights arranged to flood a given area continuously during the hours of darkness with overlapping cones of light. The two primary methods of employing continuous lighting are glare projection and controlled lighting.

(1) Glare Projection. Uses lights slightly inside a security perimeter and is directed outward. This method is useful where the glare of lights directed across surrounding territory will not annoy or interfere with adjacent operations. It may be a deterrent to a potential intruder because it makes it difficult to see inside of the protected area. It also protects security personnel by keeping them in comparative darkness and enabling them to observe intruders at considerable distance beyond the perimeter.

(2) Controlled. Best used when it is necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways, railways, navigable waters or airports. The width of the lighted strip can be controlled and adjusted to fit a particular need, such as illumination of a wide strip inside a fence. This method often illuminates or silhouettes security personnel as they patrol their routes.

b. Standby. A standby system differs from continuous lighting in that its intent is to create an impression of activity. The lights are not continuously lighted, but are either automatically or manually turned on randomly or when suspicious activity is detected or suspected by security personnel or IDS. Lamps with short restart times are essential if this technique is chosen. This technique may offer significant deterrent value while also offering economy in power consumption.

c. Movable. A stationary or portable system which consists of manually operated movable searchlights, which may be lighted during hours of darkness, or lighted only as needed. This system is normally used to supplement continuous or standby lighting.

d. Emergency. This system may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies which render

the normal system inoperative. It depends on an alternative power source, such as installed or portable generators or batteries.

4. Lighting Concepts. Exterior lighting may be designed for direct illumination, indirect illumination, intermittent illumination, or responsive area illumination.

   a. Direct Illumination. This lighting concept is most widespread and involves directing light down from a structure roof to the ground immediately surrounding the structure. Its goal is to provide a specified intensity of illumination on intruders, facilitating their detection by CCTV or security patrols.

   b. Indirect Illumination. An alternative lighting concept involves backlighting the intruders against the structure. 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.

   c. Intermittent Lighting. A deterrent lighting system can be developed to turn lights on at random times. It can use either direct or indirect illumination concepts. Deterrence can actually be higher for such a system because of its appearance of activity. Luminaries may be controlled individually or as a group.

   d. Responsive Area Illumination. 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, if installed, is subjected to the same nuisance and false alarms of any sensor system. Since the lights will be falsely activated, the area should be assessed using CCTV.

5. Protective Lighting Parameters. Except for the minimum standards described below, the commanding officer must decide what other areas/assets to illuminate and how to do it. This decision must be based upon the following:

   a. Relative value of items being protected.

   b. Significance of the items being protected in relation to accomplishment of the mission of the unit and its role in the overall national defense structure.

   c. Availability of fiscal resources to procure and install lighting and follow-on maintenance costs.

d. Availability of security forces to patrol and observe illuminated areas.

e. Energy conservation.

6. Minimum Standards.

a. Protective lighting shall be checked daily by the security force to ensure all light fixtures are operational. Inoperative lights shall be recorded and reported to the CSO or senior duty watch officer, who shall ensure that all reports are given immediate attention and corrective actions are taken.

b. Restricted areas shall be provided with sufficient illumination to enable the security force to detect, observe and apprehend unauthorized intruders.

c. Patrolled fence-lines, water boundaries, and similar areas shall be sufficiently illuminated to assist the security force in detecting illegal intrusion attempts and to act as a deterrent. Unpatrolled areas may not need to be illuminated.

d. Vehicular and pedestrian gates used for routine entry/exit shall be sufficiently illuminated to facilitate personnel identification and access control.

e. Exterior building doors shall be provided with lighting to enable the security force to observe an intruder seeking access.

f. MLCs and/or Facility Design and Construction Centers (FD&CCs) should be consulted for assistance in establishing lighting levels and lamp types.

7. Emergency Power. Restricted areas provided with protective lighting should have an emergency power source located within a restricted area. The emergency power source shall be adequate to sustain protective lighting for a minimum of 4 hours. Provisions shall be made to ensure the immediate availability of emergency power in the event of failure of the primary source. Emergency power sources shall start automatically. Emergency power systems shall be tested monthly and the records maintained for 1 year. Battery powered lights and essential communications should be available at all times at key locations within the restricted areas in the event of complete failure of both the primary and emergency sources of power.

8. Additional Protection.

a. Wiring System. Installing multiple circuits may provide an advantage in protective lighting systems. The circuits shall be arranged so that failure of

any one lamp will not darken a long section of a critical or vulnerable area. The protective lighting system shall be independent of the unit's lighting system, and be protected so that fire or disaster will not interrupt the entire system.

b. Controls and Switches. Controls and switches for protective lighting systems shall be inside the protected area and locked or guarded at all times. An alternative is to locate them in a central station similar to or as a part of the system used in IDS central monitoring stations. High impact plastic shields may be installed over lights to prevent destruction by stones, air rifles, etc.

E. Intrusion Detection Systems (IDS).

1. General. IDSs are security support measures that are designed to detect and announce intrusions or attempted intrusions. They will not prevent intrusions nor apprehend intruders. An IDS is best described as an aid to security forces, which allows them to be more efficient. It is important to remember that an IDS is ineffective unless it is supported by prompt and appropriate security force response.

2. Planning and Design Considerations.

a. Regardless of type, an IDS must be stable, reliable, and maintainable. The system must report the detection of an intruder, the failure of any critical component of the system, and any attempt to circumvent or defeat the system.

b. Factors to be considered in the selection of components and design of the system include:

(1) Size, location, criticality, and vulnerability of the security interest.

(2) Location and response time capability of security force personnel.

(3) Area environment to include building construction, sound levels inside and outside, atmospheric conditions and vegetation.

(4) Radio and electrical interference.

(5) Compatibility of the system with other security measures.

(6) Operational hours of the unit.

(7) Maintenance requirements and capabilities.

(8) Reliability of the components to include frequency of false/nuisance alarms.

(9) Degree of salvage value (equipment can be readily removed and installed elsewhere).

3. Characteristics. Essential characteristics of all IDSs include the following:

a. A sensor or sensor components located in the protected area designed to initiate an alarm upon an attempted intrusion into a protected area.

b. Control unit located in the protected area which acts as an interface between the sensor(s) and the central annunciator.

c. Signal transmission lines which transmit the alarm signals from the control unit to a central annunciator.

d. A central annunciator (which shall be constantly monitored) containing the electronic components which announce, by both visible and audible signals, intrusion into protected areas and the specific structure or location involved.

e. Fail-safe features, such as an alarm signal, at the central annunciator when abnormal operating conditions preclude the system from functioning properly, and a back-up power source.

f. Features which minimize the vulnerability to tampering or circumvention.

4. Security Standards.

a. Balanced Magnetic Switches (BMS) shall be installed on doors (if the IDS is mandatory). Due to the added cost of BMS, "unbalanced" switches may be used on doors where an IDS is not mandatory.

b. Line supervision shall be incorporated (if the IDS is mandatory) to detect any signal cutting, shorting or splicing of the transmission line. Attempts at gaining access to, or substitution or neutralization of any sensor shall be detected and signaled. An alarm shall be indicated at the alarm control center within 1 second of a line tamper attempt. Dedicated terminal junction boxes for sensor inputs and connecting cables shall be securely welded or locked and provided with tamper switches. Junction boxes containing phone lines which carry alarm system signals do not need to be locked, welded or alarmed. However, if practicable, the room containing such boxes shall be kept locked or alarmed. Visible lines shall be inspected

periodically. Due to the added cost of line supervision, it is not necessary if an IDS is not mandatory.

c. A backup power source, capable of sustaining the system for a minimum of 4 hours, shall be provided to enable uninterrupted operation. Commanding officers shall plan for and include as part of the physical security plan, appropriate measures to be taken in the event of an extended power outage.

d. On/off switches shall be located within the protected area.

e. The IDS shall include a central control station where alarms annunciate. In addition, an audible alarm shall be located outside the protected area. Alarm signals shall be reset only in the protected area or the central control station.

f. The alarm display panel shall indicate secure, access and alarm status.

5. Principles of Operation. No one system is suitable or adaptable to every location and environment. The situations and conditions at the particular site to be protected determine which devices or systems are efficient and practicable. The following are some basic principles upon which many IDSs operate:

a. Breaking an Electrical Circuit.

(1) General. Possible points of entry into buildings or enclosures can be alarmed by using electrically sensitized strips of metallic foil or wire. Any action which breaks the foil or wire breaks the electrical circuit and activates an alarm. Metallic foil is frequently used on glass surfaces. Doors and windows may also be equipped with BMSs which activate an alarm when the door or window is opened.

(2) Advantages. Consistently provides the most trouble-free service; causes few nuisance alarms. Adequate in low-risk applications.

(3) Disadvantages.

(a) Costly to install where there are many entry points to the protected area.

(b) Easily compromised when improperly applied; unprotected soft walls or ceilings may be penetrated without disturbing the system. It may also be defeated by bridging the circuits.

(c) Has little salvage value.

(d) Will not detect "stay-behinds".

b. Interruption of a Light Beam.

(1) General. The photoelectric (electric eye) type of sensor derives its name from the use of a light-sensitive cell and a projected light source. A light beam is transmitted at a frequency of several thousand vibrations per second. An infrared filter over the light source makes the beam invisible to intruders. A light beam with a different frequency, such as a flashlight, cannot be substituted for this beam. The beam is projected from a hidden source and may crisscross in a protected area by means of hidden mirrors until it contacts a light-sensitive cell. This device is connected by wires to a control unit. When an intruder crosses the beam, he breaks contact with the photoelectric cell which activates an alarm. A projected beam of invisible light can be effective for approximately 500 feet indoors and will cover a distance of up to 1000 feet outdoors. The effectiveness of the beam is decreased from 10 to 30 percent for each mirror used.

(2) Advantages.

(a) When properly installed, affords effective, reliable notice of intrusion.

(b) Useful in open portals or driveways where obstructions cannot be used.

(c) Detects "stay-behinds".

(d) Has a high salvage value; almost all equipment is recoverable.

(e) May be used to actuate other security devices such as cameras.

(f) May detect fires through smoke interruption of the beam.

(3) Disadvantages.

(a) Employment is limited to those locations where it is not possible to bypass the beam by crawling under or climbing over it.

(b) Requires some type of permanent installation.

(c) Fog, smoke, dust and rain in sufficient density will cause interruption of the light beam.

(d) Requires frequent inspections of light producing components to detect deterioration.

c. Detection of Sound.

(1) General. This type of sensor can be effectively utilized to safeguard enclosed areas, vaults, warehouses and similar enclosures. Super-sensitive, microphone-speaker sensors are installed on the walls, ceilings, and floors of the protected area. Any sound caused by attempted forced entry is detected by the sensor. Sensitivity can be adjusted.

(2) Advantages.

(a) Economical and easily installed.

(b) High salvage value.

(3) Disadvantages. Can be used only in enclosed areas where a minimum of extraneous sound exists. Also, it is not satisfactory where high noise levels are encountered, especially in proximity to aircraft and railroad traffic. Cannot be used effectively outdoors. Not authorized for use in classified spaces.

d. Detection of Vibration.

(1) General. This type of sensor can be effectively used to safeguard enclosed areas as in the sound detection type. Vibration-sensitive sensors are attached to walls, ceilings and floors of the protected area. Any vibration caused by attempted forced entry is detected by the sensor. Sensitivity can be adjusted.

(2) Advantages.

(a) Economical and easily installed.

(b) High salvage value.

(c) Flexible application.

(3) Disadvantages. Can be used only in areas where a minimum of vibration exists; not satisfactory where high vibrations are encountered, especially in proximity to heavy construction, railroad, or vehicular traffic. Cannot be used effectively outdoors.

e. Detection of Motion. An IDS using ultrasonic or microwave motion sensors can be very effective for the protection of interior areas. Such systems flood the protected area with acoustic or microwave energy and detect the Doppler shift in transmitted and received frequencies when motion occurs within the area.

(1) Ultrasonic Systems. These systems consist of transceivers, an electronic unit (amplifier) and a control unit. The transmitter generates a pattern of acoustic energy which fills the enclosed area. The receiver, connected to the electronic unit, picks up the standing sound patterns. If they are of the same frequency as the waves emitted by the transmitter, the system will not alarm. Any motion within the protected area will send back a reflected wave differing in frequency from the original transmission. The change in frequency will be detected, amplified, and the alarm signal will be activated. Multiple transceivers or a transmitter and multiple receivers may be operated from the same control unit for more effective coverage of large or broken areas. This system can only be used indoors.

(a) Advantages.

(i) Provides effective security protection against intruders concealed within the premises.

(ii) High salvage value.

(iii) Protective field is not visible, therefore, it is difficult to detect its presence or to compromise the system.

(b) Disadvantages.

(i) May require reduced sensitivity to overcome possible disturbance factors in the enclosed area.

(ii) Can be set off by loud external sounds.

(2) Microwave Systems. These systems closely parallel the operation of the ultrasonic system. A pattern of radio waves is transmitted which is partially reflected back to an antenna. If all objects within the range of the radio waves are stationary, the reflected waves return at the same frequency. If they strike a moving object, they return at a different frequency. The difference in the transmitted and received frequency is detected, thus initiating an alarm signal.

(a) Advantages.

(i) Good coverage is provided if antenna are properly placed.

(ii) Not affected by air currents, noise or sound.

(iii) High salvage value.

(b) Disadvantages.

(i) Coverage is not easily confined to desired protected area. Penetrates thin wooden partitions and windows and therefore may be accidentally activated by persons or vehicles outside the protected area.

(ii) Fluorescent light bulbs will activate the sensor.

(iii) Not authorized for use in classified spaces.

f. Detection of Change in Capacitance Due to Penetration of an Electrostatic Field.

(1) General. The capacitance or electrostatic system can be installed on a safe, wall, or openings therein. The capacitance sensor establishes an electrostatic field around the object to be protected. The body capacitance of an intruder who enters the field unbalances the electrostatic energy which activates the alarm signal.

(2) Advantages.

(a) Extremely flexible type of system; it may be used to protect safes, file cabinets, windows, doors or partitions.

(b) Simple to install and operate.

(c) Provides an invisible protective field making it more difficult for an intruder to determine when the system alarms.

(d) High salvage value - may be easily dismantled and re-installed.

(e) Compact equipment size.

(f) High grade of protection.

(3) Disadvantages. Can be applied only to ungrounded equipment.

6. Maintenance.

a. If an IDS is to be effective, the system should remain in continuous operation during the unit's non-operational hours. There are situations where it may be necessary to have a continuous 24-hour operation. Therefore, preventive and corrective maintenance shall be performed properly. Each system shall be capable of operating from an emergency power source. The time requirement for such operational capability must be evaluated; consideration should be given to such factors as alternate power supplies, maintenance support, and hours of active operation. Emergency power sources for IDS shall be tested monthly and the records maintained for 1 year.

b. Maintenance is not a difficult problem if proper care is routinely exercised. Most malfunctions, if the system has been properly selected, installed and adjusted, result from improper maintenance. To prevent malfunctions, all component parts shall be regularly inspected and tested by qualified personnel as often as recommended by manufacturers. Spare parts, as recommended by the manufacturer, shall be stocked locally, unless immediately available from local sources.

c. Normally, manufacturers will train and advise personnel on the maintenance of their equipment. To ensure proper operation of an IDS, the following shall be observed:

(1) Designated unit personnel should be available and capable of effecting immediate minor repairs, to include replacement of fuses, maintenance and replacement of the auxiliary power unit, and

correction of obvious causes of malfunctions and invalid alarms. All other forms of replacement parts and repairs shall be provided by support maintenance personnel.

(2) If a unit cannot furnish support maintenance personnel, a service contract should be established. In either case, maintenance service shall be available on a 24-hour basis. Maintenance response to critical areas shall be no more than 3 hours.

d. All plans and diagrams showing the location and technical data of installed systems, signal transmission lines and control units shall be marked "FOR OFFICIAL USE ONLY" (FOUO). Access to such plans and diagrams shall be strictly limited to persons with a need to know.

7. Monitoring. In order for an IDS to be effective it must be monitored and result in some kind of response when alarmed. Monitoring may be accomplished by either unit personnel, security/police force, or a contract monitoring service.

a. Procedures shall be developed to respond to all IDS alarms. IDS alarms to AA&E areas must be responded to by an armed response force. It is desirable for other IDS alarms to also be responded to by an armed response force to ensure their own protection. Any unit response must take into account the safety of unit personnel. A cautious investigative approach to an IDS alarm by at least two people should be considered a standard. Specific response plans should be included as part of each units Physical Security Plan.

b. For units that monitor IDS alarms locally, the alarm receiving area shall provide protection to monitoring personnel as this will be a prime target for an intruder. Admittance to this area shall be restricted by administrative controls or by designation as a restricted area.

c. For units that use security or police force personnel, or a contract monitoring service, specific action plans shall be developed to direct appropriate response actions.

d. Personnel on duty at a control unit shall maintain a record of all system events including the number of alarms and any malfunctions experienced. The purpose of this record is to provide a history of the types of alarms activated, e.g., nuisance or false alarms, etc. This record shall be maintained for 1 year. Records should reflect the following:

(1) Date, time and prevailing weather conditions.

(2) Name of person recording an alarm signal.

(3) Location of the area in which the alarm occurred.

(4) Action taken in response to the alarm.

(5) Total time that was required by response personnel to arrive at the scene of an alarm.

(6) Cause of the alarm signal.

(7) Tests of alarms.

(8) Malfunctions, including nuisance alarms.

(9) Servicing/maintenance of systems.

e. A locally developed identity verification/duress code shall be used in conjunction with each IDS to ensure positive identification of person's entering/exiting alarmed structures and opening/closing alarmed containers. These codes shall be:

(1) Developed and distributed by the CSO.

(2) Marked and protected as FOUO.

(3) Varied for each alarmed activity.

(4) Changed semi-annually unless compromised, in which case the codes shall be changed immediately.

(5) Used in conjunction with a list of authorized personnel provided to the CSO by the alarmed activity.

8. Testing.

a. All IDS and duress systems shall be adjusted and maintained at the highest attainable sensitivity that will provide optimum performance and reliability without false or nuisance alarms. Optimum performance shall be determined from the manufacturer's stated specifications and by testing the equipment upon installation and at least monthly thereafter. A record of the monthly test shall be maintained for 1 year and shall reflect the date of test, names of persons completing the test, results of the test, and any action taken in the event of malfunctions. The CSO shall arrange procedures for these tests. IDS tests may occur during normal duty

openings or closings of the protected area. Sample test procedures are as follows:

(1) Motion Detection: Overt body motion (walking through the protected area at the rate of one step per second for 4 seconds) in areas protected by ultrasonic, microwave, and other motion detection devices.

(2) Door Switches: Actual opening of doors (or other openings using door switches) which are protected by balanced magnetic door switches.

(3) Capacitance Alarm: Attempts to push hands, arms, or legs through the protected area (air ducts or vents); to touch an item being protected (door, window, wall, etc.); or to move protected objects (security containers).

(4) Vibration Detection: Hammering with a 1-pound hammer or weight on walls, floors, or ceilings protected by vibration detection equipment. Preferably this should be done midway between detectors. Damage to surfaces finished with wallboard, plaster, wood paneling, etc. (which are considered fragile surfaces) may be avoided by placing a piece of heavy scrap wood, about 2 feet long, against the point where the blows are struck. Three to six blows within 1 minute should cause an alarm.

(5) Other: IDSs consisting of either lacing or foil pad shall be tested only by qualified alarm technicians with appropriate electronic equipment. Alarm equipment which is used and tested daily (e.g., door switches, motion detectors, etc.) needs no monthly testing.

b. In addition to the above, periodic unannounced openings shall be performed to test alarm responses by the monitoring security force. These exercises determine the actual alarm response time and the ability of security personnel to implement alerting procedures associated with alarm annunciators. The tests shall be conducted in the spirit of assisting the guards in enhancing their performance, thus increasing the security provided the unit, but shall not be so frequent as to be considered a nuisance to security personnel. Testing will be coordinated with the CSO and security personnel who monitor the IDS.

NOTE. The testing outlined above assumes that the response is being provided by a Coast Guard security or police force. For those units that receive alarm response through an MOU with a local or state police force, careful consideration and planning must precede all testing. Frequent

unannounced testing could be detrimental to good relations with local law enforcement and may give cause to the "cry wolf" syndrome. It is recommend that these units conduct testing that stops short of notifying the responding civil police force. In utilizing civil law enforcement as a response force, commands must understand that response times will be dependant upon the civil force's work load. They may get there in 1 min or 1 hour if they are tied up with a traffic fatality, hostage situation, or any other civil priority situation. They will respond, but testing their response time adds very little value when it will be completely dependent upon the size, composition and other activities the responding force is engaged in. Testing should still be conducted as outlined to evaluate the monitoring process.

9. IDS Access Codes. The access codes for the operation and administration of an IDS shall be changed:

a. At least annually.

b. When someone having the code no longer needs it.

c. When the code has been or is suspected of being compromised.

F. Key and Lock Control.

1. Purpose. Key and lock control is one of the first layers of protection at a unit. Physical security is primarily maintained through the use of locks and locking devices both during and after normal working hours. Without strict control of keys and proper hardware, locks provide nothing more than a false sense of security and put unit assets and personnel at risk. Additionally, the proper use of hardware can provide inherent security while removing human error. This chapter establishes guidance for the control and administration of all security and building access related keys. Security related keys are those keys that access locks that protect funds, controlled medical substances, AA&E, and high value assets and the areas in which the keys are stored, and those keys that control access to restricted areas.

2. General

a. A key and lock control system encompassing all security-related keys and locks shall be established at all units. Keys to administrative files, storage cabinets, desks, personal lockers, etc. are not normally security-related and are not required to be included in the key and lock control system.

b. In designing the system, planners must recognize that locks are delay devices only. Lock adequacy and effectiveness will be as good as the

controls placed over them and the quality of lock used. A key and lock control system supplements other security measures used to control access and is essential for the safeguarding of information and property.

c. All units that issue keys shall have a key control officer. The key control officer shall be designated in writing by the commanding officer. Commissioned officers, chief warrant officers, enlisted personnel (E-6 or above), or civilian employees (GS-7 or above) may serve as the key control officer. Multiple designation letters will suffice, provided they include the appropriate responsibilities and references. The designee will be concerned with the supply of locks and how they are stored, the handling of keys, record files, investigation of lost keys, maintenance and operation of key repositories, and the overall supervision of the key and lock control system.

d. Units located within General Service Administration (GSA) buildings need only be concerned with security keys specific to their spaces. These spaces should not be on a master key system with the rest of the building. All other keys for building and general office access is normally managed by GSA.

e. Key custodians may be appointed to assist the key control officer in support of the key and lock control system.

f. The CSO shall have staff responsibility for the key and lock control system. Because of this responsibility, the CSO shall ensure the following is accomplished:

(1) Advise the commanding officer, the key control officer and key custodians on all matters relating to key and lock control systems.

(2) Provide for inspections of systems implemented.

(3) Provide for inspection of locking devices after hours by security personnel.

(4) Initiate an education program pertaining to key control.

3. Key Types.

a. Control Keys. The control key allows for removal and replacement of an interchangeable core (IC). These are normally found in a Master keyed system.

b. Grand Master Keys. A single key which opens a series or system of master keyed lock groups or all lock groups of an entire facility. Sometimes referred to as the Top Master Key (TMK).

c. Master Keys. A single key which opens a series or system of locks. The use of master keys is discouraged. However, if master keyed lock systems are necessary, their use shall be limited to the protection of low value assets such as office spaces.

(1) There are six levels of master keys in a full master key system. Exhibit 2-2 provides a break down of a full master key system.

(2) Some Master key systems are only partial systems and will not contain all of the variable levels. These Master keys are sometimes referred to as Incidental Masters.

d. Operating Keys. The operating key actuates the locking mechanism. Each key shall operate only the individual lock or locks for which the key is designed.

e. Special Keyed Alike (SKA). SKA keys are used for locks that are not to be master keyed in a facility, but require multiple people to have access.

f. Special Keyed Different (SKD). SKD keys are used for locks that are not to be master keyed in a facility, where strict access control is required.

g. Duplicate Keys. Those keys which duplicate operating keys and are usually stored for emergency use (e.g., loss of a key or absence of the holder of the operating key). Duplicate keys shall be stored in a key repository separate from operating keys.

h. Reserve Locks with Keys. Those locks and keys used to rotate other locks or to provide for new requirements. They shall be secured in the same manner as duplicate keys.

4. Security and Control Measures.

a. The number of individuals authorized to draw/retain keys shall be kept to the absolute minimum commensurate with security and operational requirements. Flextime will not be the sole justification for key issuance.

b. Keys shall be issued to individuals who require repeated after hours access or to their individual office space only. Individuals issued keys must be made aware of requirements to safe guard and immediately report the loss of unit issued keys.

c. Operating keys to security areas shall not be issued for personal retention or removal from the unit. This restriction also applies to keys that unlock repositories which contain keys to security areas.

d. Maintenance personnel may only be issued keys to maintenance and common spaces. During working hours, access to other spaces shall be granted only by the custodians of those spaces or the officer of the day (OOD).

e. When keys are not in use, they shall be secured in repository containers of at least 20-gauge steel or material of equivalent strength. Key repositories shall be attached to the structure to prevent easy removal and located in buildings or rooms with structural features which forestall illegal entry. Key repositories shall be located so that they are under the surveillance of operating personnel during duty hours. During non-duty hours, the building shall be locked with both locksets and deadbolts of commercial grade. Deadbolts shall have a minimum of a 1-inch throw.

f. Operating and duplicate keys which control access to repositories containing keys to security areas shall be controlled from and, when not in use, stored in central key repositories under 24 hour control of the security force or other cleared personnel or stored within a locked space. Keys to utility areas shall be controlled by the facility engineer or other designated official.

g. A key repository index shall be maintained for each repository within the key and lock control system. The index shall be used as the basis for inventories of keys controlled from the repository. The index shall be destroyed when superseded or obsolete. Exhibit 2-3 may be used for this purpose.

h. All keys within the key and lock control system shall be kept under continuous administrative accountability at all times. A key control register shall be used to record the issue and turn-in of keys. Key control registers shall contain the signature of the individual receiving the key, date and time of issuance, serial number or other identifying information of the key, signature of the person issuing the key, date and time key was returned, and the signature of the individual receiving the returned key. A separate register shall be maintained for each repository. When not in use the register shall be locked inside the repository to which it pertains. All keys

removed from the repository shall be recorded on the register. Registers shall be maintained for 6 months (after final entry). Exhibit 2-4 may be used for this purpose.

NOTE: Each command will maintain a complete register of keys, both issued and non-issued, by which to account for and conduct inventories from. Commands may keep both indexes and registers electronically, however a separate form recording the keys issued and the receiving members printed name and signature must also be maintained.

i. Keys normally issued and used as a group shall be affixed as a set on rings of at least 12-gauge wire or its equivalent which has been welded or brazed together. Each ring shall include a metal or plastic tag stamped or imprinted with a ring identification code.

j. Replacement or reserve locks, cores and keys shall be secured to preclude accessibility to unauthorized individuals.

k. All keys and padlocks within the key and lock control system shall be physically inventoried by serial number at least once every 6 months. A record of the inventory shall be maintained by the key control officer until completion of the next scheduled inventory.

l. Padlocks in use within the key and lock control system shall be rotated at least once every 12 months. Whenever possible, the rotation should be between different offices rather than within the same office. Padlocks not in use shall be secured, along with the corresponding keys, in a locked metal container which meets the requirements of a key repository. Access to the container shall be controlled in the same manner as for key repositories.

m. Under no circumstances will locks be left hanging open on a hasp, staple, hook or other device. In all cases, locks shall be re-locked immediately after opening with the key removed.

5. Control of Grand Master, Master and Control Keys. The following provisions supplement those outlined above.

a. The easiest method to destroy a master key system is to issue Grand Master or Control keys for personal use to persons who believe they need the key for convenience or status. The loss of either key requires the rekeying of every lock in its system. In larger facilities, this cost can easily reach over $100,000.00. This should be considered the value of the Grand Master and Control key and it must be protected accordingly. Under no

circumstances should a Grand Master key to a facility be issued for routine use.

b. Grand Master keys shall be protected as high value government property. They shall be placed in a SF-700, Security container Information Form, properly filled out with the names of those who are authorized access, sealed and laminated. This key shall be stored in a GSA approved security container and only be accessible to personnel in emergency situations. Standard key repository containers are not authorized for the storage of Grand Master keys.

c. Level I Master keys shall not be issued for personal retention or removal from the unit.

d. Level II-V Master keys shall not normally be issued for personal retention or removal from the unit. Due to the access allowed and the cost associated with re-keying, serious consideration must be given prior to issuance of these keys

e. Level VI Master keys should only be issued to individuals with an established need for access to multiple spaces.

6. Loss of Keys. In the event of lost, misplaced or stolen keys, all locks that could be operated by that key must be replaced or rekeyed immediately. The only exception is for keys that are known to have been lost where the key(s) are unrecoverable (such as over the side in deep water).

G. Security Containers. This section is applicable to all areas storing classified material, funds, AA&E and controlled medical substances.

1. Combinations to all security containers shall be changed:

a. Upon receipt.

b. At least annually.

c. When someone having the combination no longer requires access.

d. When the combination has been compromised or the container has been discovered unlocked and unattended.

2. SF 700, Form, shall be used to record combinations. The envelope shall be appropriately stored in an approved security container. Also, a brief Standard Operating Procedure (SOP) shall be affixed to the outside front of the container, to inform personnel of steps to be taken if the container is found open. For example,

close drawers, do not look through contents of safe, notify duty officer at a certain phone number, etc.

3. SF 701, Activity Security Checklist, shall be used to record area security checks at the close of business or daily checks for 24-hour facilities. Records shall be maintained for 3 months.

4. SF 702, Security Container Check Sheet, shall be used to record the opening/closing of a container. Records shall be maintained for 3 months.

H. Visitor Control.

1. A visitor is any individual not under official orders to the unit or otherwise employed by the unit.

2. The commanding officer of the unit being visited is responsible for the conditions under which visits are permitted. A visitors bill shall be promulgated and include, as a minimum, procedures for identifying visitors, the purpose of their visit, and the control of movement on the unit. The visitor's bill may be incorporated in the physical security plan or the unit's organizational manual.

3. Whenever any visitor expresses an unusual and persistent interest in classified or otherwise sensitive information, the commanding officer shall immediately advise the cognizant SECMGR and Coast Guard Investigative Service (CGIS) Office. A written report shall be forwarded to Commandant (G-CFI) via the cognizant SECMGR. Such reports shall include the following information:

   a. Full name, title or position.

   b. Nationality.

   c. Sponsor.

   d. Authority for the visit.

   e. Items of particular interest to the visitor.

   f. Types of questions asked.

   g. Expressed objective of the visit.

   h. Estimation of the real objective of the visit.

   i. Estimate of the ability, intelligence, and technical knowledge of the visitor and his/her proficiency in the English language.

4. Denial of Entry or Removal of Visitors.

a. The commanding officer shall not delegate the responsibility for denying entry or removal of a visitor. By issuing written "standing orders" to those controlling access, the commanding officer (CO) is not delegating responsibility but rather is delineating his guidance on command security. These "standing orders" must be signed by the current CO and not "by direction". The absence of written guidance from the CO may legally constitute an assumed delegation of responsibility.

b. When such denial of entry or removal occurs for reasons of suspicious or criminal activity, a report shall be made to Commandant (G-CFI), via the cognizant SECMGR. The SECMGR should be kept informed of all possible threat conditions and criminal activity.

EXHIBIT 2-1

EXCERPT FROM TITLE 18 U.S.C. 1382

TITLE 18--CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 67--MILITARY AND NAVY

Sec. 1382. Entering military, naval, or Coast Guard property

Whoever, within the jurisdiction of the United States, goes upon any military, naval, or Coast Guard reservation, post, fort, arsenal, yard, station, or installation, for any purpose prohibited by law or lawful regulation; or

Whoever reenters or is found within any such reservation, post, fort, arsenal, yard, station, or installation, after having been removed therefrom or ordered not to reenter by any officer or person in command or charge thereof--

Shall be fined under this title or imprisoned not more than six months, or both.

(June 25, 1948, ch. 645, 62 Stat. 765; Sept. 13, 1994, Pub. L. 103-322, title XXXIII, Sec. 330016(1)(G), 108 Stat. 2147.)

Historical and Revision Notes

Based on title 18, U.S.C., 1940 ed., Sec. 97 (Mar. 4, 1909, ch. 321, Sec. 45, 35 Stat. 1097; Mar. 28, 1940, ch. 73, 54 Stat. 80).

Reference to territory, Canal Zone, Puerto Rico and the Philippine Islands was omitted as covered by definition of United States in section 5 of this title.

Words ``naval or Coast Guard'' were inserted before ``reservation'' and words ``yard, station, or installation'' were inserted after ``arsenal'' in two places, so as to extend section to naval or Coast Guard property.

Minor changes were made in phraseology.

Amendments

1994-Pub. L. 103-322 substituted ``fined under this title'' for ``fined not more than $500'' in last paragraph.

Transfer of Functions

Functions of all officers of Department of the Treasury, and functions of all agencies and employees of such Department transferred, with certain exceptions, to Secretary of the Treasury, with power vested in him to authorize their performance or performance of any of his functions, by any of such officers, agencies, and employees, by Reorg. Plan No. 26 of 1950, Secs. 1, 2, eff. July 31, 1950, 15 F.R. 4935, 64 Stat. 1280, 1281, set out in the Appendix to Title 5, Government Organization and Employees. Coast Guard, referred to in this section, was generally a service in Department of the Treasury, but such Plan excepted from transfer functions of Coast Guard and Commandant thereof when Coast Guard was operating as a part of the Navy under sections 1 and 3 of Title 14, Coast Guard.

Coast Guard transferred to Department of Transportation and all functions, powers, and duties, relating to Coast Guard, of Secretary of the Treasury and of other offices and officers of Department of the Treasury transferred to Secretary of Transportation by Pub. L. 89-670, Oct. 15, 1966, 80 Stat. 931, which created the Department of Transportation. See section 108 of Title 49, Transportation.

Canal Zone

Applicability of this section to Canal Zone, see section 14 of this title.

EXHIBIT 2-2

Master Key systems

Master key systems consist of several levels, each of which can open the levels below it. Proper planning is a must in a Master key system. Below is an example of the level of incidental masters contained in a six pin system.

6 PIN TUMBLER SYSTEM

# of keys	Level of Key	Access level key provides
1	**Grand Master**	**Can open <u>all locks</u> keyed on the same Master Key system**
4	**Level II**	**Incidental Masters - Each key can operate ¼ of the locks below a level II key.**
16	**Level III**	**Incidental Masters - Each key can operate ¼ of the locks below a level III key**
64	**Level IV**	**Incidental Masters - Each key can operate ¼ of the locks below a level IV key**
256	**Level V**	**Incidental Masters - Each key can operate ¼ of the locks below a level V key.**
1024	**Level VI**	**Incidental Masters - Each key can operate ¼ of the locks below a level VI key.**
4096	**Operating (Change)**	**This is the lowest level in the system. Each key opens one or more specific lock.**

On the following page is a graphical representation of the Master key system as it relates to the table above. Due to space limitations, only one full branch is shown.

EXHIBIT 2-2

The following is a graphical representation of the Master key system as it relates to the preceding table.

Due to space limitations, only one full branch is shown.

In this example, lock AAADB4 can be opened by keys; AAADB4, AAADB, AAAD, AAA, AA, A and the Grand Master.

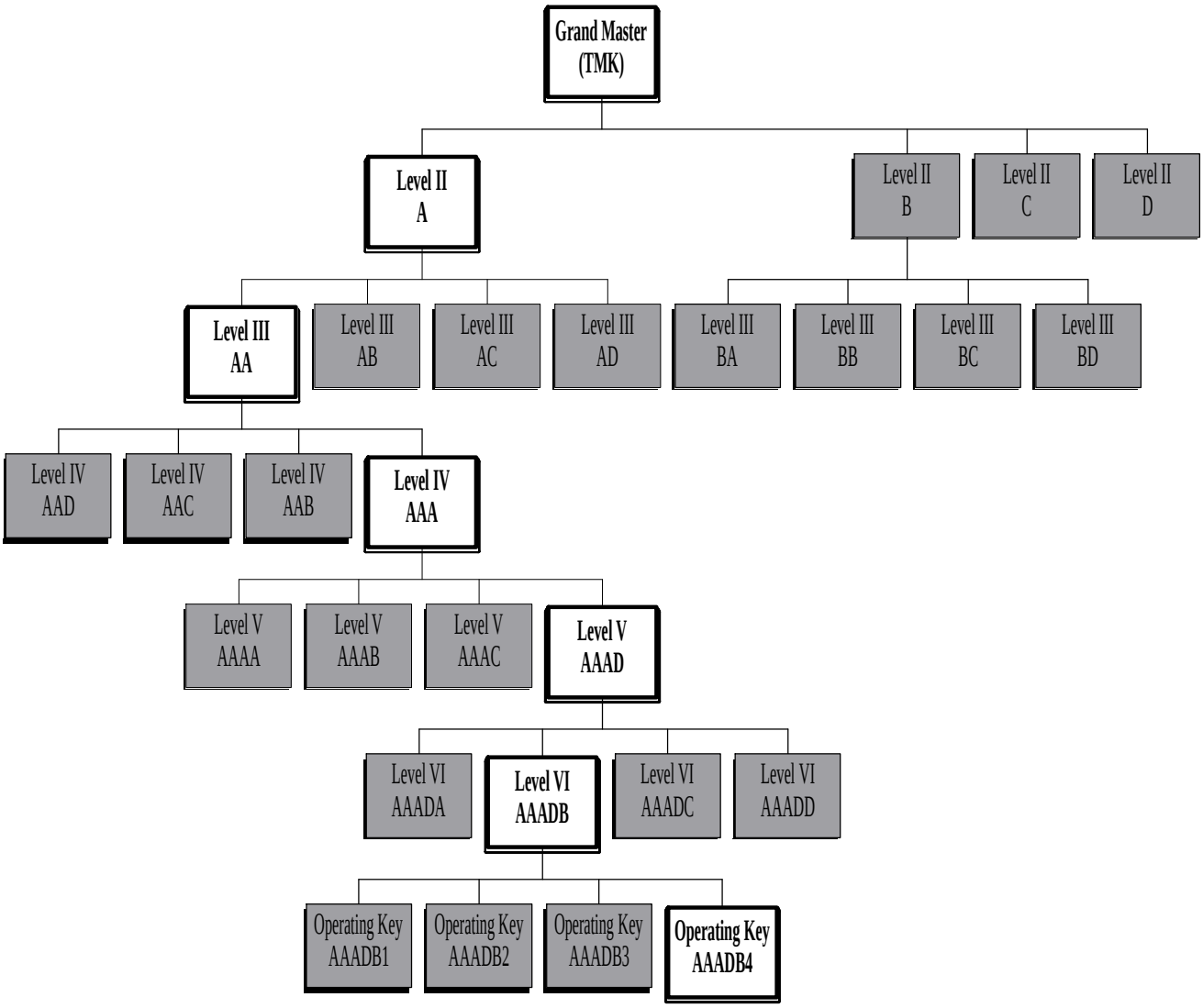


EXHIBIT 2-3

KEY REPOSITORY INDEX

REPOSITORY NUMBER		LOCATION OF REPOSITORY	
RING NUMBER	**KEY SERIAL NUMBER**	**LOCK LOCATION** (BUILDING, DOOR, CAGE NUMBER, ETC,.)	**NUMBER OF KEYS**

KEY CONTROL REGISTER

REPOSITORY NUMBER	LOCATION OF REPOSITORY

ISSUE					RETURN		
DATE	TIME	SERIAL NUMBER OF KEY(S)	PRINT NAME OF RECEIVER - SIGNATURE	SIGNATURE OF INDIVIDUAL ISSUING KEY(S)	DATE	TIME	PRINT NAME OF RECEIVER - SIGNATURE

EXHIBIT 2-4

Chapter 3 PHYSICAL SECURITY OF ARMS, AMMUNITION AND EXPLOSIVES (AA&E)

A. Purpose. This chapter establishes uniform policies and standards for physical security protection of sensitive conventional AA&E during their life cycle. The standards outlined within this chapter apply to all AA&E aboard Coast Guard facilities, including privately-owned weapons stored on a Coast Guard unit and the firearms and ammunition held for sale by Coast Guard Exchange System (CGES) activities.

B. Discussion.

1. The likelihood that thefts and unaccountable losses of AA&E will jeopardize the safety of personnel and cause damage/destruction demands that personnel judiciously comply with this chapter and apply sufficient personnel and funds to assure the development and maintenance of an adequate security posture. Compliance shall be an integral part of the overall unit physical security plan.

2. Existing facilities shall be replaced only when it has been determined by the cognizant SECMGR, Commandant (G-CFI) and the cognizant MLC and/or Civil Engineering Unit (CEU) that such facilities cannot be upgraded and/or measures cannot be applied to provide equivalent security protection.

3. When a ship is underway, a lower level of security is acceptable to be consistent with the accomplishment of the mission. Modification, relocation or tearing out of AA&E storage spaces/lockers aboard ship shall be specifically approved by the cognizant SECMGR, Commandant (G-CFI) and (G-SEN).

4. Commanding officers shall ensure that CGES activities under their jurisdiction sell firearms and/or ammunition in strict compliance with these standards. CGES officers and managers shall establish local procedures with their host commands to ensure that the sale of firearms and ammunition to patrons under the command's jurisdiction comply with these standards. CGES firearms and ammunition must be stored in compliance with the standards outlined here during store non-operating hours. No firearms or ammunition can remain in display cases on the floor when the store is closed.

C. Cost Reduction Measures. Commanding officers shall apply measures to concurrently protect against AA&E thefts and unaccountable losses and minimize costs for compliance with this chapter. Examples of such measures are:

1. Where practical, reducing the quantities of AA&E in custody of operational units consistent with operational and training requirements.

2. Where practical, reducing the quantities of AA&E which require physical protection and accountability by giving priority attention to

demilitarization/disposal of outdated and unserviceable AA&E, per, Ordnance Manual, COMDTINST M8000.2 and Small Arms Manual, COMDTINST M8370.11.

D. Waivers and Exceptions. If it is not feasible or practical (due to excessive costs) to meet the construction standards in this chapter, requests for waivers and exceptions (based on the application of compensatory measures) shall be requested. Chapter 1 provides policy and guidance for requesting waivers and exceptions. An information copy of approved requests pertaining to AA&E shall also be forwarded to Commandant (G-OCU).

E. Physical Security Objectives. Physical security objectives are to assure the use of cost effective, state-of-the-art security hardware, devices, equipment and systems which can serve as countermeasures to constantly changing attack techniques, tools, methods and/or targeting trends employed by terrorists, saboteurs or criminal elements.

F. Physical Security Planning. Chapter 1 outlines basic physical security planning requirements. Provisions of this section supplement those requirements.

1. Background

a. The acquisition of AA&E worldwide has been recognized as a prerequisite for the continued operations of violence oriented terrorist organizations and highly organized criminal elements. Stocks of AA&E in magazines and armories; disaffected military and civilian employees; and AA&E shipments via commercial and military modes are lucrative sources for obtaining quantities of AA&E which have high damage and destructive capabilities.

b. The increased activities of terrorists and criminal elements in recent years require continuous comprehensive AA&E security planning. This must be tailored to the overall physical security operations of each unit in order to assure the maximum use of available assets and capabilities to counter changes in attack techniques, technology and trends in targeting by such elements.

2. Plans Documentation and Review.

a. Commanding officers responsible for AA&E security shall issue directives that cover all phases of AA&E security. Such plans shall be reviewed at least annually for currency and compliance with this chapter. Factors which shall be considered include: threat assessments furnished by local intelligence commands or law enforcement agencies; types and sensitivities of AA&E to be safeguarded; location, size and construction of storage areas; vulnerability of AA&E to thefts or unaccountable losses; geographic location; and the capability of available security and emergency response

forces. Such information shall be designated as FOR OFFICIAL USE ONLY (FOUO).

b. Plans must recognize the need for actions to counter potential thefts by employees. Such actions include screening personnel for reliability, and monitoring inventory, accountability and disposal of AA&E to detect concealed shortages, which present opportunities for hidden employee thefts. Losses in operational or training environments dictate the need for attention and procedures to assure strict AA&E accountability and complete and accurate crosschecks during issue, expenditure and turn-in.

3. Coordination and Liaison.

a. It is vital to the protection of AA&E that close coordination and liaison exist between commanding officers and outside agencies. The objectives shall be to identify and acquire protection in depth, delineate jurisdictional authority and responsibilities to avoid duplication of effort, and where permissible, allow for exchanges of intelligence information which may support or interface with contingency plans of other agencies that will enhance local security operations.

b. Plans shall provide for the full use of outside sources in investigating AA&E losses and for sources of information concerning anticipated terrorist or criminal activities which may impact on the protection of AA&E assets. Such sources include: Coast Guard Investigative Service (CGIS), Federal Bureau of Investigation (FBI) field offices, state and local law enforcement agencies, military intelligence and investigative agencies, Bureau of Alcohol, Tobacco and Firearms (ATF) field offices, and host country agencies, where applicable.

G. Security Risk Categories.

1. Arms.

a. Category I. Non-nuclear missiles and rockets in a ready to fire configuration (e.g., Hamlet, Redeye, Stinger, Dragon, LAW, Viper). This category also applies in situations where the launcher tube and the explosive rounds, though not in a "ready to fire" configuration, are jointly stored or transported.

b. Category II. Light automatic weapons up to and including .50 caliber, i.e., M16 rifle and M60 machine guns.

c. Category III.

(1) Launch tube and gripstock for Stinger missile. *

(2) Launch tube, sight assembly and gripstock for Hamlet and Redeye missiles. *

(3) Tracker for Dragon missiles. *

(4) Mortar tubes excluding the 4.2 inch. *

(5) Grenade launchers (MK79 and M203).

(6) Rocket and missile launchers, with an unpacked weight of 100 pounds or less. *

(7) Flame Throwers. *

(8) The launcher and/or missile guidance set and/or the optical sight for the TOW. *

d. Category IV.

(1) Shoulder fired weapons, other than grenade launchers, not fully automatic, i.e., Shoulder Line Throwing Gun (SLTG), morale rifles.

(2) Handguns.

(3) Recoilless rifles up to and including 90 mm.*

2. Ammunition and Explosives.

a. Category I. Explosive complete rounds for Category I missiles and rockets. *

b. Category II.

(1) Hand or rifle grenades, high explosive and white phosphorus. *

(2) Mines, antitank and antipersonnel (unpacked weight of 50 pounds or less each). *

(3) Explosives used in demolition operations; e.g., C-4, dynamite, block TNT. *

c. Category III.

(1) Ammunition, .50 caliber and larger, with explosive filled projectile (unpacked weight of 100 pounds or less each).

(2) Grenades, concussion, incendiary, and fuses for high explosive grenades.

(3) Blasting caps. *

(4) Detonating cord. *

(5) Supplementary charges. *

(6) Bulk explosives used in the production of ammunition that can be used with a minimum of other ingredients or devices to detonate. *

d. Category IV.

(1) Ammunition with non-explosive projectile (unpacked weight of 100 pounds or less each).

(2) Grenades: illumination, smoke, and CS/CN (tear producing).

(3) Incendiary destroyers. *

(4) Riot control agents, 100 pound package or less.

(5) Ammunition for categories II through IV weapons not otherwise categorized.

(6) Fuses, except for paragraph 3.G.2.c.(2), above.

(7) Pyrotechnics.

* These items are not currently used by Coast Guard units, but are listed in the event that they are obtained for mobilization or storage for another agency.

H. Accountability. Small Arms Manual, COMDTINST M8370.11 establishes accountability and inventory requirements, including procedures for reporting missing, lost or stolen AA&E.

I. Access Control.

1. Routine or unaccompanied access shall be limited to the least number of responsible persons designated by the commanding officer. The names and positions of these persons shall be designated in writing by the commanding officer and posted inside the arms storage area. Commanding officers shall prohibit any persons on whom derogatory information casts serious doubt as to their trustworthiness from unaccompanied access to arms storage areas.

2. More than one unit may use the same arms storage area as a consolidated space. If so, weapons shall be partitioned off by a wire cage and identified by unit, when feasible. If it is not feasible to separate unit weapons by use of a partition, one commanding officer shall be designated as having overall security responsibility. Procedures shall be established to fix responsibility for access, issue, and receipt for all sensitive items stored in the arms storage area. Units with small quantities of weapons shall use weapons containers for separation. When unit weapons are separated by a partition, each unit shall maintain interior security for its own weapons. However, one designated commanding officer shall continue to have responsibility for exterior security and access. Procedures for such consolidated arrangements shall be outlined in the unit's weapons security Standard Operating Procedure (SOP).

J. Key Control. Chapter 2 outlines basic key control requirements. Provisions of this section supplement those requirements.

1. Keys to AA&E storage areas and Intrusion Detection Systems (IDSs) shall be maintained separately from other keys, and be accessible only to those individuals whose official duties require access to them. A current list of these individuals shall be kept within the unit, agency, or organization and protected from public view.

   a. The number of keys shall be held to the minimum essential. Keys shall not be left unattended or unsecured at any time. 24 hour positive control shall be maintained on all keys to AA&E storage areas.

   b. When not in use, keys shall be secured in containers of at least 20 gauge steel, or material of equivalent strength, and equipped with a three position, changeable combination lock or a combination padlock with hasp (e.g., Sargent & Greenleaf). Keys to arms storage areas shall not be removed from the unit except to provide for protected storage elsewhere.

   c. The use of a master key system for protecting AA&E ashore is prohibited. Master key systems are authorized for high security locks only within a single storage space on board ships; however, they are not to be utilized for multiple spaces.

2. An AA&E key control officer shall be designated in writing by the commanding officer. Commissioned officers, chief warrant officers, enlisted personnel (E-6 or above), or civilian employees (GS-7 or above) may serve as the AA&E key control officer. This individual may be the same person as the overall unit key control officer. A separate letter of designation is not required; multiple designation letters will suffice, provided they include the appropriate responsibilities and references.

3. Completed AA&E key control registers shall be maintained for 6 months (after final entry).

4. When individuals are charged with the responsibility for safeguarding or otherwise having keys immediately available, they shall sign for a sealed envelope of keys. When the sealed envelope of keys is transferred from one individual to another, the unbroken seal is evidence that the keys have not been disturbed.

K. Intrusion Detection Systems (IDS). Chapter 2 outlines basic IDS requirements. Provisions of this section supplement those requirements.

1. General.

a. IDSs are an essential part of the overall AA&E physical security system and must be carefully integrated with all other aspects of physical security upgrading.

b. The design and application of an IDS for AA&E protection is related to the risk category of the AA&E being stored, the location of the storage structures and the hardness of the structures. Non-hardened structures such as frame construction weapons spaces require additional types of sensors to protect the more vulnerable characteristics of such areas.

c. The requirements for hardening of structures and for use of locks and locking devices should be met prior to or concurrently with the installation of IDS for magazines.

d. Design schematics for the IDS covering AA&E storage areas should be protected as sensitive but unclassified. An exception to this would be for those areas in which classified AA&E is stored; those schematics should be classified in accordance with guidance for that particular ordnance.

2. Security Telephone Systems. Security telephone systems should be installed between alarm control centers and alarmed zones to provide for controlled entry by authorized personnel during working hours and as an additional mode for communications during non-working hours. Such systems are used not only by ordnance handling and safety personnel for accessing magazines, but also by

roving security patrols for required routine call-ins to avoid broadcasting patrol positions, and as a communication mode additional to radio during emergencies.

L. Security and Police Forces. Chapter 10 outlines basic security and police force requirements. Provisions of this section supplement those requirements.

1. Units shall review the status of security and police forces assigned to protect AA&E at least annually. Such reviews shall include operational capabilities, adequacy of orientation and training, and the currency of post orders.

2. Security and police force response to IDS alarms shall have an objective of 15 minutes for arms storage areas. The force that responds to AA&E alarms shall be armed. Local law enforcement agencies may be used for this purpose, provided a written support agreement or Memorandum of Understanding (MOU) has been established. Units not able to meet the 15 minute response objective shall (at a minimum) submit a letter to the nearest law enforcement agency (with a copy to the cognizant security manager (SECMGR)), notifying them of their location and the type of weapons on hand. Exclude quantities for Operations Security (OPSEC) considerations.

3. Security and police forces ashore shall be provided with reliable, efficient primary and backup external and internal communication systems, one of which shall be radio. These systems shall be established for magazines and magazine areas to permit notification of emergency situations. Backup systems shall be of a type other than the primary. Systems shall be easily accessible to security personnel on their fixed and mobile posts and shall be tested at least once during each shift.

M. Restricted Area Designation. Chapter 2 outlines basic restricted area requirements. Provisions of this section supplement those requirements.

1. Personnel and Vehicle Movement Control. Areas where AA&E are stored shall be designated and posted as restricted areas. Privately Owned Vehicles (POV) shall be prohibited in restricted AA&E areas with the exception of POVs with valid orders to transport AA&E. All vehicles, their drivers, other occupants and cargo being transported shall be immediately identified when vehicles seek to enter or depart restricted areas where AA&E is stored. Methods employed shall include strict enforcement of a property pass system, vehicle trip authorization system with documents carried by drivers, and routine and/or random conveyance inspections or searches.

2. Removal from Secure Storage. AA&E removed from secure storage shall not be left overnight or during weekends in structures or conveyances which have not been approved for storage per this chapter.

N. Fencing. Chapter 2 outlines basic fencing requirements. Provisions of this section supplement those requirements. The requirement for fencing of AA&E storage areas shall be determined on an individual case by case basis, by the criteria herein and by site surveys. Factors that shall be considered are potential threats, proximity of storage areas to public property, isolation of storage areas, sensitivity of AA&E in storage, and overall levels of other security being provided or planned. The requirement for a large quantity of fencing around the entire outer perimeter of an area may not be essential or cost effective. If an outer perimeter has security fencing, then security fencing of inner zone AA&E storage areas may not be required. If an outer perimeter has barbed wire fencing or no fencing, then security fencing of inner zone AA&E storage areas may be required. If an outer perimeter is partially fenced with security fence, then it may be cost effective to install fencing to complete the loop, rather than to install security fencing around structures storing AA&E in the inner zone. If natural barriers, such as mountains, cliffs, rivers, seas or other terrain which are difficult to traverse, form portions of the perimeter and provide equivalent or better security than fencing, then security fencing of inner zone storage areas may be more practical and cost effective than fencing the perimeter.

O. Lighting. Chapter 2 outlines basic lighting requirements. Provisions of this section supplement those requirements. Protective lighting shall be provided at all exterior doors of AA&E storage areas. Exterior lights shall be positioned so that identification may be made of personnel requesting entry while not impairing the vision of the occupant of the area. Areas appropriate for this lighting are building entrances, corridors and entrance doors to rooms. Switches to exterior lights shall be located so that they are not readily accessible to unauthorized persons.

P. Arms Storage Requirements.

1. Policy.

a. Category I and II arms shall be stored in an approved armory or in a Class 5, GSA approved weapons container within a weapons space. Outside of approved armories, the use of approved arms racks for weapons storage is only authorized for mobile units and only when space and weight constraints, and/or approved operational readiness circumstances dictate. In addition, one of the following requirements shall be met:

(1) Continuous 24 hour live watch. A live watch is defined as "awake and alert", not "sleeping and breathing".

(a) For afloat units, this requirement is met if a quarterdeck watch is continuously maintained.

(2) Protected by an IDS that is supported by an armed response.

b. Category III and IV arms shall be stored in an approved armory, or in a Class 5, GSA approved weapons container within a weapons space. Outside of approved armories, the use of approved arms racks for weapons storage is only authorized for mobile units and only when space and weight constraints, and/or approved operational readiness circumstances dictate. The use of arms racks for weapons storage necessitates the implementation of one of the requirements of subparagraphs P.1.a.(1) or (2) above.

2. Containers. Any weapons container with an empty weight of less than 500 pounds shall be secured to the premises unless it is protected by an IDS or located within an armory or vault. It may be secured by bolts and/or heavy metal straps, welded, or if it is intended to remain part of the structure, it may be secured by imbedding it in concrete.

3. Arms Racks.

a. Arms racks shall be equivalent to standard Mosler models and be locked with installed high security locks or padlocks having steel shackles and bodies which meet or exceed the resistance requirements for forced or surreptitious entry of A-A-1927D (American Model Number 5200 meets this specification). Arms racks shall be fastened to the structure with bolts or with chains equipped with the same padlocks prescribed above. Chains used to secure racks shall be heavy duty hardened steel, welded, straight link galvanized and at least 5/16 inch thickness or of equivalent resistance to force required to cut/break the padlocks prescribed above. An example of an equivalent chain is type 1, Grade C, Class 4, NSN 4010-00-149-5583, NSN 4010-00-149-5575, or NSN 4010-00-171-4427. Those racks utilizing hinged locking bars shall have the hinge pins peened or welded to prevent removal.

b. Loose-fitting hardware can allow weapons to be removed from the rack or disassembled in the rack. To ensure the weapon pockets have not slipped out of adjustment, they shall be checked quarterly for proper fit of the weapons in the racks and proper placement of the weapon pockets on the rack.

4. Exception. Units not able to meet the requirements of paragraphs 3-P-1-a or 3-P-1-b above may store their AA&E at sites owned or managed by other government agencies or local police departments, subject to the following provisions:

a. A written support agreement or MOU with the holding agency shall be established.

b. A receipt from the holding agency listing all weapons by serial number and type, and ammunition by quantity and type shall be retained.

c. The accountability requirements of Small Arms Manual, COMDTINST M8370.11 shall be met and inventories shall be conducted by Coast Guard personnel.

d. The holding agency must be able to provide security equal to or greater than that required by this chapter.

e. Coast Guard personnel must have immediate access (not to exceed 1 hour) to the weapons and ammunition.

5. Storage in Private Residences. Coast Guard owned weapons and ammunition for agents, competitive shooting team members, morale, etc. may be stored in private residences, subject to the following provisions:

a. Due to the "cost versus risk", it is not practical for personnel to modify construction levels in their homes. An emphasis must be placed on common sense precautions and reasonable security measures taken to prevent loss or theft.

b. Weapons and ammunition shall be stored out of plain sight, preferably in a locked interior closet or cabinet. The quantity of ammunition stored shall not exceed a total Net Explosive Weight (N.E.W.) of 15 pounds. See Navy Gun Ammunition, SW030-AA-MMO-010 or contact your district armory.

c. Garages should not normally be used for storage; however, if this is the best location for security or safety reasons, the door shall be locked and there should be no indication weapons are stored therein.

d. Storage of weapons and ammunition shall conform to all local ordinances and regulations.

e. When weapons are not in use, the installation of "Gun safety locks" is mandatory to prevent the firearm from being discharged. These locks are approximately $10.00 each and will guard against the accidental firing of weapons in the home. **CAUTION**: **Ensure that the firearm is unloaded before installing any gun safety lock.**

Q. Ammunition and Explosives (A&E) Storage Requirements.

1. Policy. Ready service ammunition shall be stored in either an armory, a Class 5 GSA approved weapons container within a weapons space or in approved magazines. All other ammunition and all explosives shall be stored in approved

magazines. On board all cutters, construction in accordance with current ships plans is acceptable for A&E storage. Specifications and drawings for approved magazines may be obtained from the Naval Facility Engineering Command (NAVFAC), Atlantic Division, 1510 Gilbert Street, Norfolk, VA 23511-2699, (757) 322-4205.

2. Security Standards.

a. Doors to magazines shall be of solid steel construction as delineated in latest approved NAVFAC drawings.

b. Openings such as vents, windows and ducts to magazines and buildings shall be constructed to provide equivalent penetration resistance as that provided by the walls of magazines, buildings and structures.

3. Exception. To maintain an acceptable balance between security and unit operational requirements in responding to Search and Rescue (SAR) without unnecessary delay, area and district commanders may authorize the storage of pyrotechnics (pyro) onboard their ready SAR resources.

a. All ready pyro shall be accounted for daily by sight and logged in a permanent record. Pyro not required to be available for immediate SAR response, or immediate small boat response on cutters underway, shall be stored in accordance with this chapter. Pyro found in life rafts is exempt from the storage requirements of this chapter.

b. The security of pyro is extremely important. Personnel shall judiciously comply with all accountability and loss reporting requirements. Area and district commanders shall determine and promulgate suitable pyro storage plans for their nonstandard SAR resources without type manuals. These security provisions shall be included in physical security plans as outlined in Chapter 1.

R. Armory Construction Specifications. On board all cutters, armory construction in accordance with current ship plans is acceptable. The following standards apply to shore-based armories:

1. Walls. Walls shall consist of 8 inches of concrete reinforced with No. 4 reinforcing bars placed vertically at 9 inches on center in each direction and staggered horizontally on each face to form a grid approximately 4 1/2 inches square; or alternatively, 8 inch concrete block with No. 4 bars threaded through the block cavities filled with mortar or concrete and with horizontal joint reinforcement at every course; or as a minimum 8 inches of brick interlocked between inner and outer courses. Alternatively, a modular type vault designed and approved for

AA&E storage may be used; however, the design must provide a degree of security equivalent to the design standards of this section.

2. Ceilings and Roofs. Ceilings and roofs shall be designed to provide a comparable degree of security as that of the walls. Reinforcing bar spacing shall form a grid approximately 4 1/2 inches square, utilizing No. 4 reinforcing bars or larger. If the ceiling or roof is of concrete pan-joist construction, the thinnest portion shall not be less than 6 inches and the clear space between joists will not exceed 20 inches; the reinforcing grid requirements for flat slab construction also apply. Roof structures and ceilings of existing facilities shall provide an equal or greater degree of security than that required for windows and doors.

3. Floors. Floors, if on grade, shall be a minimum of 6 inches concrete construction reinforced with 6 x 6 or W4 x W4 mesh or equivalent bars. Where the floor slab acts as the ceiling for an underlying room or area, the ceiling standards apply.

4. Doors.

   a. Doors shall be constructed of 1 3/4 inch thick solid wood or laminated wood with 12 gauge steel plate on the outside face, or be industrial type 1 3/4 inch thick, hollow steel construction with a minimum 14 gauge skin plate thickness, internally reinforced with vertical continuous steel stiffeners spaced 6 inches maximum on center.

   b. Door bucks, frames and keepers shall be rigidly anchored and provided with antispread space filler reinforcements to prevent disengagement of the lock bolt by prying or jacking the doorframe. The frames and locks for both interior and exterior doors shall, in addition, be so designed and installed as to prevent removal of the frame facing or the built-in locking mechanism sufficiently to disengage the lock bolt from outside of the secured room when the door is closed and locked.

   c. Construction requirements for doorframes and thresholds should be as exacting as those for the doors themselves. For example, where metal doors are utilized, the frame and threshold also should be of metal of minimum 14 gauge thickness.

   d. The main entrance door shall be equipped with a high security locking system, consisting of the Sargent and Greenleaf (S&G) 831B padlock coupled with the NAPEC Mark II (MOD VIII), NAPEC (Mark II MOD IX), or one of the BMR TUFLOC series 60 locks. A GSA approved steel vault door with a built-in three position, dial type, changeable (Group 1R) combination lock, may be used in lieu of other doors or locks.

e. The main entrance door of armories shall be equipped with an inside locking device or bar for use when the space is manned (day gate).

5. Hinges.

a. Hinges shall be located on the inside of the space whenever possible and will be of sufficient strength and size to withstand constant use and the usual weight of the doors. Hinges shall be of the fixed pin security hinge type or the hinge pin shall be peened or welded to prevent removal.

b. All exterior doors with exposed hinges shall also be provided with two or more supplemental brackets, pins or other devices to prevent opening of the door by removal of the hinge pin or destruction of the exposed portion of the hinge. The devices used shall provide sufficient positive engagement and resistance to shearing forces to prevent opening of the door at the hinge side (edge) of the door.

6. Windows and Other Openings. Windows are prohibited. Ducts, vents, or similar openings of a size sufficient to permit entry or removal of arms (90 square inches or greater) shall be equipped with:

a. Hardened steel bars (3/4 inch or larger in diameter) provided the vertical bars are not more than 4 inches apart with horizontal bars welded to the vertical bars in such a manner that the openings do not exceed 32 square inches; or

b. Riveted steel grating (weight of 13.2 lbs./sq. ft) or welded steel grating (weight of 8.1 lbs./sq. ft) with 1 X 3/16 bearing bars (See Military Handbook (MILHDBK) 1013/5, steel plywall hardening selection and installation guide, MIL-G 18014B, Type A, Class B).

c. Bars and steel grating shall be securely embedded in the structure of the building or welded to a steel frame which shall be securely attached to the wall with fasteners inaccessible from the exterior of the arms storage area.

S. Weapons Space Specifications. Non-armory spaces used for weapons storage are referred to as “weapons spaces.” They do not meet the construction standards for armories and are used in conjunction with Class 5 GSA approved weapons containers. Weapons storage racks are not authorized for use in weapons spaces at shoreside facilities. On board all cutters, weapons space construction in accordance with current ship plans is acceptable. The following standards apply to shore-based weapons spaces:

1. Walls. Walls shall be permanent in nature and be constructed as a solid barrier from true floor to true ceiling.

2. Ceilings and Floors. Standard construction for ceilings and floors is acceptable. Spaces containing drop ceilings may only be used if no other suitable space is available, unless walls are constructed true floor to true ceiling. If drop ceilings must be used, compensatory measures as determined by the cognizant security manager are required.

3. Doors. Doors for weapons spaces shall be 1 ¾ inch thick, solid wood or laminated wood with 12 gauge steel plate on the outside face.

4. Locks. Weapons spaces shall be equipped with both lock sets and dead bolts of commercial grade, capable of accepting a high security cylinder or 7 pin keyway. Dead bolts shall have a minimum of a 1 inch throw. Strike plates shall be reinforced with 3 ½ inch screws.

5. Hinges. Hinges for weapons spaces shall be affixed with 3 ½ inch screws to secure them to the door jamb. Hinges shall be located on the inside of the space whenever possible and will be of sufficient strength and size to withstand constant use and the usual weight of the doors. Hinges located on the exterior shall be of the fixed pin security hinge type or the hinge pin shall be peened or welded to prevent removal.

6. Windows and Other Openings. Weapons Spaces should not normally contain windows. Where windows are present, they shall be secured in a permanent manner to prevent them from being opened. Windows, ducts, vents, or similar openings of a size sufficient to permit entry or removal of arms (90 square inches or greater) shall be equipped with:

   a. Riveted steel grating (weight of 13.2 lbs./sq. ft) or welded steel grating (weight of 8.1 lbs./sq. ft) with 1 X 3/16 bearing bars (See Military Handbook (MILHDBK) 1013/5, steel plywall hardening selection and installation guide, MIL-G 18014B, Type A, Class B).

   b. Steel grating shall be securely embedded in the structure of the building or welded to a steel frame which shall be securely attached to the wall with fasteners inaccessible from the exterior of the arms storage area.

7. Intrusion Detection System (IDS). Weapons spaces shall be equipped with an IDS, with a minimum of a BMS and motion sensor.

T. Shipboard Doors/Hatches.

1. Main entrances to AA&E spaces shall be provided with normal and emergency lighting adequate to provide sufficient lighting for examination of locking devices during periods of reduced visibility. Topside lockers and entrances to AA&E spaces opening onto weather decks are excluded from this requirement.

2. The main access to AA&E storage areas shall be secured with high security hardware as outlined in paragraph 3-R-4-d.

3. Doors to A&E storage areas (less Category I) require high security hardware unless such areas are served by a common compartment on the same deck with a single entrance meeting the high security hardware requirements. All other access doors shall be secured from the inside with sliding bolts, bars, or pins, or with padlocks on the outside.

4. Power or manually operated doors operated only from within the secured area do not require a locking system.

5. Under no circumstances will emergency escape scuttles and hatches be padlocked.

6. Scuttles and hatches shall be of the type that open only from the inside or contain a quick release locking pin.

U. Arms Ammunition and Explosives (AA&E) Shipments and Transporting. COMDTINST M8370.11, Small Arms Manual, outlines requirements for transporting and shipments of firearms and ammunition.

Chapter 4 TECHNICAL SECURITY COUNTERMEASURES (TSCM) PROGRAM

A. General

1. Electronic surveillance has become a low cost method of information collection. Electronic sensors and instruments are readily available to the general public. How to and cookbook type information about these devices is readily available via the Internet and the public library. These techniques are being used not only by organized crime and foreign intelligence agencies but also by commercial industry and the general public to gather information for a competitive edge against the Coast Guard. The target is usually information such as drug interdiction and defense related operational plans, and long range operational and funding information that gives away our capabilities and intentions. However, any information that you wish to protect is at risk. The Coast Guard's TSCM program looks for information collection and transmission devices as well as physical security vulnerabilities and counters the threat through detection, prevention and recovery.

2. TSCM services are highly specialized surveys/inspections and as such, are particularly vulnerable to compromise. In order for a TSCM survey to be effective and to protect the information involved, certain restrictions pertain. All information concerning timing, location, equipment, or methodology employed in a TSCM survey, (or its findings), which if divulged would tend to aid in circumventing the survey is classified. This includes all correspondence and discussion regarding requests for pending TSCM surveys and results of completed surveys/inspections. The effectiveness of a TSCM Survey depends on the strict adherence to these guidelines. Coordination for receiving services should be arranged through the cognizant Security Manager or Headquarters Command Security Officer.

B. Purpose

The purpose of the program is to protect sensitive and classified information, which if revealed to unauthorized personnel would damage the National Security or the Internal Security and missions of the Secretary of Transportation or the Coast Guard. This is accomplished through the function of detecting and preventing unauthorized disclosure through technical means.

C. Background

1. Historically, foreign intelligence services have employed technical devices in espionage operations directed against U. S. installations, to gain access to national security information. In today's world, foreign intelligence services are also used to gather information on treaties and for economic gain.

2. The Coast Guard, as a military and law enforcement agency that also enters into political negotiations for fisheries and seagoing commerce, routinely handles

classified defense information, and sensitive but unclassified law enforcement and economic information. Off the shelf technology, available to virtually anyone, including organized criminal elements and terrorists, has greatly increased the ability and potential for technical surveillance.

D. Policy

1. Protecting sensitive discussion areas from technical penetration is the responsibility of every commander. A comprehensive security program should be established for the protection of all sensitive discussion areas. When discussions at the TOP SECRET/SCI level are held within a space on a daily or otherwise routine basis, TSCM support performed by qualified technical security specialists should be requested.

2. The Chief of Coast Guard Security (G-CFI) serves as the TSCM Program Manager within the Coast Guard and is responsible for providing TSCM support, technical direction and centralized management of all Coast Guard TSCM efforts, and TSCM support for the Secretary of Transportation.

3. The TSCM program manager (G-CFI) is the sole activity within the Coast Guard authorized to procure and use equipment for TSCM purposes. Coast Guard commands shall obtain TSCM support only from or via Commandant (G-CFI) and by no other agency or activity. This restriction includes support for Sensitive Coast Guard sponsored projects at contractor facilities.

4. All Coast Guard TSCM services shall be conducted in accordance with DoT Order 1650.1, Technical Security Countermeasures Program and Security Policy Board Procedural Guides 1, 2, and 3.

E. Discussion.

1. Selection of Spaces Requiring TSCM Support. Due to the cost of technical manpower, travel and equipment, reasonable selectivity must be exercised in identifying spaces to receive TSCM support. At the discretion of the Chief of Coast Guard Security (G-CFI), TSCM support will be provided in accordance with the following criteria:

   a. Qualifying Spaces/Facilities. Support will be provided for those spaces where highly sensitive or classified discussions take place routinely and which have continuous access controls established as part of an effective security program to preclude undetected access. Guidance to achieve this is provided elsewhere in this instruction.

   b. Conferences. Conferences, symposiums, exhibits, clinics, conventions and meetings involving sensitive or classified discussions should be held in

secure spaces. When such facilities are not available, one-time meetings will be supported if they are held in facilities not open to the general public, have the potential for good audio and physical security throughout the conference, and the information scheduled for discussion is classified TOP SECRET.

c. Flag Offices/Residences. TSCM surveys of flag offices and quarters, because of their targetability, may be provided despite minimal security provisions. It should be noted that TSCM surveys conducted under such conditions have no residual value and it cannot be assumed after the survey that such spaces will continue to be safe for sensitive discussions.

d. New/Renovated Facilities. Normally, new installations or spaces having undergone major renovations will not receive TSCM support until all construction is completed, the spaces are manned, are fully operational and security measures are implemented. Pre-construction liaison with the SECMGR and TSCM program manager is encouraged to ensure the standards set forth herein are clearly understood and incorporated into the construction or modification plans.

e. Ships/Aircraft. TSCM support will not normally be provided to Coast Guard ships or aircraft because of the low technical security threat which exists while they are deployed.

2. Recurring Support. No facility will qualify automatically for routinely recurring TSCM service. In principle, once an area has been the subject of a fully instrumented TSCM survey with favorable outcome, the results are considered valid as long as the security integrity of the facility is maintained. The need for recurring service will be determined by the TSCM program manager based on a formalized threat assessment.

NOTE: Unless justified and approved by the Chief of Coast Guard Security (G-CFI), TSCM support will not normally be provided to areas that have had previous support if major discrepancies were identified and no corrective action has been initiated.

3. Operational Security (OPSEC). In order for a TSCM survey to be effective and to protect the information involved, certain restrictions pertain. **No discussion of the TSCM Survey or related information shall take place, prior to and during the conduct of a survey, in or around the areas of interest.** It must be assumed until the survey indicates otherwise, that a clandestine intercept device is actually in place. Should discussions concerning the pending support take place within the space, the device would likely be removed prior to the survey and later reinstalled or simply be switched off remotely. To find a device that is turned off is difficult at best. Under such circumstances the probability of surfacing a clandestine intercept

device is greatly diminished. This applies to the time before, during and after the TSCM Survey. **The effectiveness of a survey depends on the strict adherence to these guidelines.** Written requests for TSCM service are to be handled in accordance with the classification guidance provided within this chapter, and the number of persons apprised kept to an absolute minimum. **Non-secure telephone requests for TSCM support are considered compromised and are not authorized**. Coast Guard TSCM team members will be issued annual travel orders and other measures shall be taken to protect TSCM operations.

F. Finds. Upon the discovery of a suspected technical device, **do not attempt to remove the device.** Immediately take action to secure the area to preclude attempts to remove the device. **Immediately notify Commandant (G-CFI) of the discovery, via secure means (STU-III or Secret Message) through the cognizant SECMGR. If possible, the secure call should be placed at a location other than the building in which the discovery was made. If the device has been located in a "secure" area, then you should suspect that other secure areas within the building have also been compromised.** No information concerning the discovery of the device shall be released to other persons until such time as Commandant (G-CFI) directs.

G. Support

1. Sensitive Compartmented Information Facilities (SCIF's) and Communications (COMSEC) Security Facilities will normally be scheduled for TSCM Surveys by Commandant (G-CFI) via the cognizant SECMGR. The cognizant SECMGR shall keep Commandant (G-CFI) informed on the status of all new construction and renovations of spaces and facilities which are normally surveyed. For a detailed list of required information to be sent to (G-CFI) prior to a survey see Exhibit 4-1.

2. When a unit that processes, discusses, or stores any level of classified or sensitive information suspects a technical penetration, they shall immediately notify their cognizant SECMGR. The cognizant SECMGR shall immediately notify Commandant (G-CFI). The procedures listed in paragraph 4.E.3. and 4.H. shall be strictly complied with.

3. The cognizant SECMGR shall then contact (G-CFI) to obtain further detailed information regarding program support.

4. Survey Request Procedure. Commanding Officers and Officers-in-Charge requiring unscheduled support, will submit their requests through their cognizant SECMGR to Commandant (G-CFI), with as much lead-time as possible. The procedures listed in paragraph 4.E.3. and 4.H. must be strictly complied with.

   a. Requests must include, as a minimum, the following facility information:

(1) Complete identification of the area requiring TSCM support, to include:

(a) Name of the area

(b) Room number

(c) Building number

(d) Address

(e) Floor plan

(f) Electrical and telephone wiring diagrams.

(g) Air conditioning and heating duct diagrams.

(h) "As built" construction blueprints.

(i) List of adjacent tenants bordering the entire perimeter of the area to be inspected (including those above and below).

(j) Square footage of the area.

NOTE: For a detailed list of required information to be sent to (G-CFI) prior to a survey see Enclosure (4).

(2) Identity and telephone number of the command point of contact and an alternate.

(3) Clearance requirements for the TSCM support personnel.

(4) Date of last TSCM report and the status of previous recommendations provided, if any.

(5) Information that may impact on the scheduling, i.e., date scheduled construction will commence, completion date of construction in progress, etc. Should unexpected events which could interfere with a TSCM survey occur after support has been scheduled, the requester should notify the program manager as soon as possible to prevent unnecessary expenditures of manpower and funds.

b. Commands will normally be notified of the survey team's arrival date via classified message.

c. Upon arrival, the survey team will report to the commanding officer or the designated point-of-contact.

d. At completion of the survey, the team will out-brief the command about the findings of the survey and will provide a classified written report to the command via the chain of command upon return to headquarters.

e. Requests for a one-time conference or meeting should be received by Commandant (G-CFI) sixty (60) days prior to the event.

H. Classification Guidance. All correspondence and discussion regarding a TSCM Survey, request for services or the discovery of a suspected technical device, shall be classified at the **SECRET** level. All correspondence will carry the following classification caveats: "**WARNING NOTICE: INTELLIGENCE SOURCES OR METHODS INVOLVED"**, and "**NOFORN**."

CL By: 2181532
CL Reason: 1.5(c)
Decl on: X1
Drv From: SEC 9-82

I. TSCM Reports

1. As an adjunct to a command's security program, TSCM security technicians can provide TSCM threat briefings to command personnel. The briefings are classified and will normally be provided after completion of TSCM support for a facility or installation.

2. Commands will ensure that weaknesses identified as a result of TSCM services are corrected. If corrective action is required, notify Commandant (G-CFI) in writing via the cognizant SECMGR, within 60 days, of the corrective action or the status of pending corrective action. If corrective actions are delayed due to non-availability of funding, supply a copy of your budget request for the corrective action.

3. The most recent TSCM survey report and all related correspondence shall be maintained on file.

Chapter 5 TERRORIST THREAT CONDITIONS (THREATCONs)

A. Purpose. This chapter establishes uniform procedures and measures for use in responding to progressive levels of terrorist threats to Coast Guard units ashore and afloat. These terms, definitions and recommended security measures are intended to facilitate both Coast Guard and inter-agency support of Antiterrorism activities. The Threat Conditions (THREATCONs) listed below do not directly correlate to Defense Readiness Conditions (DEFCONs) which are wartime postures set by the National Command Authorities. The Coast Guard THREATCONs are consistent with those of Joint Pub 3-07.2, Tactics, Techniques, and Procedures for Antiterrorism.

B. Responsibilities.

1. Commandant (G-CFI) is the program manager for threat countermeasures, as it relates to actions and measures to deter, detect, defeat and respond vigorously to all terrorist attacks, and the protection of Coast Guard resources, information, personnel, facilities, assets, and critical infrastructure. Commandant (G-CCS) is responsible for directing the implementation of a Coast Guard-wide THREATCON. Area commanders shall direct an area-wide THREATCON. District commanders shall direct a THREATCON throughout the district, including headquarters and area units geographically located within their district. Commanding officers may direct THREATCONs for units within their area of responsibility (AOR). Once a THREATCON is declared, the selected security measures are implemented immediately.

2. Areas, Districts and commanding officers may declare a higher THREATCON within their AOR, but may not lower a THREATCON imposed by higher authority.

3. Individual units should generate local instructions and procedures adapting the THREATCON measures to meet local command structure and assets, operational environment, special evolutions, and other unit specific factors.

4. Liaison should be established with local, state, and federal law enforcement agencies to develop a system whereby information about anticipated threats can be shared in a regular and timely manner.

5. Attainment reports are required, unless otherwise directed.

6. The command or unit's role in terrorism prevention and protection.

   a. The U.S. Coast Guard is responsible for the security of its facilities, assets, resources, personnel, and information (Internal Security). It is also responsible for the development and implementation of security standards with respect to terrorist attacks on maritime activities, including but not

necessarily limited to assaults on passenger ships, cargo vessels, and navigation aids (External Security). Regular liaison should be maintained with all local representative agencies to ensure the efficient and timely flow of threat information.

b. When information is received that suggests that an act may, will or has taken place, a report by message to your operational commander and the local FBI must be sent. The FBI maintains jurisdiction over terrorism within the U. S.; however, the Coast Guard will provide assistance as required. Also, notify the National Terrorism Hotline, 800-424-8802, manned by the Coast Guard National Response Center in Washington, DC.

NOTE: When Coast Guard units and personnel are under the Operational Control (OPCON) of a joint force commander or component commander of a Commander-in-Chief (CINC), they will implement the THREATCONs of that commander.

7. In the event that a terrorist action does occur aboard a Coast Guard unit, District, Area and local OPLANs should be consulted for specific actions required.

8. During heightened threat conditions, tenant commands shall work with their host command to identify areas where they can augment and assist in providing security in depth for the combined facility.

C. Threat Analysis and Assessment Factors. Identification and characterization of terrorist threats to personnel and assets is the first step in developing an antiterrorism plan. Once commanders understand the threat they can assess their ability to prevent, survive, and respond to an attack. Threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, trends, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying the probability of a terrorist attack and results in a threat assessment. The following general assessment factors should be used when considering implementation of THREATCONs. These factors apply only to the assessment of terrorist threats against U.S. interests. Assessment factors are:

1. Existence. Applies when a terrorist group is present, assessed to be present, or able to gain access to an area of concern. Group need not have posed a threat to U.S. interests in the past.

2. Capability. Applies when a terrorist group has acquired, been assessed to have, or demonstrated the ability to carry out an operation against U.S. interests in areas of concern. This includes resources such as intelligence, mobility, personnel, etc.

3. Intentions. Applies when a terrorist group has recently demonstrated anti-U.S. terrorist activity, or stated or assessed intent to conduct such activity. Terrorist groups often display behaviors which are clear, unambiguous indicators of intent.

4. History. Demonstrated terrorist activity over time. Applies when a group's history of terrorist acts and behavior reflects an anti-U.S. stand or includes previous attacks against U.S. interests. Activity need not have been violent; i.e., terrorist attack against U.S. interest could be rhetorical or threatening utterances or statements.

5. Targeting. Applies if there are known plans or confirmed intentions and preparation of a terrorist group to target U.S. interests. Targeting can be either specific or non-specific. If targeting is not against U.S. interests, this factor should not be considered.

6. Security Environment. Internal political and security considerations that impact on the capability of terrorist elements to carry out their intentions.

D. Levels of Threat. Terrorist Threat Levels are a five-step scale of standardized terms used to describe the severity of threats based upon intelligence community judgements on the likelihood of terrorist attack. Threat levels are the result of combinations of the threat analysis and assessment factors discussed above. The factor, Security Environment, is considered separately as a modifying factor and will influence the assigned threat level. The applicability of any or all of the assessment factors, as defined above, will produce a threat level that is negligible, low, medium, high or critical.

1. NEGLIGIBLE. Existence and/or capability may or may not be present

2. LOW. Factors of existence and capability must be present. History may or may not be present.

3. MEDIUM. Factors of existence, capability and history must be present. Intentions and trends may or may not be present.

4. HIGH. Factors of existence, capability, history, intentions and trends must be present.

5. CRITICAL. Factors of existence, capability, and targeting of U.S. interests must be present. History, intentions and trends may or may not be present.

> **NOTE:** Terrorist Threat Level HIGH is differentiated from CRITICAL because analysts lack targeting information. It is differentiated from MEDIUM because analysts have sufficient credible information to assess the threat factor of Intentions toward U.S. Government interests.

E. Threat Condition (THREATCON) Definitions. Threat assessments include assigned threat levels and provide the latest details on terrorist activities for a particular location. While there is no direct correlation between threat information, (e.g., Intelligence Summaries, Warning Reports, and Spot Reports), and THREATCONs, such assessments provide information to assist commanders in determining the appropriate THREATCON to declare. THREATCONs may also be suffixed with the geographic area deemed at risk. Once a THREATCON is declared, the selected measures should be implemented immediately. THREATCONs have the following associated conditional meanings:

1. THREATCON NORMAL. This condition applies when a general threat of possible terrorist activity exists but warrants only routine security posture.

2. THREATCON ALPHA. This condition applies when there is a general threat of possible terrorist activity directed against units and personnel, the nature and extent of which are unpredictable, and the circumstances do not justify full implementation of the measures of THREATCON BRAVO. However, it may be necessary to implement certain selected measures from THREATCON BRAVO as a result of intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

3. THREATCON BRAVO. This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, without affecting operational capability, and without aggravating relations with local authorities. All previous measures remain in effect.

4. THREATCON CHARLIE. This condition applies when an incident occurs or when intelligence is received indicating that some form of terrorist action against units and personnel is imminent. Implementation of this measure for more than a short period will probably create hardship and will affect the peacetime activities of the unit and its personnel. All previous measures remain in effect.

5. THREATCON DELTA. This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

F. Suggested Protective Measures.

1. General. The measures outlined below are for use aboard all U.S. Coast Guard commands. These measures serve two purposes: first, the crew is alerted, additional watches are created, and there is greater security; second, these measures display the command's resolve to prepare for and counter the terrorist threat. These actions will convey to anyone observing the command's activities that the unit is prepared and that the particular facility is an undesirable target.

The measures outlined below do not account for local conditions and regulations, special evolutions, or current threat intelligence. The command must maintain flexibility. As threat conditions change, the unit must be prepared to take action to counter the threat. When necessary, additional measures must be taken immediately.

a. THREATCON ALPHA Measures

(1) MEASURE 1. At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of United States installations. Watch for abandoned parcels or suitcases and any unusual activity. Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

(2) MEASURE 2. The Command Security Officer (CSO), duty officer or other appointed personnel with access to building plans as well as the plans for area evacuations must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available.

(3) MEASURE 3. Secure buildings, rooms, and storage areas not in regular use.

(4) MEASURE 4. Increase security spot checks of vehicles and persons entering the unit and unclassified areas under the jurisdiction of the Coast Guard.

(5) MEASURE 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

(6) MEASURE 6. As a deterrent, apply measures 14, 15, 16, 17, or 18 from THREATCON BRAVO, either individually or in combination with each other.

(7) MEASURE 7. Review all plans, orders, personnel details, and logistic requirements related to the introduction of higher THREATCONs. Arrange firearms qualification and training to ensure a sufficient number of qualified personnel for increased THREATCON postures.

(8) MEASURE 8. Review and implement, as appropriate, security measures for high-risk personnel. Your nearest Coast Guard

Investigative Service (CGIS) office should be consulted regarding protective service operations and advice. Notify your cognizant Security Manager when this measure is implemented.

(9) MEASURE 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

(10) MEASURE 10. To be determined.

b. THREATCON BRAVO Measures.

(1) MEASURE 11. Repeat Measure 1 and warn personnel of any other potential form of terrorist attack.

(2) MEASURE 12. Keep all personnel involved in implementing anti-terrorist contingency plans on immediate recall.

(3) MEASURE 13. Review all plans, orders, personnel details and logistic requirements related to the implementation of the measures contained in the next higher THREATCON.

(4) MEASURE 14. Where possible, cars and such objects as crates, trash containers, etc., are to be moved at least 100 feet from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the application of centralized parking.

(5) MEASURE 15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

(6) MEASURE 16. At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

(7) MEASURE 17. Examine all mail for letter or parcel bombs. This examination is increased above normal.

(8) MEASURE 18. Check all deliveries to messes, clubs, etc. Advise dependents to check all home deliveries.

(9) MEASURE 19. Increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and dependents.

(10) MEASURE 20. Update staff and dependents on the general situation in order to stop rumors and prevent unnecessary alarm.

(11) MEASURE 21. At an early stage, inform security personnel of any action being taken and why.

(12) MEASURE 22. Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers. Identify the visitor's destination. Ensure that proper dignity is maintained and, if possible, ensure that female visitors are inspected only by a female qualified to conduct physical inspections.

(13) MEASURE 23. Operate random patrols to check vehicles, personnel, and buildings. Increase security surveillance of waterfront areas including wharfs, piers, caissons, critical communications facilities/assets, etc.

(14) MEASURE 24. Protect off-base military personnel and military vehicles in accordance with prepared plans. Remind drivers to lock parked vehicles and to institute a positive system of checking before they enter and drive a vehicle.

(15) MEASURE 25. Implement additional security measures for high-risk personnel, as appropriate. Your nearest Coast Guard Investigative Service (CGIS) office should be consulted regarding protective service operations and advice. Notify your cognizant Security Manager when this measure is implemented.

(16) MEASURE 26. Brief personnel who may augment security forces on the use of deadly force. Ensure that there is no misunderstanding of these instructions.

(17) MEASURE 27. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

(18) MEASURE 28 and 29. To be determined.

c. THREATCON CHARLIE Measures.

(1) MEASURE 30. Continue all THREATCON ALPHA and BRAVO measures and introduce those that remain outstanding. Review all plans, orders, personnel details and logistic requirements related to the introduction of the next higher THREATCON.

(2) MEASURE 31. Keep all personnel responsible for implementing antiterrorist plans at their places of duty.

(3) MEASURE 32. Limit access points to the absolute minimum.

(4) MEASURE 33. Strictly enforce control of entry and randomly search vehicles.

(5) MEASURE 34. Enforce centralized parking of vehicles away from sensitive buildings.

(6) MEASURE 35. Issue weapons and protective equipment to security forces. Local orders should include specific instruction on issue of ammunition. Ensure that armed personnel are briefed on and fully understand Commandant's Use Of Force Policy, the current threat posture, and the Rules of Engagement.

(7) MEASURE 36. Introduce increased patrolling of the unit.

(8) MEASURE 37. Protect all designated Vulnerable Points (VPs) and give special attention to VPs outside military establishments. VPs should be identified in your Physical Security Plan.

(9) MEASURE 38. Erect barriers and obstacles to control traffic flow.

(10) MEASURE 39. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to attacks.

(11) MEASURE 40. To be determined.

d. THREATCON DELTA Measures.

(1) MEASURE 41. Continue or introduce all measures listed for THREATCONs ALPHA, BRAVO and CHARLIE.

(2) MEASURE 42. Augment security forces as necessary.

(3) MEASURE 43. Identify all vehicles already on the unit within operational or mission support areas.

(4) MEASURE 44. Search all vehicles and their contents before allowing entrance to the unit.

(5) MEASURE 45. Control all access and implement positive identification of all personnel with no exceptions. Strictly control access to areas affected by terrorist actions. Allow only properly identified security force, investigators, and emergency aid personnel to enter.

(6) MEASURE 46. Search all suitcases, briefcases, and packages brought into the unit.

(7) MEASURE 47. Control access to all areas under the jurisdiction of the Coast Guard.

(8) MEASURE 48. Make frequent checks of the exterior of concerned buildings and parking areas.

(9) MEASURE 49. Cancel all nonessential administrative journeys and visits.

(10) MEASURE 50. Coordinate the possible closing of public and military roads and facilities with local authorities.

(11) MEASURE 51. To be determined.

2. Shipboard Terrorist THREATCON Measures. The unique nature of the shipboard environment requires additional considerations that generally do not apply to the stateside fixed facility. In addition to the basic THREATCON procedures, a variety of other tasks may need to be performed by the cutter. This is particularly true for units deploying to areas where the threat of terrorist attack is high, or to areas where they may be under the Operational Control of a DoD Theater CINC or Joint Force Commander.

a. The measures outlined below are for use aboard U.S. Coast Guard cutters. Emphasis is directed toward antiterrorism measures designed to protect vessels in port or at anchorage. While the simple solution to THREATCON CHARLIE or DELTA is to get underway, this option may not always be available.

b. Additionally, units deploying under DoD Theater CINC or Joint Force Commander control, shall conduct a pre-deployment vulnerability assessment prior to deployment and shall implement appropriate protection measures to reduce risk and vulnerability. Assessments and the subsequent implementation of standards must occur in a timely manner, and should be incorporated in pre-deployment planning and training. Pre-deployment assessments should assist commanders in updating AOR specific training

and in obtaining necessary physical security materials and equipment to implement protective measures.

c. These measures are intended as supplemental to the general measures outlined in paragraph 5.F.1. above.

(1) THREATCON ALPHA Measures

(a) MEASURE S-1. Brief crew on threat, ship security, and security precautions to be taken while ashore.

(b) MEASURE S-2. Muster and brief security personnel on the threat and rules of engagement, and on Commandant's "Use of Force" policy.

(c) MEASURE S-3. Review security plans and keep them available. Keep essential personnel who may be needed to implement security measures on call.

(d) MEASURE S-4. Commands shall assess the security threat to their unit. Consistent with local rules and regulations, post qualified armed sentries aboard the vessel as needed. Arrange firearms qualification and training to ensure a sufficient number of qualified personnel for increased THREATCON postures.

(e) MEASURE S-5. Commands shall assess the security threat to their unit. Consistent with local rules and regulations, post a qualified armed pier sentry and pier entrance sentry as needed.

(f) MEASURE S-6. Issue two-way radios to all sentries, roving patrols, quarterdeck watch and response force. If practical, all security personnel shall be equipped with at least two systems of communication. Encrypted communications should be used at all times.

(g) MEASURE S-7. Issue night vision devices to selected posted security personnel.

(h) MEASURE S-8. Coordinate pier/fleet-landing security with SOPA, collocated forces, and local authorities. Identify anticipated needs for mutual support (security personnel, boats, and equipment) and define methods of activation and communication.

(i) MEASURE S-9. Tighten shipboard and pier access control procedures. Positively identify all personnel entering pier/fleet-landing area.

(j) MEASURE S-10. Consistent with local rules, regulations, and status of forces agreement, establish unloading zones on the pier away from ship.

(k) MEASURE S-11. Where possible, deploy barriers to keep vehicles away from the ship. Barriers may be ship's vehicles, equipment, or items available locally.

(l) MEASURE S-12. Post signs in local languages to explain visiting and loitering restrictions.

(m) MEASURE S-13. All occupants of vehicles entering pier shall be required to display identification. Suspicious personnel/vehicles shall be inspected for weapons and /or explosives.

(n) MEASURE S-14. Inspect all personnel, hand-carried items, and packages before they come aboard. Where possible, screening should be at the pier entrance or foot of brow.

(o) MEASURE S-15. Direct departing and arriving liberty boats to make a security tour around the ship and give special attention to the waterline and hull. Boats must be identifiable night and day to ship's personnel.

(p) MEASURE S-16. Water taxis, ferries, bum boats, and other harbor craft require special concern because they can serve as ideal platforms for terrorists. Unauthorized craft should be kept away from the ship; authorized craft should be carefully controlled, surveilled, and covered.

(q) MEASURE S-17. Identify and inspect work boats.

(r) MEASURE S-18. Secure spaces not in use.

(s) MEASURE S-19. Regulate shipboard lighting to best meet the threat environment. Lighting should include illumination of the waterline on both sides of the vessel.

(t) MEASURE S-20. Rig hawsehole covers and rat guards on lines, cables, and hoses. Consider using an anchor collar.

(u) MESURE S-21. Raise accommodation ladders, stern gates, and jacob ladders when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.

(v) MEASURE S-22. Conduct security drills to include bomb threat and repel boarders exercises.

(w) MEASURE S-23. Review all plans, orders, personnel and logistic requirements related to the individual actions in THREATCON BRAVO for possible implementation.

(x) MEASURE S-24. To be determined.

(2) THREATCON BRAVO Measures:

(a) MEASURE S-25. Maintain appropriate THREATCON ALPHA measures.

(b) MEASURE S-26. Review liberty policy in light of the threat and revise it as necessary to maintain safety and security of ship and crew. Enforce a liberty curfew.

(c) MEASURE S-27. Conduct divisional quarters at foul weather parade to determine status of on-board personnel and disseminate information. Brief crew to ensure they understand the additional security requirements, to stop rumors and to prevent undue alarm.

(d) MEASURE S-28. Ensure an up-to-date list of bilingual personnel for the operational area is readily available. Ensure warning tape in pilot house/quarterdeck that warns small craft to remain clear is in both the local language and English.

(e) MEASURE S-29. Remind all personnel to: (a) be suspicious and inquisitive of strangers, particularly those carrying suitcases or other containers; (b) be alert for abandoned parcels or suitcases; (c) be alert for unattended vehicles in the vicinity; (d) be wary of any unusual activities; (e) notify the OOD of any suspicions.

(f) MEASURE S-30. Remind personnel to lock their parked vehicles and carefully check them before entering.

(g) MEASURE S-31. Designate and brief picketboat crews. Prepare boats and place crews on fifteen minute alert. If situation warrants, make random picket boat patrols in immediate vicinity of the ship with the ship's small boat. Boat crews should be armed with rifles and issued appropriate protective equipment.

(h) MEASURE S-32. Under the supervision of an armed sentry, establish brow watch on pier to check identification and inspect personnel and baggage before personnel board ship. If available, employ metal and explosives detection equipment.

(i) MEASURE S-33. Man Signal Bridge or pilot house and ensure flares are available to ward off approaching craft.

(j) MEASURE S-34. Consistent with local rules, regulations, and status of forces agreement, CO should establish and post enough qualified armed sentries to maintain full surveillance of the vessel and immediate pier areas and entrances. Sentries should be armed with rifles and issued appropriate protective equipment.

(k) MEASURE S-35. Consistent with local rules, regulations, and status of forces agreement, arm members of the quarterdeck watch and issue appropriate protective equipment.

(l) MEASURE S-36. Consistent with local rules, regulations, and status of forces agreement, provide shotgun and ammunition to quarterdeck and issue appropriate protective equipment. If situation warrants, place sentry with shotgun inside the superstructure at a site from which the Quarterdeck can be covered.

(m) MEASURE S-37. Issue arms and appropriate protective equipment to selected qualified personnel to include OOD and JOOD.

(n) MEASURE S-38. Consistent with local rules, regulations, and status of forces agreement, establish an armed security patrol when the situation warrants.

(o) MEASURE S-39. Muster and brief ammunition loaders/handlers and messengers.

(p) MEASURE S-40. Implement procedures for expedient issue of firearms and ammunition from ship's armory. Ensure a set of armory keys is readily available and in possession of an officer designated for this duty by the commanding officer.

(q) MEASURE S-41. Load additional small arms magazines to ensure adequate supply for security personnel and response forces.

(r) MEASURE S-42. Inform local authorities of actions being taken as THREATCON increases.

(s) MEASURE S-43. Test communications with local authorities and other U.S. Coast Guard/U.S.Navy vessels in port.

(t) MEASURE S-44. Instruct watches to conduct frequent random searches under piers, with emphasis on potential hiding places, pier pilings, and floating debris.

(u) MEASURE S-45. Conduct searches of the ship's hull and boats at intermittent intervals and immediately before it puts to sea.

(v) MEASURE S-46. Move cars and objects such as crates and trash containers 100 feet from the ship.

(w) MEASURE S-47. Hoist boats aboard when not in use. Picketboats should remain ready for launch.

(x) MEASURE S-48. Terminate all public visits.

(y) MEASURE S-49. Set material condition YOKE, main deck and below.

(z) MEASURE S-50. After working hours, reduce entry points to ship's interior by securing selected entrances from inside.

(aa) MEASURE S-51. Duty department heads ensure all spaces not in regular use are secured and inspected periodically.

(bb) MEASURE S-52. If two brows are rigged, remove one of them.

(cc) MEASURE S-53. Maintain capability to get underway on short notice or as specified by SOPA. Consider possible relocation sites. Rig brow/accommodation ladder for immediate raising/removal.

(dd) MEASURE S-54. Ensure .50 cal mounts are in place with ammunition in ready service lockers (.50 cal machine guns themselves will be maintained in the armory, pre-fire checks completed, ready for use).

(ee) MEASURE S-55. Prepare fire hoses. Brief designated personnel on procedures for repelling boarders, small boats, and ultra-light aircraft.

(ff) MEASURE S-56. Obstruct possible helicopter landing areas in such a manner as to prevent hostile helicopters from landing. If unable to obstruct, maintain surveillance of all possible landing areas.

(gg) MEASURE S-57. Review riot/crowd control procedures, asylum seeker procedures, and bomb threat procedures.

(hh) MEASURE S-58. Monitor local communications (ship to ship, TV, radio, police scanners, etc.).

(ii) MEASURE S-59. Implement additional security measures for high-risk personnel as appropriate. Your nearest Coast Guard Investigative Service (CGIS) office should be consulted regarding protective service operations and advice. Notify your cognizant Security Manager when this measure is implemented.

(jj) MEASURE S-60. Review all plans, orders, personnel details and logistic requirements related to the implementation of the individual actions in THREATCON CHARLIE.

(kk) MEASURE S-61 and S-62. To be determined.

(3) THREATCON CHARLIE Measures:

(a) MEASURE S-63. Maintain appropriate THREATCON ALPHA and BRAVO measures.

(b) MEASURE S-64. Cancel liberty. Execute emergency recall.

(c) MEASURE S-65. Be prepared to get underway on one (1) hour's notice or less. If conditions warrant, request permission to sortie.

(d) MEASURE S-66. Augment existing security watches and deploy sentries to protect command structure.

(e) MEASURE S-67. Place armed sentries on a superstructure level from which they can best cover areas about the ship.

(f) MEASURE S-68. Establish .50 cal or machine gun positions.

(g) MEASURE S-69. If available, deploy STINGER surface-to-air missiles in accordance with established rules of engagement.

(h) MEASURE S-70. If not restricted by environmental obstacles, man surface search, air search, and navigational radar to assist in early detection and warning. Coordinate with SOPA.

(i) MEASURE S-71. Ships with high-power sonars operate actively for random periods to deter underwater activity. Man passive sonar capable of detecting boats, swimmers, or underwater vehicles. Position any non-sonar-equipped ships within the acoustic envelope of sonar-equipped ships. Coordinate with SOPA.

(j) MEASURE S-72. Man one or more repair lockers. Establish communications with an extra watch in Damage Control Central.

(k) MEASURE S-73. Deploy ship's small boat. Boats should be identifiable night and day from the ship (e.g., by lights or flags).

(l) MEASURE S-74. At discretion of CO, deploy helicopter as observation platform. Helicopter should be identifiable

night and day from the ship. If not deployed, the helicopter should be hangared.

(m) MEASURE S-75. Activate antiswimmer watch. (Portions of watch may already be implemented by previous THREATCON measures).

(n) MEASURE S-76. Issue weapons and appropriate protective equipment to other selected Officers and Chief Petty Officers in the duty section.

(o) MEASURE S-77. Units with concussion grenades shall issue them to topside security personnel.

(p) MEASURE S-78. Erect barriers and obstacles as required to control traffic flow.

(q) MEASURE S-79. Strictly, enforce entry control procedures and searches.

(r) MEASURE S-80. Enforce boat exclusion zone.

(s) MEASURE S-81. Cancel all nonessential off-ship administrative trips.

(t) MEASURE S-82. Discontinue contract work. Limit topside work parties.

(u) MEASURE S-83. Set material condition ZEBRA, main deck and below.

(v) MEASURE S-84. Secure from the inside all unguarded entry points to the interior of the ship.

(w) MEASURE S-85. Rotate screws and cycle rudders at frequent and irregular intervals.

(x) MEASURE S-86. Rig additional firehoses. Charge the firehoses when manned just prior to actual use.

(y) MEASURE S-87. Review all plans, orders, personnel details and logistic requirements related to the implementation of the individual actions in THREATCON DELTA.

(z) MEASURE S-88. To be determined.

(4) THREATCON DELTA Measures:

(a) MEASURE S-89. Maintain appropriate THREATCON ALPHA, BRAVO and CHARLIE measures.

(b) MEASURE S-90. Permit only necessary personnel topside.

(c) MEASURE S-91. Prepare to get underway and, if possible, cancel port visit and depart.

(d) MEASURE S-92. If available, post qualified armed sentries with fully automatic weapons and protective equipment to cover possible helicopter landing areas.

(e) MEASURE S-93. Arm sufficient number of ship's crew to fully man a self defense force. Issue appropriate protective equipment.

(f) MEASURE S-94. If available, deploy grenade launchers to cover approaches to ship.

(g) MEASURE S-95. To be determined.

3. Aviation Facility Terrorist THREATCON Measures. In addition to basic THREATCON procedures, a variety of other tasks may need to be performed at aviation facilities. This is particularly true for airbases located in areas where the threat of terrorist attacks is high.

a. Airfields represent special security challenges because of the unique character of facilities and the assets they support. All of the foregoing discussion applies to airfields. Airfield security planners may also wish to consider the establishment of multiple internal security perimeters, hardening of selected buildings against terrorist attack, hardening of petroleum storage areas, aircrew facilities, maintenance facilities, and other facilities collocated on the installation.

b. In the process of securing structures and facilities, however, it is important to examine runways and taxiways with great care. These are not merely slabs of asphalt and concrete poured on the ground; they are intricate, complex architectural structures containing all the building elements normally associated with complex high-rise office or apartment buildings. Runways and taxiways are criss-crossed with electrical, water, and sewer lines. There are often distribution systems buried adjacent to or underneath

portions of runway and taxiway structures. The process of constructing two-to-three mile long stretches of pavement often requires substantial reconfiguration of the local topography, creating the need for extensive drainage and storm-water management systems. Thus, airfields abound with vulnerable utility penetrations not often seen in other facility environments.

c. Airfields are often adjacent to areas with substantial wildlife activity. Exterior intrusion alarm systems are prone to provide much data on movement which is regarded as false, i.e., non-human. Exterior intrusion alarms applied without great care to airfield perimeter security barriers can actually degrade security by desensitizing security personnel responsible for classification and assessment of the threat information that is being reported.

d. Another unique aspect of airfield security is the nature of the activity and the type of assets to be found there. Aircraft generally are most vulnerable to mechanical problems, human error, or ground-to-air attack during landings and takeoff. The requirements to maintain lift at low speeds generally restricts aircraft operation to a fairly narrow corridor within a few degrees of the direction of the airfield runways. The performance envelope of aircraft also restricts the volume of airspace in which an aircraft can operate within a few miles of an airfield.

e. The introduction of sophisticated electronic systems to support aircraft takeoffs and landings in all weather and visibility conditions has also added additional vulnerabilities to airfield activities. Attacks on airfield electronics could be devastating.

f. Hence, airfields have an exceptional requirement for beyond-the-perimeter surveillance. They may also have an exceptional requirement for beyond-the-perimeter response. Consideration should be given to planning for the establishment of observation posts in off-base areas beneath or adjacent to flight paths for landings and takeoffs.

g. All of the unique vulnerabilities outlined above require the airfield commander to consider additional measures in protecting their assets. The following measures are intended as supplemental to the general measures outlined in paragraph 5.F.1. above.

(1) <u>THREATCON ALPHA and BRAVO Measures</u>

(a) MEASURE AV-1. Brief all personnel on the threat and the commands unique vulnerabilities, especially pilots, ground support crews and air traffic controllers.

(b) MEASURE AV-2. Inform local police of the threat. Coordinate plans to safeguard aircraft flight paths into and out of air stations.

(c) MEASURE AV-3. Ensure duty officers are always available by telephone.

(d) MEASURE AV-4. Prepare to activate contingency plans and issue detailed air traffic control procedures if appropriate.

(e) MEASURE AV-5. Be prepared to receive and direct aircraft from other stations.

(f) MEASURE AV-6. Perform thorough and regular inspections of areas within the perimeters from which attacks on aircraft can be made.

(g) MEASURE AV-7. Take action to ensure no extremists armed with surface-to-air missiles can operate against aircraft within the perimeter.

(h) MEASURE AV-8. Establish checkpoints at all entrances and inspect all passes and permits. Identify documents of individuals entering the area. A 100% positive ID check of all individuals should be enforced.

(i) MEASURE AV-9. Search all vehicles, briefcases, packages, etc., entering the area.

(j) MEASURE AV-10. Erect barriers around potential targets if at all possible.

(k) MEASURE AV-11. Maintain firefighting equipment and conduct practice drills.

(l) MEASURE AV-12. Hold practice alerts within the perimeter.

(m) MEASURE AV-13. Conduct, with local police, regular inspections of the perimeter; especially the area adjacent to flight paths.

(n) MEASURE AV-14. Advise the local police of any areas outside the perimeter where attacks could be mounted and which cannot be avoided by aircraft on takeoff or landing.

(o) MEASURE AV-15. Advise aircrews to report any unusual activity near approach and overshoot areas.

(p) MEASURE AV-16. Review all plans, orders, personnel details and logistic requirements related to the actions in THREATCON CHARLIE for possible implementation.

(q) MEASURE-AV-17 through A-20. Spare.

(2) THREATCON CHARLIE Measures:

(a) MEASURE AV-21. Maintain appropriate THREATCON ALPHA and BRAVO measures.

(b) MEASURE AV-22. Brief all personnel on the increased threat.

(c) MEASURE AV-23. Inform local police of the increased threat.

(d) MEASURE AV-24. Coordinate with the local police on any precautionary measures taken outside the airfield's perimeters.

(e) MEASURE AV-25. Implement appropriate flying countermeasures specified in SOPs when directed by air traffic controllers.

(f) MEASURE AV-26. Inspect all vehicles and buildings on a regular basis.

(g) MEASURE AV-27. Detail additional guards to be on call at short notice and consider augmenting firefighting details.

(h) MEASURE AV-28. Carry out random patrols within the airfield perimeter and maintain continuous observation of approach and overshoot areas.

(i) MEASURE AV-29. Reduce flying to essential operational flights only. Cease circuit flying if appropriate.

(j) MEASURE AV-30. Escort all visitors.

(k) MEASURE AV-31. Close relief landing grounds where appropriate.

(l) MEASURE AV-32. Check airfield diversion state.

(m) MEASURE AV-33. Be prepared to react to requests for assistance.

(n) MEASURE AV-34. Provide troops to assist local police in searching for terrorist on approaches outside the perimeter of military airfields.

(o) MEASURE AV-35. Review all plans, orders, personnel details and logistic requirements related to the actions in THREATCON DELTA for possible implementation.

(p) MEASURE AV-36 through AV-40. Spare.

(3) THREATCON DELTA Measures:

(a) MEASURE AV-41. Maintain appropriate THREATCON ALPHA, BRAVO, and CHARLIE measures.

(b) MEASURE AV-42. Brief all personnel on the very high levels of threat.

(c) MEASURE AV-43. Inform local police of the increased threat.

(d) MEASURE AV-44. Cease all flying except for specifically authorized operational sorties.

(e) MEASURE AV-45. Implement, if necessary, appropriate flying countermeasures.

(f) MEASURE AV-46. Be prepared to accept aircraft diverted from other stations.

(g) MEASURE AV-47. Be prepared to deploy light aircraft and helicopters for surveillance tasks or to move internal security forces.

(h) MEASURE AV-48. Prepare to move aircraft to alternate airfields.

(i) MEASURE AV-49. Close military roads allowing access to the airbase.

(j) MEASURE-AV-50. Spare.

Chapter 6 FUNDS FACILITIES AND STORAGE

A. Applicability.

1. The standards and procedures in this chapter apply to the protection of all appropriated, nonappropriated and all other Government funds or negotiable instruments under Coast Guard control. Negotiable instruments include but are not limited to; cash, traveler's checks, penalty postage meters, Government checks, sub-vouchers, credit cards, and all other instruments or systems that support the disbursement of Government monies . For ease of discussion within this chapter, all such instruments shall be referred to by the term "Funds".

2. The protective measures outlined within this chapter should also be considered when assessing the security requirements for facilities that house systems and applications involved in the electronic control and distribution of funds or the processing of information which offers the opportunity to divert economically valuable resources including funds, supplies, and materials.

3. Funds storage areas should be designated as restricted areas in accordance with Chapter 2.

   NOTE: The mere existence of a container does not automatically require the location it is in to be a restricted area. For example, a room with a container that only stores funds may not need restricted area controls, whereas, a room with a container and where money transactions and handling regularly occur would require restricted area controls. Areas where transactions only occur on an occasional basis would require the extra controls only during the transactions or handling and not at other times. Cognizant Security Managers (SECMGRs) should be consulted and compensatory measures established for proper control during all planned levels of activity.

4. Although these standards are not binding on funds controlled by a private association, those businesses located on Coast Guard property should be strongly encouraged to comply with this chapter. SECMGRs are encouraged to take a proactive approach and include such businesses in their evaluations.

B. Responsibilities.

1. Command.

   a. Commands shall coordinate with the SECMGR to ensure that adequate protective procedures are developed and implemented.

b. The command is responsible for providing appropriate security containers and ensuring that the funds entrusted to their personnel are protected as prescribed herein.

c. The command shall prepare written internal control procedures as prescribed herein for the safeguarding of funds and ensuring that all unit personnel are familiar with these procedures.

d. The command shall develop emergency procedures to follow in the event of a hold-up or other critical incident. These procedures should be included as part of the unit physical security plan as discussed elsewhere in this manual.

e. The command must require positive safe closing and checking procedures when the funds are unattended during the workday and at the close of business.

f. The command shall immediately report funds that are lost , stolen or unaccounted for in accordance with the procedures established by the various funds program managers, with information copies to the cognizant SECMGRs.

2. Area and District Security Managers (SECMGR).

a. Coordinate with the command to ensure that adequate protective procedures are developed and implemented.

b. Conduct periodic inspections of the security controls to verify that the procedures are being followed and that the physical security controls are functioning properly (e.g., CCTV, panic alarms, hold-up cameras, security containers).

c. Provide instruction in changing the combination(s) to containers utilized for the storage of funds.

d. Follow up, as appropriate, on all reports regarding the loss or theft of funds.

C. Consideration Factors for Funds Site Selection. The following security factors should be taken into consideration by both the command and the servicing security element when establishing funds facilities:

1. The location and type of building in which the fund is situated (e.g., commercially owned building versus a government owned or leased facility.

2. The specific location of the fund within the facility (e.g., proximity to elevators and stairwells, and whether or not it is located in a segregated area as opposed to an open work area).

3. The relative crime rate for the area in which the funds facility is located.

4. The closeness and response time afforded by the servicing security force or local law enforcement authority.

5. The applicability of the following supplemental security measures as warranted by the relative risk factors:

   a. Panic or hold-up alarms.

   b. Closed Circuit Television monitoring.

   c. Hold-up cameras.

   d. Bullet resistant partitions.

   e. Money clip alarms.

   f. Daytime cleaning of funds areas.

   g. Hold-up money packets.

   h. Single entry points to transaction and handling areas.

D. Cost Reduction Measures. Measures should be taken to protect against thefts and unaccountable losses. For example, when possible, reduce the amount of cash on hand and rely on automated transactions and bank credit cards.

E. Funds Storage Containers. The following subparagraphs prescribe the minimum requirements for storage of funds. Previously approved storage containers now in use may continue to be used if, in the judgement of the cognizant SECMGR, they provide satisfactory protection.

1. Storage Containers Limitations. The use of approved commercial burglary resistant safes with an Underwriters' Laboratories (UL) classification or General Services Administration (GSA) approved security containers for all funds is encouraged. However, there may be circumstances when it is not possible, e.g., due to cost and/or weight constraints.

a. Under $2,000 - For ashore and mobile units, the commanding officer shall establish container requirements. Any of the security containers or burglary resistant safes listed in subparagraph 6.D.2 may be used.

b. $2,000 - $9,999 - For ashore units, a GSA approved security container that carries a Class 1 or Class 5 rating or a burglary resistant safe carrying at least an UL classification of Tool-Resistant Safe, TL-15, and having a Group 1R combination lock shall be used. For mobile units, existing "built in" containers may be used.

c. $10,000 - $49,999 - For all units, both ashore and mobile, a GSA approved security container that carries a Class 1 or Class 5 rating or a burglary resistant safe carrying at least an UL classification of Tool-Resistant Safe, TL-15, and having a Group 1R combination lock shall be used.

d. $50,000 or more - For both ashore and mobile units, a burglary resistant safe or vault carrying at least an UL classification of Tool-Resistant Safe, TL-30, and having a Group 1R combination lock shall be used.

2. Storage Container Categories.

a. Burglary Resistant Safes. Commercial burglary resistant safes are listed by Underwriters' Laboratories (UL), according to the following classifications. These containers are manufactured to UL Standard 687 and are designed to protect the contents against forced entry. The numerical value utilized in the classifications represents the time in minutes which the safe should resist forced entry. These safes provide a greater degree of protection than the GSA rated security containers.

(1) Tool-Resistant Safe - TL-15.

(2) Tool-Resistant Safe - TL-30.

(3) Torch and Tool-Resistant Safe - TRTL-30 and TRTL-30X6.

(4) Torch and Tool-Resistant Safe - TRTL-60.

b. Security Containers. GSA approved security containers are manufactured under the following Federal specifications. The Class 1 and Class 5 cabinets have been rated the greatest protection against forced entry. The other classes of security containers do not meet forced entry protection requirements.

(1) The following security containers are primarily used for the protection of classified national security information.

(a) Class 1 or Class 2 security filing cabinet; AA-F-357 (GSA-FSS).

(b) Class 3, 4, 5, and 6 security filing cabinets; AA-F-358 (GSA-FSS).

(c) Class 5 or Class 6 Map and Plan File; AA-F-363 (GSA-FSS)

(d) Class 6 Drawer File; AA-F-358 (GSA-FSS).

(e) Class 7 security filing cabinet; AA-F-2815

(2) The following security containers are primarily used for the protection of funds, narcotics and other sensitive items.

(a) Class 5 Money Safes; AA-S-1518A

(b) Class 5, Size IV general purpose security cabinet; AA-F-363 (GSA-FSS)

3. Storage Container Requirements.

a. Funds shall not be stored in any container used to store classified material, controlled medical substances, Arms, Ammunition and Explosives (AA&E), or other items of intrinsic value. Containers shall be located in a locked room where reasonable security measures can be effectively implemented.

b. Any funds container on casters, weighs less than 500 pounds or is not protected by an Intrusion Detection System (IDS), (or not located inside a vault), shall be secured to the premises. These containers may be secured by fastening with bolts and/or heavy metal straps, welded, or if it is intended to remain part of the structure, it may be secured by imbedding it in concrete.

c. If the vault, safe, or container is visible to the exterior of the facility where host installation police or security patrols pass, the container shall be illuminated.

4. Storage Container Records. The following records shall be maintained for each funds storage container:

a. Standard Form (SF) 700, Security Container Information, is self-explanatory and is used each time the safe combination is changed. Part 1 of the form will be attached to the inside of the safe on the back of the door or if applicable on the inside of the locking drawer of the funds container. Ensure the date of the combination change is properly annotated in the appropriate block. Disposition of the current SF 700 parts 2 and 2A should be as outlined in paragraph 6.G.

b. Standard Form (SF) 701, Activity Security Checklist, shall be used to record area security checks at the close of each duty or business day. Retain SF 701 at least three months following the last entry.

c. Standard Form (SF) 702, Security Container Check Sheet, shall be affixed to the exterior of each funds container. Record each opening and closing of the funds container. Only one end-of-day final check of a funds container is required. Retain SF 702 at least three months following the last entry.

NOTE: If a loss of funds has occurred within the last 12 months requiring any action, retain these forms until such action has reached its final conclusion.

F. Money Packets (for ashore units). If $2,000 or more in cash is kept in a funds container during non-operating hours, in a cashier cage, or in an isolated cash register during operating hours, one packet of money (including foreign currency where applicable) shall be kept as follows:

1. The packet shall consist of at least three $20 bills (or equivalent foreign currency).

2. The denomination, class of currency (Federal Reserve Note, United States Note), and Series year (including letter suffix) of these bills shall be recorded. This record shall be stored in a container separate from the one storing the funds.

3. This packet need not be maintained at each cash register of a facility (such as an exchange or commissary); however, the commanding officer should decide how many packets will be maintained at these operating locations.

4. The intention of this requirement is to aid in the investigation and prosecution after a theft has occurred.

5. Units storing only traveler's checks need only maintain a log of issued and non-issued checks in a separate container or file cabinet.

G. Keys and Combinations. Chapter 2 outlines basic requirements for keys and the recording and changing of combinations. Provisions of this section supplement those requirements.

1. The keys or combinations shall be kept only by the custodian, except that the custodian shall place one key or the combination to the safe in a sealed envelope (SF 700) suitably marked so that an unauthorized opening may be detected. This envelope shall be stored in a GSA approved container separate from the one storing the funds, and used only in the event of an emergency. When needed, it shall be examined and opened by two authorized persons who shall then witness the opening of the container and prepare an affidavit as to its contents at the time of the opening. The combinations shall be changed or locks re-keyed when the emergency situation is over.

2. Combinations shall be memorized by authorized individuals. Combination records shall not be carried in wallets or concealed on persons or in the workplace.

3. Combinations to all storage containers shall be changed:

   a. When the container is first put into local service.

   b. At least annually.

   c. When someone having the combination no longer requires access.

   d. When emergency access to funds is required and the container is accessed in the absence of the authorized funds custodian(s).

   e. When the combination has been compromised or the container has been discovered unlocked and unattended.

   f. As soon as possible following the discovery of a loss of funds.

4. Key operated locks to all storage containers shall be rekeyed:

   a. When the container is first put into local service.

   b. When someone having the key no longer requires access.

   c. When the key or lock has been compromised, lost, misplaced, stolen or the container has been discovered unlocked and unattended.

   d. As soon as possible following the discovery of a loss of funds.

H. Protective Lighting. Chapter 2 outlines basic lighting requirements. Provisions of this section supplement those requirements. Vulnerable exterior areas such as windows,

doors, crawl spaces, etc., not visible to normal vehicular or foot traffic, shall be illuminated at night. Interior containers (if visible to the exterior where security patrols pass) shall also be illuminated.

I. Intrusion Detection Systems (IDS). Chapter 2 outlines basic requirements for IDS requirements. Provisions of this section supplement those requirements.

1. Requirements. When security is considered to be inadequate and cannot be upgraded efficiently through other means, an IDS should be installed. An effective IDS is a prime deterrent in preventing the loss of funds by theft. To gain the full benefit from the psychological deterrence of an IDS, each alarmed area shall be identified by conspicuously posting warning signs, labels, or decals that can normally be obtained from the alarm manufacturer or installer.

2. Selection. Each funds facility must be critically evaluated for protective needs to ensure that the best and most economical system suited to local conditions is obtained.

a. The least acceptable alarm protection is a system confined only to the container used to store the funds. When programming or budgeting for a new system, priority should be given to the areas where comparatively large and vulnerable amounts of funds are likely to be stored during non-operating hours.

b. When more than one IDS is planned, systems should be compatible so that a central alarm annunciator panel can be used.

3. Essential Characteristics. IDSs under consideration should:

a. Be capable of promptly detecting any attack on the outer doors, windows, walls, floors, or ceiling of each funds/negotiable instrument storage room. Any attack on the container should also cause an alarm. Be flexible and allow large or small areas to be protected with small cost differentials.

J. Escort Procedures.

1. The commanding officer shall determine when the use of escorts is required, ensure that movements of funds are scheduled and consolidated to the maximum extent possible, and establish procedures in which escorts will operate both on and off the unit. Personnel assigned as escorts shall not carry the funds. The escort's function is to act as security and not as the courier. Contract armored car service may be utilized in lieu of required escorts when deemed cost beneficial by the commanding officer.

2. Escorts may be armed or unarmed depending upon local conditions. The commanding officer's decision allowing armed escorts must be based on providing adequate protection against the local criminal threat. Constant radio contact is recommended.

3. Established procedures should cover the positioning of the escort with relation to the funds carrier in vehicles or on foot, and the action to be taken in the event of a robbery attempt. Routes between points and times of departure shall be varied. Movements of funds off the unit should be closely coordinated with the local police if deemed appropriate. Escorts assigned should call the security force immediately prior to departure and give the time and place of departure, route of travel, destination, and estimated time of arrival. The security force should be notified upon termination of the escort. Escorts shall obey traffic regulations and all instructions of any local police escorts as long as they do not violate Federal law or lessen the protection of the funds. Escorts shall not use sirens or blue lights except in emergencies. Specific procedures shall be detailed in the unit's anti-robbery plan.

K. Penalty Postage Meters. Specific guidance on the operation and accountability of the postage metering system can be found in Coast Guard Postal Manual, chapter 9 COMDTINST M5110.1 (series). The information provided here shall be considered as the minimum security measures necessary to ensure the accountability and control of the penalty postage metering system. The basic general use postage metering system consists of at least three functional parts that may or may not be housed separately. The postage meter (or meter head) is what controls the negotiable instruments and generally has a lock with a removable key. Specific security procedures for the protection of these meters and keys shall be developed and included in the unit's anti-robbery plan.

1. Accounting Responsibilities.

a. Individuals operating metering equipment will provide proper care and security for the equipment. To do this, a meter operator shall:

(1) Allow no one, except United States Postal Service (USPS) officials, to break the seal placed on a postage meter. Breaking or tampering with this seal is a postal offense punishable under the Uniform Code of Military Justice.

(2) Ensure that unauthorized persons do not use the metering equipment, and that the equipment only processes official mail.

(3) Ensure that the meter is locked when not in use. At the end of each duty day, or when temporarily absent from the mail center, remove the locked meter head and place it in an approved safe or secure storage area.

2. Custody of Meter Keys. Chapter 2 outlines basic requirements for keys and the recording and changing of combinations. Provisions of this section supplement those requirements.

   a. Activities shall maintain accurate custody records and control of all meter keys. This includes all operating, duplicates and meter maintenance keys as applicable.

   b. During working hours, the meter should be locked when not in use but the key does not have to be removed if kept under constant positive control (live supervision) by an authorized user. This means, if you have to leave the area where the meter is and another designated user is not maintaining control, the key shall be removed and the door locked.

   c. At the end of each duty day, the meter key shall be secured in an approved safe or secure storage area.

   d. The disposition of all meter keys shall be verified semiannually.

3. Meter Security.

   a. Meters. Remove the meter and place it in a locked safe or secure storage area overnight and at any other time the operator is temporarily absent and adequate surveillance cannot be maintained to prevent use of the meter.

      (1) If it is impractical to remove the meter due to the mechanical construction of the system, then lock the meter, remove the power cord, and secure the key and power cord in a locked safe or secure storage area.

      (2) Immediately report the loss, theft, and recovery of a lost or stolen meter to the local post office, the equipment vendor, through command channels to the Coast Guard Postal Program Manager, and to your cognizant Security Manager. Reports shall include the meter make, model, and serial number; the date, location, and details of the loss, theft, or recovery; and a copy of the police report when applicable.

L. Government Credit Cards. Specific guidance on the use and accountability procedures for government credit cards can be found in Coast Guard Simplified Acquisition Procedures Handbook, chapter 5 COMDTINST M4200.13 (series). The information provided here shall be considered as the minimum security measures necessary to ensure the physical accountability and control of these negotiable instruments. The fact that these cards can be used instead of purchase/delivery orders, Standard Form 44, Blanket Purchase

Agreements, or unit imprest funds, coupled with the growing abuse and theft of credit cards nation wide, along with their negotiable value of up to $25,000.00 make them highly vulnerable to misuse if lost or stolen. Specific security procedures for the protection of these negotiable instruments shall be developed and included in the unit's anti-robbery plan.

1. Although these cards may be issued to specific individuals and imprinted with their name, they are government property and should be controlled and accounted for accordingly.

2. When not being used, the cards shall be adequately safeguarded in a locked safe or secure storage area.

3. Immediately report the loss, theft, or recovery of a lost or stolen government credit card through local command procedures and channels to your cognizant Security Manager and to the appropriate authorities as outlined in Coast Guard Simplified Acquisitions Handbook, COMDTINST M4200.13 (series). Reports shall include the card serial number; cardholder's complete name; the date, time, location, and details of the loss, theft, or recovery; a copy of the police report when applicable; date that the issuing authority/activity was notified; and any additional requirements outlined in Coast Guard Simplified Acquisitions Handbook, COMDTINST M4200.13 (series).

M. Travelers Checks. As outlined elsewhere in this chapter, the safeguarding requirements for travelers checks is the same as that required for cash. Specific guidance on the establishment of a travelers check site can be found in, Coast Guard Certifying and Disbursing Manual, COMDTINST M7210.1 (series).

N. Robbery Prevention and Planning.

1. The unit physical security plan shall include procedures for actions to be taken in the event of a robbery. Plans shall be marked and safeguarded as FOR OFFICIAL USE ONLY (FOUO) and include the following:

   a. Actions to be taken by funds handling employees.

   b. Actions to be taken by the security force/escorts.

   c. Actions to be taken by the supporting law enforcement agency or agencies.

   d. Agencies, officials to be notified, and the individual, by position, responsible for the notification.

2. Anti-robbery plans shall be coordinated with all local law enforcement agencies. In the case of a Coast Guard funds facility located in non-Coast Guard buildings or

on non-Coast Guard property, the plan shall be fully coordinated with the host activity. Liaison with outside agencies shall be conducted in conjunction with the host installation.

3. Anti-robbery plans for facilities maintaining $2,000 or more during operating hours shall be tested by the Command Security Officer (CSO) at least annually.

4. Anti-robbery prevention training shall be presented to all new employees during orientation and annually to all funds handling personnel by the CSO or funds custodian. Local or State police with a crime prevention unit may offer a good source for this training.

5. The following prevention measures should be considered in anti-robbery planning:

   a. Two persons should open and close the funds facility where staffing permits.

   b. Frequently test all alarm devices to ensure their proper operating conditions.

   c. Where an IDS is installed and the funds container is zoned separately, it should remain alarmed until it becomes necessary to open it for official business.

   d. Instruct employees to carefully observe persons loitering in or near the facility.

   e. Encourage employees to challenge unidentified personnel.

   f. Keep the amount of cash in cashier cages at a minimum level.

   g. Require employees to secure all funds from their immediate work area prior to their departure.

   h. Avoid establishing unnecessary operating routines.

   i. Upon the closing of business, ensure all safes, vaults, doors and other points of access to the facility are locked.

   j. Establish security procedures to institute for spaces during funds/negotiable instrument transactions.

Chapter 7 PRIVATE MOTOR VEHICLE ACCESS CONTROL PROGRAM

A. Purpose. This chapter establishes policy and procedures for the registration and marking of Privately Owned Motor Vehicles (POVs) in order to control their access to and operation on Coast Guard property and Department of Defense (DoD) facilities.

B. General. The Certificate of Compliance - Private Motor Vehicle Registration (CG-3308A) and the Coast Guard Private Motor Vehicle Access Decal (CG-4801) (see Exhibits 7-1 and 7-2) are intended to facilitate in the control of access to Coast Guard units and DoD facilities. This is in lieu of showing state registration, operator's license and proof of financial responsibility, and if applicable, proof of completion of a motorcycle safety course, each time a facility is accessed. Under normal, low threat, conditions security personnel shall accept a current copy of the CG-3308A and valid identification card as proof of registrant and/or vehicle meeting the requirements of this chapter.

C. Policy. Program implementation is at the discretion of the commanding officer. Units participating in this program shall ensure that all POVs entering a unit comply with this chapter. The operation of a POV and other motor powered two or three wheeled vehicles constitutes a conditional privilege which must meet the sustaining conditions covered by the certification on CG-3308A.

1. POV access to and operation on government facilities is a privilege and not the inherent right of any individual.

2. Only units that have been evaluated and properly designated in writing by a SECMGR shall issue the decals and tabs.

3. The CG-4801, Coast Guard Private Motor Vehicle Access Decal, shall be used to identify vehicles eligible for access to a participating command.

4. A unit, which does not require access decals for access to their unit, shall not issue access decals for the sole purpose of allowing access to facilities not under the jurisdiction and responsibility of their unit. The member should apply for a decal from the Coast Guard unit or DoD facility that is frequently visited.

5. In order for a unit to qualify and be designated as a decal issuing authority, the unit itself must require display of the decal to enter their facility, or a facility under their cognizance. Application for designation shall be made to the cognizant Security Manager.

6. The CG-4801, Coast Guard Private Motor Vehicle Access Decal, is not a pass. The decal, which is the property of the U.S. Government, shall be permanently affixed to the vehicle for which issued at all times; however, if required by military authority, it shall be surrendered.

7. Mail order registration of the CG-4801, Coast Guard Private Motor Vehicle Access Decal is specifically not authorized. Issuance of the decal via mail has been proven to violate the programs integrity and inter-service acceptance.

8. Unauthorized or fraudulent use of the CG-4801 would exist if a bearer uses the decal, or vehicle to which attached, in a manner that would enable the bearer to obtain otherwise unlawful access to facilities to which they are not entitled.

9. Alteration of these decals or date tabs, possession of more than one decal or date tab for the same vehicle, possession of unauthorized decals or date tabs, possession of fraudulently obtained decals or date tabs, possession of decals or date tabs when not currently a member authorized under the provisions of this instruction, is contrary to these instructions and may subject the offender to disciplinary action or criminal prosecution under 18 U.S.C. 499, 506, 701, or 1002.

10. Unless security requirements dictate otherwise, valid POV registration and decals from other installations and activities of the Armed Forces shall be honored at all Coast Guard facilities that utilize POV decals for access control.

11. Unit commanding officers are the final authority for determining whether or not an individual has a frequent, demonstrated need to have on-base driving privileges.

D. Privately Owned Vehicle Access Registration (POV).

1. Objectives. The objectives of POV access registration are as follows:

a. To provide safeguards against financially irresponsible or careless drivers when coupled with local and state requirements for the operation of motor vehicles, i.e., vehicle safety inspections, insurance, or other forms of financial responsibility and licensing of motor vehicle operators;

b. To place a maximum lifetime of 4 years on the validity of the registration and decal;

c. To provide an accountability and record keeping system for administrative purposes;

d. To define conditions under which vehicle access may be granted and revoked;

e. To impose requirements on POV owners for registration consistent with current DoD regulations to ensure continued access to DoD facilities;

f. To improve security at Coast Guard and DoD facilities by providing a means for security forces to readily identify that a POV is associated with Coast Guard personnel.

2. Privileges. If registration requirements are met, registration privileges shall be granted to:

a. Personnel Eligibility.

(1) Active duty and Reserve Coast Guard personnel;

(2) Active duty and Reserve members of other armed forces if they have frequent, demonstrated need to visit a Coast Guard unit;

(3) Dependents of active duty and reserve members, retired military members and dependents, and widows and widowers of deceased members as long as they continue to retain authorized military privileges and have a frequent, demonstrated need to visit a Coast Guard unit;

(4) Commissioned officers of the National Oceanic and Atmospheric Administration (NOAA) and the U.S. Public Health Service (USPHS), both active and retired members and their dependents, as long as they retain authorized military privileges, as authorized by Title 37 U.S.C., and have a frequent, demonstrated need to visit a Coast Guard unit.

(5) Civilian personnel employed by the Coast Guard or Department of Transportation (DOT), including long term “permanently attached” civilian contractors, as long as there is a demonstrated need for daily access to a Coast Guard unit;

(6) Coast Guard Auxiliarists as long as there is a frequent, demonstrated need for access to a Coast Guard unit that requires the CG-4801 for vehicular access. This is to provide access for duty in support of Coast Guard operational missions. Regular use of an exchange or morale activity is not a “demonstrated need” for a decal. Once the operational need is over, the decal shall be removed from the vehicle, (A locally generated pass may be easier for command administration).

(7) Civilian personnel who have been officially retired from the Coast Guard Exchange System (CGES) and are issued an official retirement ID. The member must have been officially granted exchange privileges such as gas station, convenience stores,

employee credit unions, and MWR facility usage. This is to provide access to privileges aboard Coast Guard facilities only, and will be implemented at the discretion of the unit commanding officer.

b. Vehicle Eligibility.

(1) Privately owned, motorized, wheeled vehicles that may legally operate on public roads or highways, providing that all other eligibility requirements are met.

(2) Commercial use vehicles owned by eligible personnel are not eligible for a CG-4801, Coast Guard Private Motor Vehicle Access Decal, if the vehicle is registered in the name of a company, corporation or partnership, and not in the name of the otherwise eligible owner.

(3) Vehicles designed exclusively for construction and material handling, vehicles used solely off the road, and bicycles with fractional horsepower engines shall not be registered.

3. Deviations.

a. In the following instances, registration requirements of this chapter may be waived, subject to the discretion of the commanding officer:

(1) When POVs are currently registered with another armed force and display a current DoD decal;

(2) When a Coast Guard unit is located totally within a DoD facility, and Coast Guard personnel obtain POV access under that facility's policies and procedures;

(3) When vehicles are owned by federal, state or local governments;

(4) When necessary in overseas locations, as required by local conditions, treaties, agreements and other arrangements with a foreign government;

(5) When a POV is operated by a visitor who is issued a temporary pass that is valid for no more than 31 days.

b. Personnel and dependents driving POVs that do not properly display a decal shall be subject to normal visitor check-in procedures at Coast Guard units or DoD facilities.

c. A unit which does not require access decals for access to their unit shall not issue access decals for the sole purpose of allowing access to facilities not under the jurisdiction and responsibility of their unit. The member should apply for a decal from the Coast Guard unit or DoD facility which is frequently visited.

4. Requirements. Individuals who request POV access registration, including recertification and temporary visitors passes, must demonstrate a need for vehicular access to the facility and shall provide the following documents:

a. Valid government identification card, (This identification card must be completely and properly filled out, both front and back, signed by the issuing authority and member, include a photo ID in the space provided, and be properly sealed or laminated);

b. Valid state motor vehicle drivers license for the type of vehicle being registered;

c. Valid state certificate of vehicle registration in the name of the individual entitled to access decal privileges;

d. The POV must have a valid metal license plate. POVs having temporary license plates (e.g., cardboard, plastic, paper, etc.) are not eligible to receive Coast Guard POV access decals until a permanent plate has been assigned by the state of registration for the vehicle, and has been permanently attached to the registered vehicle.

e. Proof of compliance with minimum requirements of the financial responsibility, compulsory insurance or no fault insurance laws of the state in which the vehicle is registered, or of the state in which the unit is located if no financial responsibility is required by the state of registry;

f. Proof of satisfactory completion of a safety and mechanical vehicle inspection by state or jurisdiction in which the vehicle is registered. This requirement is waived for units in areas not requiring a vehicle safety inspection or where out-of-state vehicles are not required to be inspected; however, states can require that all vehicles, regardless of state of registry, be inspected and meet safety and pollution control standards. Furthermore, commanding officers may establish minimum vehicle safety standards as a condition of registration. The intent is to ensure that we comply with all state and local requirements.

g. The decal issuing official or cognizant SECMGR, in the jurisdiction in which the POV is being operated, shall also be notified if there is any change, lapse or cancellation of any vehicle insurance.

5. Procedures for Completing CG-3308A.

   a. Registrants shall complete items 1 through 10 of the CG-3308A.

   b. The approving authority, normally the commanding officer or a designated representative, shall complete item 11.

   c. The issuing authority, which may also be the approving authority, shall complete items 12 through 15.

   d. The expiration date shall either be as close to the anticipated date of expiration of the service contract, or a maximum of 4 years (3 years for two or three wheeled vehicles) from date of issuance, whichever is earlier. Recertification may be accomplished in item 14.

   e. The issuing authority shall provide the decal and expiration tabs to the registrant. A copy of Exhibit 7-2 should be given to the registrant to ensure decals/tabs are properly affixed to the vehicle.

6. Distribution of CG-3308A.

   a. The CG-3308A shall be maintained (by serial number) by the issuing authority for a period of 4 years from the date of initial issue, or 1 year after expiration or recertification, whichever is latest.

   b. A copy (with latest recertification) shall be given to the member and available for inspection by security personnel upon request.

7. Transfer Out of Issuing Authority's Area of Responsibility (AOR). The owner of a registered vehicle need not be issued a new decal when transferring until the expiration of the current decal.

8. Temporary Access and Visitor Passes. Commands are authorized to grant temporary registration pending permanent registration or in other circumstances when deemed appropriate. Applicants for a visitor’s pass or temporary access form shall comply with the requirements of paragraph 7.D.4. In addition, the following provisions apply:

   a. Visitor passes and temporary access forms shall not be valid for more than 31 days.

   b. Locally generated and reproduced passes and forms may be used but will not be identical to the official forms covered under this instruction. The passes and forms shall contain a highly visible expiration date marking.

c. Visitor passes and temporary access forms shall be displayed in a manner that allows ready visibility by security personnel.

d. Visitor passes and temporary access forms shall be good for access only to the issuing activity.

9. Decal Display.

a. The CG-4801 and expiration tabs must be readily visible to gate guards and security forces when the vehicle is approaching facility entrances.

b. The decal may be installed on the front bumper of the vehicle on the driver's side (optimum choice). Unless prohibited by state or local regulations, the decal may be placed at the top of the center of the windshield, behind the rear-view mirror, or on the lower left hand, (driver's side), corner of the windshield. Motorcyclists may mount the decal lengthwise on the vehicle where it may easily be seen.

c. The expiration tab shall be affixed parallel with and adjacent to the RIGHT edge of the decal. The tabs are available for JAN and JUL only.

d. The optional retired or reservist tabs are obsolete, but may continue to be used while supplies last. They shall be affixed parallel with and adjacent to the RIGHT edge of the expiration tab.

e. The optional rank tabs shall be affixed parallel with and adjacent to the LEFT edge of the decal.

f. Exhibit 7-2 denotes the correct placement of the decal and tabs.

NOTE. Because of security concerns, the mounting of the CG-4801 and associated tabs on devices (e.g., metal or plastic plates, etc.) that are not a permanent part of the POV body or structure is prohibited. Decals not permanently affixed to the vehicle for which issued are subject to confiscation and/or termination, and the member may be subject to disciplinary action or criminal prosecution.

10. Termination of Access.

a. Commanding officers may revoke access privileges under any of the following conditions:

(1) If the owner fails to comply with or maintain state or Coast Guard registration requirements.

(2) If the registrant's service with the Coast Guard is terminated (except for military members retiring).

(3) If the owner uses or permits the use of the POV in connection with illegal activities.

(4) If the owner's driving privileges are revoked on any Coast Guard unit or DoD facility or their eligibility or registration is terminated.

(5) If the owner has sold or otherwise disposed of a registered vehicle without providing adequate proof of the decal being removed. Normally adequate proof shall consist of the remains of the decal, or having the commanding officer or a designated representative witness the destruction of the decal. It is not the intent of this provision to limit the number of vehicles that may be registered to a person, but simply to ensure that decals are accounted for.

(6) If the current decal becomes effaced, illegible or incomplete (just cause for re-issuing the decal).

(7) If the owner is no longer entitled access to Coast Guard units

b. Decals may be seized for just cause by any commanding officer or a designated representative or by any security organization of the Armed Forces. When a decal is seized for any reason, a report shall be forwarded to the original issuing authority or the cognizant Security Manager by returning the members copy of the CG-3308A with annotation “Decal Destroyed” along with the reason for removal. An issuing authority is a unit authorized by the cognizant district security manager (SECMGR) to issue vehicle access decals.

E. Motorcycle Access Registration Requirements.

1. Valid state license with motorcycle endorsement is required.

2. Compliance with the helmet and safety laws for the location in which the motorcycle is being operated is mandatory for access to a Coast Guard unit.

F. Security and Accountability.

1. Accountability. A record of issued decals shall be maintained (by serial number) by the issuing authority for a period of 4 years from the date of initial issue, or 1 year after expiration or recertification, whichever is latest. Unissued decals shall be inventoried (by an individual with no direct interest) annually and the results maintained for 1 year. A copy of the inventory shall be forwarded to the cognizant district SECMGR.

2. Storage. Decals and expiration tabs shall be stored in a locked container of at least 12-gauge steel. Access and key controls shall be established in accordance with Chapter 2.

3. Responsibilities. Units designated as issuing authorities are responsible for the stocking of unissued decals. They shall maintain a record of decals issued to each facility under their cognizance by serial number. Designated issuing authority units are authorized direct procurement of the decals and shall be responsible for maintaining an accurate audit trail from receipt of the decal, to issue, and to expiration or destruction of the decal. Headquarters units, area units and MLCs shall request decals imprinted with the number of the district in which they are geographically located. Bulk shipments of decals (100 or more) shall be sent via registered mail.

G. Availability of Forms.

1. Units properly designated as an issuing authority by their cognizant Security Manager are the sole authority for ordering decals from the Coast Guard Supply Center. Unit issuing authorities should order the appropriately marked decals, expiration tabs and optional tabs directly from the Coast Guard Supply Center (see Exhibit 7-3).

2. Issuing authorities shall develop annual demand figures and submit reports to their cognizant Security Manager to assist in program management and procurement cycle planning.

H. Decal and Tab Description. Decals shall be procured by the Coast Guard Supply Center and shall meet the minimum Federal Specification L-S 300B, type 2, class 4, reflectivity 2, minimum 5 year life.

1. Basic decal:

a. Size: 2 1/2 X 5 inches.

b. Background - White.

c. Decal shall consist of the following:

(1) Coast Guard Blue and Red Stripe with the Coast Guard Seal

(2) The words "COAST GUARD" in Coast Guard Red

(3) The words "REGISTERED VEHICLE" in black.

(4) A serial number in black with the first two numbers or letters "HQ" representing the district or Headquarters, followed by a hyphen; the remaining numbers are sequential.

2. Expiration tab:

a. Size: 7/8W X 2 1/2H inches.

b. Background: The expiration tab shall be color-coded to indicate registrant's status according to the following:

(1) Officers (Active/Reserve/Retired) - Blue.

(2) Enlisted (Active/Reserve/Retired) - Red.

(3) Civilians (Employees/Auxiliarists) - Green.

c. The numbers representing the expiration date shall be white, with either a 01 or 07 over a hyphen, over the last two numbers of the year of expiration.

EXHIBIT 7-1

FORM CG-3308A

DEPARTMENT OF TRANSPORTATION U.S. COAST GUARD CG-3308A (Rev. 10-84)	**CERTIFICATE OF COMPLIANCE - PRIVATE MOTOR VEHICLE REGISTRATION** *(THIS FORM IS AFFECTED BY THE PRIVACY ACT OF 1974)*

PRIVACY ACT STATEMENT

AUTHORITY: 44 USC 3101 and E.O. 12174

PRINCIPAL PURPOSE: To establish an official record for the issuance of U.S. Coast Guard Privately Owned Vehicle Registration Decals.

ROUTINE USES: To provide for the verification of compliance with appropriate state POV registration and financial responsibility laws. It includes control of POV's operating and accessing military installations. Determines issuance, revocation or renewals of U.S.C.G. Decals. Disclosure to law enforcement authorities is authorized.

DISCLOSURE: Disclosure of this information is voluntary, but failure to provide the information will result in non-issuance of U.S.C.G. POV Decals.

GENERAL INFORMATION

1. NAME *(Last, first, middle) (TYPE or PRINT)*	2. GRADE	3. SOCIAL SECURITY NUMBER
4. UNIT/STATION		5. WORK TELEPHONE NO.

6. APPLICANT STATUS *(Check one box only)*

☐ ACTIVE ☐ RESERVE ☐ RETIRED

☐ CIVILIAN EMPLOYEE ☐ COAST GUARD AUXILIARY ☐ OTHER *(Specify)* _____

7. VEHICLE INFORMATION

a. VEHICLE I (1) STATE OF REGISTRATION	(2) VEHICLE IDENTIFICATION NUMBER	(3) LICENSE PLATE NUMBER
(4) DATE ISSUED	(5) DATE OF EXPIRATION	(6) DECAL NUMBER
b. VEHICLE II (1) STATE OF REGISTRATION	(2) VEHICLE IDENTIFICATION NUMBER	(3) LICENSE PLATE NUMBER
(4) DATE ISSUED	(5) DATE OF EXPIRATION	(6) DECAL NUMBER
c. VEHICLE III (1) STATE OF REGISTRATION	(2) VEHICLE IDENTIFICATION NUMBER	(3) LICENSE PLATE NUMBER
(4) DATE ISSUED	(5) DATE OF EXPIRATION	(6) DECAL NUMBER

8. CERTIFICATION

I CERTIFY that I am cognizant of the pertinent insurance laws and regulations of the state in which my vehicle is registered and applicable Coast Guard regulations on the registration/operation of private motor vehicles. I now possess motor vehicle liability insurance coverage in amounts not less than the minimum prescribed by the state in which my vehicle is registered, for the motor vehicle registered in my name by the U.S. Coast Guard. I further certify I am in compliance with applicable state requirements on vehicle ownership/registration and inspection and possess a valid operator's license. I fully understand my personal responsibility as a vehicle registrant/driver. I agree to remove all Coast Guard vehicle registration media from my vehicle upon its disposal in the event my registration privilege is terminated for any reason. I further certify that I will notify my commanding officer/officer-in-charge when any change occurs in the data listed herein.

9. SIGNATURE OF APPLICANT	10. DATE	11. SIGNATURE/TITLE OF APPROVING AUTHORITY

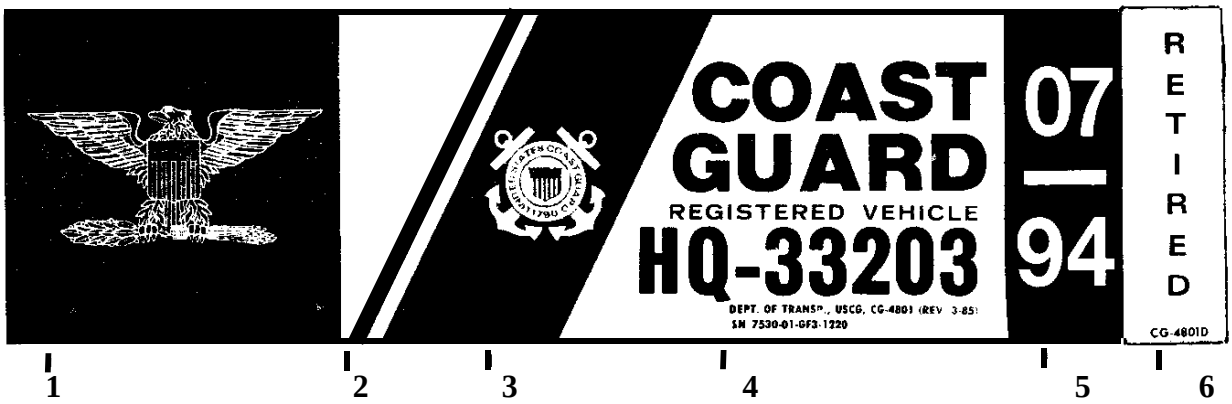
12. SIGNATURE OF ISSUING OFFICIAL

13. REMARKS 14. RE-CERTIFICATION ON _____ 15. DATE COPY FORWARDED TO DISTRICT SECURITY MANAGER _____

PREVIOUS EDITION IS OBSOLETE

EXHIBIT 7-2

COAST GUARD REGISTRATION DECAL AND TABS



1 – OPTIONAL RANK TAB

2 – REGISTRATION DECAL, COAST GUARD BLUE STRIPE

3 – REGISTRATION DECAL, COAST GUARD RED STRIPE

4 – REGISTRATION DECAL, WHITE BACKGROUND

5 – DATE EXPIRATION TAB (COLOR ACCORDING TO STATUS)

6 – OPTIONAL STATUS TAB (OBSOLETE)

EXHIBIT 7-3

LIST OF STOCK NUMBERS (SN)

A. Form: CG-3308A CERTIFICATE OF COMPLIANCE - 7530-00-F02-1600

B. Basic Decal:

1. DECAL VEHICLE REG 01 - 7690-01-GF3-1100
2. DECAL VEHICLE REG 05 - 7690-01-GF3-1130
3. DECAL VEHICLE REG 07 - 7690-01-GF3-1140
4. DECAL VEHICLE REG 08 - 7690-01-GF3-1150
5. DECAL VEHICLE REG 09 - 7690-01-GF3-1160
6. DECAL VEHICLE REG 11 - 7690-01-GF3-1170
7. DECAL VEHICLE REG 13 - 7690-01-GF3-1190
8. DECAL VEHICLE REG 14 - 7690-01-GF3-1200
9. DECAL VEHICLE REG 17 - 7690-01-GF3-1210
10. DECAL VEHICLE REG HQ - 7690-01-GF3-1220

C. Expiration Tab:

1. Officer (Active/Reserve/Retired):

   a. DECAL EXP BLUE 01-99 - 7690-01-GG0-1239
   b. DECAL EXP BLUE 07-99 - 7690-01-GG0-1240
   c. DECAL EXP BLUE 01-00 - 7690-01-GG0-1243
   d. DECAL EXP BLUE 07-00 - 7690-01-GG0-1244
   e. DECAL EXP BLUE 01-01 - 7690-01-GG0-1430
   f. DECAL EXP BLUE 07-01 - 7690-01-GG0-1431
   g. DECAL EXP BLUE 01-02 - 7690-01-GG0-1432
   h. DECAL EXP BLUE 07-02 - 7690-01-GG0-1433
   i. DECAL EXP BLUE 01-03 - 7690-01-GG0-1434
   j. DECAL EXP BLUE 07-03 - 7690-01-GG0-1435
   k. DECAL EXP BLUE 01-04 - 7690-01-GG0-1436
   l. DECAL EXP BLUE 07-04 - 7690-01-GG0-1437

2. Enlisted (Active/Reserve/Retired):

   a. DECAL EXP RED 01-99 - 7690-01-GG0-1241
   b. DECAL EXP RED 07-99 - 7690-01-GG0-1242
   c. DECAL EXP RED 01-00 - 7690-01-GG0-1245
   d. DECAL EXP RED 07-00 - 7690-01-GG0-1246
   e. DECAL EXP RED 01-01 - 7690-01-GG0-1422
   f. DECAL EXP RED 07-01 - 7690-01-GG0-1423
   g. DECAL EXP RED 01-02 - 7690-01-GG0-1424

h. DECAL EXP RED 07-02 - 7690-01-GG0-1425
i. DECAL EXP RED 01-03 - 7690-01-GG0-1426
j. DECAL EXP RED 07-03 - 7690-01-GG0-1427
k. DECAL EXP RED 01-04 - 7690-01-GG0-1428
l. DECAL EXP RED 07-04 - 7690-01-GG0-1429

3. Civilian (Employee/Auxiliarists):

a. DECAL EXP GREEN 01-99 - 7690-01-GG0-1249
b. DECAL EXP GREEN 07-99 - 7690-01-GG0-1250
c. DECAL EXP GREEN 01-00 - 7690-01-GG0-1251
d. DECAL EXP GREEN 07-00 - 7690-01-GG0-1252
e. DECAL EXP GREEN 01-01 - 7690-01-GG0-1438
f. DECAL EXP GREEN 07-01 - 7690-01-GG0-1439
g. DECAL EXP GREEN 01-02 - 7690-01-GG0-1440
h. DECAL EXP GREEN 07-02 - 7690-01-GG0-1441
i. DECAL EXP GREEN 01-03 - 7690-01-GG0-1442
j. DECAL EXP GREEN 07-03 - 7690-01-GG0-1443
k. DECAL EXP GREEN 01-04 - 7690-01-GG0-1444
l. DECAL EXP GREEN 07-04 - 7690-01-GG0-1445

D. Optional Rank Tabs: The following tabs are optional. However, they may be required at some facilities for permit parking:

1. DECAL ADMIRAL 4 STAR - 9905-01-GG0-1115
2. DECAL ADMIRAL 3 STAR - 9905-01-GG0-1114
3. DECAL ADMIRAL 2 STAR - 9905-01-GG0-1113
4. DECAL ADMIRAL 1 STAR - 9905-01-GG0-1112
5. DECAL BUMPER CAPTAIN - 7530-01-GF2-8300

Chapter 8 SECURITY IDENTIFICATION BADGE SYSTEM

A. Purpose. This chapter governs the use and issuance of the Coast Guard Security Identification Badge (CG-5439) and Visitors Security Badge (CG-5439E). It provides information and procedures necessary to complete the Coast Guard Security Badge Record (CG-5448) and provides authorization to issue Coast Guard Security Identification Badges.

B. General. This system supports the various security programs as follows:

1. Information Security - the primary purpose for the badge is to immediately verify and identify an individual's present level of access to classified information.

2. Physical Security - the badge provides ready photographic verification of the holder’s status as a Coast Guard employee. The badge may be used in conjunction with other devices as necessary to enhance physical security, e.g., the card may be utilized with an electronic access control system to track an individual's travels, to grant entry or exit to selected areas, or to control entry times, dates, or conditions.

C. Policy.

1. Program implementation is at the discretion of the commanding officer. These badges are the only security badges that will be recognized Coast Guard-wide, for the control of access to classified information.

2. Upon written request, Commandant (G-CFI) will provide supply source information to Command Security Officers (CSOs). CSOs shall control and issue security badges to authorized personnel upon written request of the Classified Material Control Officer (CMCO). Security clearances shall be verified prior to requesting security badges. If a unit uses the badging system to enhance physical security alone, the individual's supervisor shall provide the written request to the CSO.

3. Personnel issued badges shall wear them prominently displayed in front, above the waist on the outer garment. The badge shall be displayed at all times while on units, except at special functions or ceremonies as deemed necessary by the unit. The security badge may be displayed in other government-controlled facilities, if necessary. The badge shall not be displayed outside of the unit area or other authorized government facilities. When off duty, the bearer shall remove the badge from the uniform or work attire and safeguard as a valuable government item.

D. Format/Characteristics.

1. The Security Identification Badge is a plastic, 2 3/8" by 3 7/8" card (see Exhibit 8-3). The security badge and badge record color coding corresponds with the approved classified information cover sheet color coding prescribed by General Services Administration (GSA)/Information Security Oversight Office (ISOO), 32 CFR 2003.

   a. TOP SECRET: Orange card with solid orange photograph background.

   b. SECRET: Red card with solid red photograph background.

   c. CONFIDENTIAL: Blue card with solid blue photograph background.

   d. NO ACCESS: Green card with solid white photograph background.

2. The security badge indicates the bearer's authorized access level. The badge is not meant to presume need to know or replace authorized receipt systems such as those used for classified message handling. The responsibility for determination of need to know before allowing access to classified information remains with the person controlling the information. Personnel controlling the access to restricted areas must still establish the bearer's need to enter for official business before allowing entry. Prior to transferring or discussing classified information, security badges shall be inspected visually to verify access level.

3. Visitor badges do not have subject photographs or identification information but are serially numbered and controlled. They follow the same color coding as the regular security badges and have a large color "V" overlaid on the face of the badge. This badge is intended to visibly identify visitors as authorized personnel while they are present within the unit.

E. Procedures.

1. Each area/district staff has been provided with complete badging system equipment. If a unit desires to check out the equipment or procure their own equipment, coordination shall be made with the cognizant SECMGR.

2. The CG-5448 (see Exhibit 8-1) shall be typewritten, using a 12 pitch-typing element. The signatures on the record and card insert shall be executed in black ink. The information required is self-explanatory, except as noted:

   a. The "Badge Number" is the serial number of the security badge (located on the back) issued to the individual;

b. The "Office" is the staff routing indicator or title, as appropriate (G-OPD, Ai, CO, XO, etc.);

c. The "Expiration date" is the last working day of the month, 4 years from the date of issue; i.e., 10/96 means the badge was issued during October 1992 and expires on 31 October 1996. The member's rotation date may also be used.

3. The CG-5448, regardless of the access level indicated, shall be retained by the CSO. The CMCO who conducted the individual's indoctrination briefing shall maintain a copy of the record. The record shall be designated FOR OFFICIAL USE ONLY (FOUO) and marked appropriately upon completion. Upon termination of access to classified information, the badge record and any copies shall be destroyed using the same methods approved for FOUO material.

4. Authorization to gather privacy information for routine uses of the information and the effect on individuals is provided in the Privacy Act Statement (see Exhibit 8-2). The Privacy Act Statement with signature and date shall be placed on the reverse side of the CG-5448 (see Exhibit 8-1).

F. Security and Accountability.

1. Accountability. A system shall be established to include a positive method for the return, destruction, or expiration of security badges when no longer authorized for use. A record of badges shall be maintained by the issuing authority for 4 years. Unissued badges shall be inventoried annually and the results maintained for 1 year.

2. Storage. Badges shall be stored in a locked container of at least 12-gauge steel. Access and key controls shall be established in accordance with Chapter 2.

3. Responsibilities. Badges will be returned to the CSO for destruction upon transfer. The CSO shall be immediately notified if a badge is lost or stolen.

EXHIBIT 8-1

FORM CG-5448
COAST GUARD SECURITY BADGE RECORD

COAST GUARD SECURITY BADGE RECORD

Name: (Last, First, Middle) Access Level

Badge Number Office Exp. Date

I.D. Number (Last four digits of SSN)

Approving Official's Signature

ATTACH
FILE
PHOTO

I have received my Security Badge.

I understand that this badge is for my official use only, and that it remains the property of the United States Coast Guard and must be returned upon request.

Member's Signature: Date:

U.S. Department of Transportation
United States Coast Guard

DEPT. OF TRANSPORTATION USCG, CG-5448 (9/86)

NAME

I.D. NO. | DIST. NO. | UNIT NO.

EMPLOYEE SIGNATURE

APPROVING SIGNATURE | EXP. DATE

BADGE INSERT

REVERSE SIDE

I HAVE READ AND ACKNOWLEDGE THE GATHERING OF THE INFORMATION CONTAINED HEREWITH IN ACCORDANCE WITH THE PRIVACY ACT OF 1974.

(SIGNATURE) (DATE)

EXHIBIT 8-2

PRIVACY ACT STATEMENT

Department of Transportation
Coast Guard Security Badge Record

CG-5448

1. AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING THE LAST FOUR DIGITS OF THE SOCIAL SECURITY NUMBER (SSN): Title 14 United States Code 93, Title 14 United States Code 141, Title 41 Code of Federal Regulations 101-20.302, Title 18 United States Code 1382, Title 5 United States Code 552a.

2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS TO BE USED: This Security Badge Record data will enable the record holder to more accurately administer and control the integrity of the Security Badge Program.

3. ROUTINE USES: Will include verifications by badge type or color, badge number, photograph, to whom badge was issued and to ensure the proper access level badge was issued for an individual's work assignment or area.

4. WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL IF NOT PROVIDING INFORMATION: For military personnel, the requested information is mandatory due to military security requirements. In the case of all other personnel, the requested information is voluntary. If the information is not furnished, the security badge will not be issued and access to controlled areas will not be allowed.

Chapter 9 LOSS PREVENTION

A. Purpose. This chapter establishes policy and procedures to maintain a comprehensive Loss Prevention Program. Loss prevention measures are actions taken to establish or maintain an adequate physical security and loss prevention posture. A vigorous Loss Prevention Program is essential at every unit to reduce property losses.

B. Property Management. Property Management Manual, COMDTINST M4500.5 (series) sets forth specific policies and procedures relative to the Property Management Program. Investigative Assistance, COMDTINST 5520.5 (series), provides the criteria to determine if investigative assistance by Coast Guard Investigative Service (CGIS) is warranted.

C. Responsibilities.

1. The Command Security Officer (CSO) is responsible for the implementation of the Loss Prevention Program, and the establishment, administration and coordination of all physical security measures to safeguard personnel and prevent unauthorized access to equipment, materials and documents. Additionally, the CSO shall:

   a. Ensure all personnel are educated and aware of their security and loss prevention responsibilities. Security Awareness, Training and Education Program, COMDTINST M5528.1 (series), and Military Personnel Security Program, COMDTINST M5520.12, provide guidance on conducting and recording briefings.

   b. Continuously review existing internal control procedures to provide the maximum protection for government property.

   c. Ensure that inventory records include the complete property identification data. In the event of loss or theft, this information will be required for investigative purposes.

   d. Ensure loss prevention measures are included in the unit physical security plan.

2. All personnel are responsible for immediately reporting losses to their supervisor. Personnel shall ensure that their areas are kept locked when no one is in the space.

D. Loss Reporting Procedures.

1. Reporting losses provides a measure of effectiveness for internal controls, stimulates reviews of inventory and accountability procedures, and reflects both weaknesses and strengths in the Physical Security Program.

2. The loss or theft of government property having an acquisition cost of $100 or more shall be reported to the cognizant security manager (SECMGR), with an information copy to Commandant (G-CFI). Exhibit 9-1 (sample message report) indicates the information required. If the aggregate dollar value is $1000 or more, the report shall also be sent to the cognizant CGIS office, with an information copy to Commandant (G-O-CGIS). Reports shall be submitted within 72 hours of discovery.

3. A report of recovery shall be made when the lost or stolen item is recovered. Reports shall include the following information:

   a. Notification to all addresses initially notified.

   b. Reference to the initial message report.

   c. List of item(s) recovered.

   d. Location and brief circumstances of the recovery.

4. Cognizant SECMGRs shall review reports of lost or stolen government property and if appropriate, conduct a security investigation to determine what additional investigation, if any, should be conducted as the result of lost or stolen government property. At the conclusion of the security investigation, SECMGRs shall recommend an administrative or criminal investigation be conducted, or when satisfied that no benefit would be derived from further investigation, close the case.

   a. Should circumstances warrant further investigation, a report shall be submitted to the commanding officer of the unit, with a copy to Commandant (G-CFI). The report shall include the following information:

      (1) Date of incident and circumstances that led to the security investigation.

      (2) Details of what was uncovered during the investigation, i.e., who, what, when, where, why, and how.

      (3) Recommendation/direction of the type of additional investigation to be conducted based on the information uncovered during the security investigation. If a criminal investigation is recommended, a copy shall be forwarded to the cognizant CGIS office.

   b. If no further investigation is warranted, it is not necessary to close the case in writing. Verbal notification to the unit will normally suffice.

5. Commandant (G-CFI) shall review reports of lost or stolen government property involving district and area staffs, and if appropriate, conduct a security investigation, and subsequently close the case. The Chief of Coast Guard Security (G-CFI) is the final review authority for all security related administrative investigations.

6. The loss or theft of Arms, Ammunition & Explosives (AA&E) shall be reported in accordance with the procedures outlined in Small Arms Manual, COMDTINST M8370.11. However, small arms and ammunition incapable of lethal use, i.e., demilitarized or replica drill weapons or practice or dummy ammunition shall be reported in accordance with this chapter.

7. If an item is unrecoverable, complete a Board of Survey (CG-5269) in accordance with Property Management Manual, COMDTINST M4500.5 (series), with a copy to the cognizant SECMGR.

E. Pilferage.

1. Pilferage may occur anywhere. The protection of supplies and equipment in storage areas, during the issue process, while in transit, and during use must be considered. The greatest deterrent to the pilferage problem is the risk of getting caught. A unit can control pilferage and decrease its vulnerability to this theft by reducing the targets of opportunity. In conjunction with an aggressive program of deterrence, reducing the targets of opportunity can be very effective. Depending on resources, one or more of the following may be used to reduce the targets of opportunity:

a. Decrease access to the item.

b. Provide strict inventory for early detection of loss.

c. Increase personnel involvement in spotting and preventing loss.

F. Personal Need or Desire. A person's need or desire for an item can only be altered by offsetting that need with serious deterrents. Stiff security measures and the imposition of swift and harsh penalties for offenders may convince the individual that they do not actually need the item, or that the cost of getting caught trying to obtain it illegally far outweighs the cost of obtaining it legally.

G. Inventory Control. Strict inventory control allows a unit to keep a tight control on the location of items, which, in turn, allows for early identification of a lost item and greatly increases the chances of catching the thief. The casual pilferer is much more likely to take an item that will not be missed for several days, thus decreasing the chances for being caught.

H. Inspections.

1. All personnel and vehicles are subject to inspection in accordance with Coast Guard regulations and General Services Administration (GSA) directives when entering and leaving a unit. Any person observed removing property that is not clearly identified as personal property shall be challenged and the authority for removal of the property shall be fully established.

2. The purposes of inspections are to ensure:

   a. Classified material is arriving/departing the unit properly packaged and with proper authorization;

   b. Government property is being delivered or removed from the unit with proper documentation;

   c. Unauthorized items are not being brought into the unit.

3. Inspections shall be conducted on a random basis and the results submitted to the commanding officer for review.

4. Articles to be inspected include, but are not limited to:

   a. Attaché/brief cases

   b. Pocketbooks/purses/handbags

   c. Lunch pails/buckets

   d. Shopping bags/paper bags

   e. Packages, cartons, boxes, etc.

EXHIBIT 9-1

SAMPLE REPORT OF LOSS OF GOVERNMENT PROPERTY

(DATE TIME GROUP)

FM ACCOUNTABLE UNIT

TO COGNIZANT SECMGR (FOR $100 OR MORE)
AND
COGNIZANT CGIS OFFICE (FOR $1000 OR MORE AND IF CGIS ASSISTANCE IS REQUESTED)

INFO COMDT COGARD WASHINGTON DC//G-CFI/G-O-CGIS//

BT

UNCLAS //N05530//

SUBJ: REPORT OF LOSS OF GOVERNMENT PROPERTY

A. COMDTINST M5530.1 (SERIES), CHAP 9

1. TYPE OF ITEM: *FACSIMILE MACHINE*

2. SERIAL NUMBER: *05930184365*

3. OWNER-APPLIED NUMBER: *CG00001124*

4. BRAND NAME: *PANASONIC*

5. COLOR AND MODEL NUMBER: *GRAY, PX-150*

6. DOLLAR VALUE: *$550.00*

7. DATE OF LOSS: *31 MAR 94*

8. LOCATION AND BRIEF CIRCUMSTANCES OF THE LOSS: *DISCOVERED MISSING UPON COMPLETION OF OFFICE RENOVATIONS. ITEM WAS LAST ACCOUNTED FOR WHILE MOVING INVENTORY TO WAREHOUSE BEFORE RENOVATIONS BEGAN***.**

9. PERSONNEL NOTIFIED (IF ANY): *NOTIFIED OOD AND COMMAND SECURITY OFFICER. (INCLUDE LOCAL LAW ENFORCEMENT AGENCY IF APPROPRIATE AND INDICATE IF REPORT FILED).*

10. CORRECTIVE ACTION TAKEN TO PREVENT SIMILAR LOSS: *ENSURE ALL OFFICE EQUIPMENT IS STORED IN A CONTROLLED ACCESS SPACE AND INCREASED INVENTORIES / SPOT CHECKS CONDUCTED DURING RENOVATION PROCESS.*

11. INTENTIONS REGARDING FURTHER LOCAL INVESTIGATION: *OUTLINE INTENTIONS. ARE YOU CONDUCTING AN ADMIN INVESTIGATION?*

12. CGIS ASSISTANCE REQUESTED: *(YES/NO); OUTLINE WHAT ASSISTANCE YOU ARE REQUESTING.*

BT

Chapter 10 SECURITY AND POLICE FORCES

A. General. Commanding Officers, may, at their discretion establish a security force to meet local security needs. Commanding Officers may also establish a police force, to meet internal law enforcement needs, upon approval of Commandant (G-CFI). This chapter sets the minimum standards and guidelines if such forces are established. Cognizant Security Managers (SECMGRs) should be consulted for guidance in complying with this chapter.

B. Purpose. Security and police forces are enforcement and protection mediums, which constitute one of the most important elements of a unit's Physical Security Program. Security and police forces consist of designated persons who are specifically organized, trained, and equipped to provide physical security and/or law enforcement for the unit. Properly used, they can be one of the most effective and useful tools in a comprehensive, integrated Physical Security Program.

C. Responsibilities.

1. Commandant (G-CFI) develops policy, procedures and standards governing the operation of Coast Guard security forces and police departments, and serves as the U.S. Coast Guard Police Commissioner and final approving authority for all Coast Guard Police Departments.

2. The individual unit commanding officer has the ultimate responsibility for the security of their command.

3. On Coast Guard facilities with multiple commands/units, the host command is responsible for the physical security of the overall facility, internal law enforcement within the facility, and for providing security force and/or police force protection for the facility and personnel assigned to the facility. The above responsibility of the commanding officer may be altered by a written host/tenant agreement, which should specifically delineate the variation in responsibilities. This agreement shall be reviewed by the cognizant SECMGR.

4. The Command Security Officer (CSO) of the host command is the commanding officer's principal advisor for physical security and internal law enforcement. He or she is responsible for monitoring and assuring the implementation of this instruction in regards to security and/or police force services.

5. The Chief of Police (CP) of the host command shall direct/supervise all police/internal law enforcement operations, and where applicable, security force operations.

6. Units shall not consolidate or integrate security and police forces with fire prevention/protection forces.

D. Categories.

1. Security Guards.

a. General Service (GS-085) security personnel are uniformed civilian employees of an agency of the government, who guard and protect government property. They do not have police powers, or the authority to enforce the UCMJ. Military personnel may also serve as security guards. and may have authority to enforce the UCMJ, Security personnel shall be identified by a security patch, as shown in Exhibit 10-1.

b. Guard services may also be provided by a contractor. Contract security must be carefully overseen; otherwise, service may not fulfill particular security needs.

2. Police. Military and General Service (GS-083) police personnel assigned to a Coast Guard police department shall be given the authority to enforce federal and local laws as applicable, as well as the Uniform Code of Military Justice (UCMJ). Police personnel shall be identified by a police badge and patch, as shown in Exhibit 10-1.

3. Foreign Security and Police Forces. In overseas locations, certain Coast Guard units are also protected by foreign nationals. In such cases, rules and policies governing foreign security and police forces will be determined locally per applicable agreements, laws and treaties.

E. Establishment.

1. Each base commander has the inherent authority to establish a base security force by virtue of the Commandant's general powers to "maintain and operate" Coast Guard shore facilities (14 U.S.C. 93(b) and (j)). Because a base commander has an obligation to protect their facility, it is within their discretion to establish a Coast Guard security/police force to accomplish that goal. The commanding officer may also enter into a contract with a civilian security agency for the protection of the facility.

2. The establishment and certification of a Coast Guard Police Department shall only be accomplished through the written approval of the U.S. Coast Guard Police Commissioner (G-CFI). Commanding officers desiring to establish a police department shall submit requests for certification to Commandant (G-CFI). The request must outline their need and intentions for the use of the police force and include a statement of justification as to why a security force will not meet their needs.

3. While it is true that Coast Guard commissioned, warrant and petty officers are "Officers of the Customs" by virtue of 14 U.S.C. 143 and 19 U.S.C. 1401, that fact is unrelated to the authority of a commanding officer to establish a security/police force. The Coast Guard's general maritime authority under 14 U.S.C. 89 is also unrelated to a base commander's authority to establish a base security/police force. Neither of these statutes should be used as reference for the establishment or conduct of base security/police forces.

F. Functions.

1. Detect/deter and defeat terrorism.

2. Prevent/deter theft and other losses caused by fire damage, accident, trespass, sabotage, espionage, etc.

3. Protect life, property and the rights of individuals.

4. Enforce rules, regulations and statutes.

5. Implement and enforce the personnel identification and control system.

6. Observe and patrol designated perimeters, areas, structures and activities of a security interest.

7. Detain/apprehend/arrest persons and vehicles gaining unauthorized access to security areas.

8. Check designated depositories, rooms, or buildings, of a security interest during other than normal working hours to determine that they are properly locked or otherwise secure.

9. Report to the appropriate supervisor, as a matter of prescribed routine under normal conditions, and as necessary in the event of unusual circumstances.

10. Perform essential escort duties.

11. Respond to intrusion alarm signals or other indications of suspicious activity.

12. Generally, safeguard data, materials, and equipment against unauthorized access, loss, theft, or damage.

13. Conduct pedestrian and vehicle inspections and searches, in accordance with this manual, current unit policy, and the Manual for Courts-Martial (MCM) (Military Rules of Evidence 313, 314, 315).

G. Authority.

1. Although it does not confer general, law enforcement authority, 14 U.S.C. 93(e) authorizes a base commander to conduct investigations that may be of assistance to the Coast Guard in its performance of any of its powers, duties or functions. Accordingly, Coast Guard police or security forces may be used to conduct investigations that fall short of criminal investigations. Primary responsibility to conduct criminal investigations lies with the Coast Guard Investigative Service (CGIS) in accordance with Investigations Manual,COMDTINST M5527.1A.

2. The authority to apprehend is described in Article 7, UCMJ (10 U.S.C. 807) and R.C.M. 302, Manual for Courts-Martial. See also Appendix 21, Manual for Courts–Martial for a discussion of the power to apprehend. The word "apprehend" is used in lieu of arrest when dealing with members of the U.S. Armed Forces. The peculiar military term “apprehension” is statutory (article 7(a)) and cannot be abandoned in favor of the more conventional civilian term “arrest”.

   a. Arrest is the restraint by an order not imposed as punishment for an offense and directs that a person stay within a certain area.

   b. Apprehension is the taking into custody of a person, apprehension under the UCMJ is, therefore, approximately equal to the common law definition of arrest.

   c. Confinement is the physical restraint of a person.

3. Regardless of the type of jurisdiction. Coast Guard members, as members of U.S. society, have common law “citizen” arrest authority. Citizens generally have the power to arrest someone for the commission of an offense, if that offense is committed in their presence. In order to perfect a citizen’s arrest, reasonable force (short of deadly) may be used. However, any use of force that is unreasonable may expose the arresting citizen to both civil and criminal liability. Because the law surrounding citizen’s arrest is complex and varies from state to state, it is best to avoid its use as a means of military law enforcement

4. All military law enforcement officials, have the power to apprehend military members upon probable cause (a reasonable belief that an offense has been or is being committed and the person to be apprehended committed or is committing the offense), provided that the apprehension is made in the execution of law enforcement duties. Article 7, UCMJ (10 U.S.C. 807), Rules for Courts-Martial (R.C.M.) 302(c). In addition, a commissioned, warrant, or petty officer has the power to apprehend a military member based upon probable cause even when he or she is not performing law enforcement duties. They also have the authority to apprehend persons subject to the Uniform Code of Military Justice (UCMJ) who

take part in quarrels, frays, or disorders, wherever they occur. Article 7, UCMJ (10 U.S.C. 807) R.C.M. 302(c).

a. Military law enforcement officials include security police, military police, master-at-arms personnel, members of the shore patrol, and persons designated by proper authority to perform military criminal investigative, guard, or police duties, whether subject to the code or not. R.C.M. 302(b)(1). Moreover, any commissioned, warrant, or petty officer has the authority to apprehend persons subject to the code. R.C.M. 302(b)(2). Coast Guard police officers would clearly qualify as military law enforcement officials.

b. Because military law enforcement personnel below the rank of petty officer only have the power to apprehend while they are engaged in law enforcement duties. It is important for all Coast Guard police officers below the rank of E-4 to wear badges and other insignia denoting them as military law enforcement officials. <u>From a policy standpoint, all Coast Guard members who are assigned to military law enforcement duties shall display the appropriate badge and insignia regardless of rank</u>.

5. Authority for military law enforcement officials to apprehend civilians has been inferred from UCMJ Art. 9(e), 10 U.S.C. 809(e) and from 18 U.S.C. 1382 (makes punishable the entry onto a military installation for any purpose prohibited by law or regulation, or after having been removed therefrom). The authority is limited to the confines of the military facility or in some circumstances the areas immediately surrounding the military facility, and must be based on probable cause. This authority is derived from the power to maintain order, security, and discipline on a military reservation as is necessary to military operations.

a. Although it would be legally permissible for a military law enforcement official, when engaged in "hot pursuit," to apprehend a civilian who flees off base. Extreme caution should be exercised when this type of enforcement action is undertaken. The suspected criminal action must warrant the pursuit outside of the military facility. In addition, military law enforcement personnel, by agreement, may assist federal or local law enforcement agencies. 14 U.S.C. 141(a). When doing so, they may gain law enforcement authority over civilians outside of the military facility, by virtue of their status as agents of the law enforcement agency that they are assisting. However, caution should be exercised anytime Coast Guard police officers attempt to assert control over a civilian outside the confines of the military facility to which they are assigned. If it is later determined that the Coast Guard police officer was acting outside the scope of his or her authority, both the Coast Guard and the individual member could be subject to considerable liability.

b. In addition to the limited authority to apprehend civilians, military law enforcement officials may also conduct reasonable searches based on a valid arrest or search warrant.

H. Jurisdiction.

1. General.

a. The jurisdictional status of a particular base is irrelevant to whether or not a base commander may establish a police force. Since the underlying authority for the police force is derived from the power to maintain order, security, and discipline on the military reservation, the establishment of a Coast Guard police force, even when the Coast Guard has only proprietary jurisdiction, would be permissible.

b. Where jurisdiction becomes important, is in the determination of which laws apply on a particular base and whether local law enforcement personnel have jurisdiction to enforce those laws.

2. Types. The three types of jurisdictions are exclusive, concurrent and proprietary. Each unit must be aware of the type of jurisdiction it falls under in order to publish proper guidance for its security and police forces. Jurisdiction is not determined by the commanding officer but is federally mandated. Units should consult with local and district legal authorities if jurisdiction has not been clearly established.

a. Exclusive Federal Jurisdiction. On an exclusive federal jurisdiction, all federal criminal law and most state criminal law (through the Assimilative Crimes Act, 18 U.S.C. 13), are applicable to all persons (military and civilian) aboard the facility. Even when state law is being enforced on an exclusive federal enclave, it is considered "federal law" because the state law has been "assimilated" into federal law pursuant to the Assimilative Crimes Act. In view of the fact that it is federal law which is being enforced on an exclusive federal reservation, only the federal government has the power to make and, through its various agencies including the military, to enforce the law. Thus, only the specific federal criminal statutes and the crimes adopted through the Assimilative Crimes Act are applicable. Generally, state laws have neither force nor effect; and state and municipal police authorities and other local law enforcement officials generally have no jurisdiction. Thus, on such a military base, it is the base police, or some other federal law enforcement entity, which have the power to apprehend offenders.

NOTE. To avoid the task of maintaining a complete code of civilian criminal laws for military bases and other federal property, Congress passed the Assimilative Crimes Act. In this statute,

Congress provided that all acts or omissions occurring in an area under federal jurisdiction (exclusive or concurrent) that would constitute crimes if the area were under state jurisdiction, will constitute the same crimes, similarly punishable, under federal law. For illustration, Congress has not enacted a traffic code. However, a person speeding on a Coast Guard facility could be charged with a federal traffic violation because the local state's traffic laws are adopted for federal use on that facility.

b. Concurrent Federal Jurisdiction. Both the federal and state government (including county and municipal subdivisions) has authority to make and enforce general municipal laws on the land in question. Thus, one offense could be a crime against the federal government and also against a local state's law. Both Coast Guard and state authorities could enforce and prosecute under their respective law. State and municipal police have concurrent authority to arrest persons (military or civilian) aboard a concurrent jurisdiction base. Normally, civilians who commit offenses on concurrent jurisdiction bases are turned over to local law enforcement. Military law enforcement officials should "detain" the civilian offender, until the individual can be turned over to the local police.

c. Proprietary Jurisdiction. A proprietary jurisdiction exists when the federal government has acquired a degree of ownership in the base similar to that of a landowner or tenant, but has not obtained legislative authority over the area. Generally, the state or local municipal law enforcement entity would have the exclusive power of enforcement and arrest over civilians who commit an offense aboard a base with only proprietary jurisdiction. However, the Coast Guard has the right (as does any landowner or tenant), to protect its property. In addition, state and local authorities cannot interfere with any valid military activity on such land. Military law enforcement officials may "detain" the offender, until the individual can be turned over to the local police.

3. Territorial. Military reservations are generally categorized as having either exclusive federal jurisdiction or concurrent federal jurisdiction. The federal government may also hold territory in a status of proprietary interest. Jurisdiction in this context refers to the authority to enact and enforce general criminal laws within a given area. This refers to units with two or three types of jurisdictions within itself.

4. Assistance to Local Authorities. The Coast Guard may utilize its personnel and facilities to assist any federal agency, state, territory, possession, or political subdivision thereof, or the District of Columbia, to perform any activity for which such personnel and facilities are especially qualified.

a. Title 14 U.S.C. 141(a) provides authority for Coast Guard personnel, including Coast Guard military law enforcement personnel, to assist state or local governments. It specifically requires that the state or local government request the assistance of the Coast Guard, and limits that assistance to activities for which the Coast Guard personnel or facilities being requested are specifically qualified. Before providing assistance, advice should be obtained from local and district legal authorities.

b. If Coast Guard police units are requested to assist federal, state or local law enforcement agencies, they may do so provided they only perform law enforcement duties. Consistent with that authority, base commanders may also enter into Memorandum of Understanding (MOU) for providing law enforcement assistance to the local law enforcement agencies. All MOUs should be reviewed by the cognizant Coast Guard legal office prior to its entry into force.

5. Posse Comitatus Act. The Posse Comitatus Act (Title 18 U.S.C. 1385) prohibits the use of any part of the Army or Air Force to enforce local, state, or federal laws except as congress may authorize. Moreover, the Act applies only to the DoD forces and normally has no application to the Coast Guard. Although not expressly applicable to the Navy and Marine Corps, the Act is regarded as a statement of federal policy, which is closely followed by the Department of the Navy. Though the Navy and Marine Corps are not expressly included within the provisions of the Act, they have adopted the policies of the Act by regulation. However, Department of Defense (DoD) assistance is not entirely precluded. Congress has facilitated effective cooperation between DoD and non-DoD agencies. Refer to Title 10 U.S.C. 371-378. NOTE: THE POSSE COMITATUS ACT DOES NOT APPLY TO THE COAST GUARD. Generally, the Posse Comitatus Act does not restrict military law enforcement officials from enforcing law aboard military bases. It would not inhibit a Coast Guard police force while it is conducting normal military law enforcement operations.

I. Size. The size of security and police forces is dependent upon many factors:

1. Size and location of the unit.

2. Assets to be protected.

3. Number, type and size of restricted areas.

4. Use of alternate security support measures and effectiveness of mechanical or electronic security measures.

5. Quality of security/law enforcement support provided by other agencies.

6. Total daily population of the unit and its composition, including residents in housing areas.

J. Security and Police Force Standing Orders. The commanding officer of each unit shall publish and maintain security and police force standing orders pertaining to each post. These orders are the written and approved authority given by the commanding officer to personnel to execute and enforce regulations.

1. All standing orders shall specify the limits of the post, the hours the post is to be manned and the orders, duties, uniform, arms and equipment prescribed for personnel.

2. Copies of standing orders shall be conspicuously displayed or immediately available for reference by all security and police force personnel.

3. All standing orders shall be brief, clear and concise, and written in simple language. The CSO/CP shall conduct a detailed review at least annually.

4. Mobile units may incorporate these standing orders into the Commanding Officer's standing orders for the Officer of the Deck if such orders are deemed necessary for the security of the unit.

K. Personnel Selection.

1. Care in the initial selection of security and police force personnel and in elimination of the marginal performer during early training is paramount. Turnover in security and police forces is undesirable for the following reasons:

a. Release of personnel trained in sensitive operations creates a possible source of information for persons seeking to discover vulnerable points of a security system.

b. There is a high financial cost factor in training replacements.

c. Frequent turnover breaks continuity of procedural familiarity and experience, which results in reduced readiness and less effective protection.

2. Personnel previously released from security or police duties for other than normal conditions (rotation, end of active service, hardships, etc.), shall not be reconsidered for return to security or police duty.

3. Physical Health Standards. Security and police force personnel shall be physically agile, mentally alert and possess good judgment.

a. They must not have any medical condition(s), medication(s), or restriction(s) which would preclude their full performance of duties as a protection officer.

b. They must be free of any psychological or mental condition which could cause impaired alertness, judgement, or motor ability. A history of clinically significant emotional or behavioral problems shall require thorough clinical evaluation which may include, but not necessarily be limited to , psychological testing and psychiatric evaluation.

c. They must possess normal motor power, range of motion, neuro-muscular coordination and dexterity.

d. They shall be free of any condition, habit, or practice which could reasonably be expected to result in sudden, subtle, or unexpected incapacitation.

e. They shall have no background of incidents of attempted suicide or an expressed threat of suicide.

f. They shall be free of any condition in which a person's intake of alcohol is sufficient to damage their physical health, job performance, personal functioning, or when alcohol has become a prerequisite to their daily functioning.

g. They shall have no background of condition in which a person is addicted to or dependant on drugs as evidenced by habitual use or a clear sense of need for the drug. This includes the use of prescribed or otherwise legally obtainable medication taken in such a dosage that a temporary delay in taking such medication might result in unacceptable incapacity.

h. They shall be free of the physical inability to wear the uniforms and equipment as issued.

i. They shall be free of any other disease or condition which would interfere with the full performance of duties as a protection officer.

4. U.S. Coast Guard security and police force personnel shall clearly speak and write the English language, as well as understand direction given in English.

5. As specifically covered by law, any individual who has been convicted of a qualifying misdemeanor crime of domestic violence, is not able to lawfully possess or receive firearms or ammunition for any purpose including their official duties. This disability applies to firearms and ammunition issued by government agencies, firearms and ammunition purchased by officials for use in performing their official

duties, and personal firearms and ammunition possessed by such individuals. Such individuals shall not be assigned to any security/police function that has the possibility of requiring access to firearms.

6. Minimum civil service qualifications are specified in civil service qualification standards. Positions shall be established on the basis of duties actually performed (e.g., a position with more than 50 percent police duties will be classified in the police series (GS-083)).

7. All contract guard services shall be coordinated with the cognizant SECMGR.

L. Personal Supervision. Close personal supervision of security and police forces are a necessary element for a successful security program. Supervisors shall perform the following functions:

1. Supervise the issue and recovery of all security and police force weapons and ammunition, in accordance with Small Arms Manual, COMDTINST M8370.11 (series).

2. Inspect security and police force personnel prior to posting.

3. Inform security and police force personnel of any special orders or instructions.

4. Inspect security and police posts at least once per shift to ensure personnel and systems are functioning properly.

5. Ensure compliance with all standing orders, directives, laws and ordinances.

M. Indirect Supervision. Various means may be used to facilitate and supplement personal supervision of security and police forces.

1. Recorded Tour Systems. Under these systems, security and police forces record their patrols or presence at designated places throughout the unit by use of portable watch clocks or central watch-clock stations (e.g., Detex time punch clock, Morse watchman etc.). These systems are an effective means of ensuring that certain points are regularly patrolled.

2. Portable Radios or Call-In Boxes. Telephone boxes can be located at points throughout large units. Security and police forces can use these call-in boxes to call in and report or receive instructions. Portable radios and remote paging devices are recommended because they are cost effective and afford versatility.

N. Determination of Posts. Since no two units will present the same degree of risk or contain identical situations, it is impractical to set fixed rules to apply to all units. Commanding officers must ensure that an analysis of their unit is performed to determine the number

and type of posts required to provide optimum and cost-effective protection. Consideration should be given to employing alternative security measures whenever feasible, such as Intrusion Detection Systems (IDS), Closed Circuit Television (CCTV), securing nonessential gates, etc.

O. Types of Posts. Posts will normally be of three basic types:

1. Fixed. Where security and police personnel normally remain at one point or within a specific area, (e.g., gates and towers).

2. Mobile. These posts may also be referred to as roving patrols. They are used for perimeter surveillance, area patrols, etc. Security and police forces may be on foot or in vehicles, or both.

3. Administrative. These posts include the CSO/CP and other supervisory personnel; identification and pass clerks; dispatchers; alarm system monitoring personnel; physical security and law enforcement training specialists; investigators, court liaisons, etc.

P. Post Requirements and Considerations.

1. Gates. Gates shall be limited to the minimum number required to permit expeditious flow of traffic in and out of the unit. Except where justified by consistently heavy traffic throughout the day or by other security considerations, one sentry per gate will normally suffice. Rush hour augmentation manning must be included in post calculations. Using personnel obtained temporarily from mobile posts to man fixed posts reduces emergency response capability to alarms, accidents and traffic problems. Full-time use of a guard at a railroad gate or a construction gate when nothing more than intermittent use is made of the gate may not be justified unless the guard has collateral duties.

2. Perimeter. The justification for perimeter posts is in direct proportion to the necessity for preventing unauthorized entry. Unit “A” may have to be maintained at all costs. Perimeter protection there would call for a combination of approved fencing, protective lighting and IDSs, all supported by numerous fixed posts and with mobile patrols operating in relatively small areas. On the other hand, unit “B” may be able to meet security requirements by using nothing more than a fixed or mobile post.

3. Area Posts. Guarding of areas must be commensurate with the importance of the area/assets being guarded and the threat. For example, heads of state, foreign dignitaries, guesthouses, contraband storage warehouses, etc., may require an increased level of protection.

4. Motorized Patrols. Two person patrols are more desirable due to personal safety, as well as providing immediate backup during responses to high-risk areas.

5. Funds Escorts. Escorts for funds movement should, whenever possible, comply with applicable state and local laws concerning weapons and emergency vehicles. If funds escort requirements can be anticipated on a frequent or recurring basis, use of commercial armored car service should be considered. Chapter 6 provides additional guidance for funds escorts.

6. Visitor Escorts. It is normally not appropriate to establish full-time security and police posts for visitor escorts within restricted areas. The person receiving visitors or his/her representative should escort to and from the restricted area gate. Similarly, in the case of off-station trucks, the department to which shipments are consigned will furnish necessary escorts within restricted areas, unless specific directives concerning the type or sensitivity of the shipment require armed security or police escorts. Commanding officers shall determine the need for providing visitor escorts within non-restricted areas based on local need.

Q. Determination of Strength.

1. The degree of security achieved at any unit will depend on the efficiency of security and police forces assigned. However, seldom will any unit have sufficient available manpower to provide all the personnel that are desirable. Accurate man-hour planning must be carefully computed before reliable manpower requirements can be determined.

2. Calculation is influenced by many factors:

   a. Mission of the unit.

   b. Type and jurisdiction of the property.

   c. Geographic location and size of the unit.

   d. Topography of the area.

   e. Economic and political atmosphere.

   f. Existing and potential threats.

   g. Logistical, operational and quality of support provided by other agencies.

R. Estimating Security and Police Force Strength Requirements.

1. When determining staffing requirements, refer to Staffing Standards Manual, COMDTINST M5312.11 (series).

2. Factors include the hours of refresher training per year per person, normal days off for annual and sick leave as well as specialized training. If special assignments are valid security and police responsibilities and the man-hour requirements are consistent and can be gauged on the basis of "averages" indicated by past experience, appropriate adjustment of security and police force requirements can be made. If, however, such requirements are intermittent or generally of limited duration, consideration should be given to the use of overtime or doubling up of posts. Special details or miscellaneous assignments, which are not valid security and police functions, must be curtailed.

3. Post requirements for some supervisory personnel may be included in post computations (such as one field supervisor required 24 hours per day, 7 days per week, to provide oversight and evaluation of security and police personnel effectiveness).

S. Emergency Planning and Auxiliary Security and Police Forces.

1. As part of the crisis management portion of the physical security plan, plans must be prepared for security and police force personnel to provide additional security, as required, during emergencies. These plans may also provide for the essential training of augmentation personnel and rapid identification and acquisition of emergency equipment and supplies. Other elements, including civilians, may be used as support/staff elements during emergencies for functions such as medical assistance, firefighting, construction, casualty evacuation, communications, etc. Written support agreements or Memorandums of Understanding (MOU) shall be executed with federal, state and local agencies that provide assistance and response.

2. Units with large populations may form auxiliary security and/or police forces. They should be organized as a branch of the permanent security and police force and shall fall under the supervision of the CSO/CP.

   a. The size will depend on the size of the unit, criticality of assets to be protected and the number of personnel required to man additional security and police posts. It should be sized to permit full manning of posts and patrols required in Terrorist Threat Condition (THREATCON) "D" and be able to sustain a security posture for at least 5 days.

   b. Auxiliary security and police forces may be composed of permanently assigned personnel from host and tenant commands. They should be

organized into two watches that include supervisors and individual post standers. Personnel should be required to qualify in accordance with current unit security and police standards prior to assignment.

(1) Following initial training and weapons qualification, personnel should be assigned duties twice a month as a means of continued training. Entire auxiliary security and police forces should have quarterly exercises to further training and education in their security or police duties.

(2) Personnel should be provided with the equipment necessary to perform their security or police duties.

T. Security Investigations for Security and Police Forces. A National Agency Check with Local Agency Checks and Credit Check (NACLC) is required for all security and police force personnel in accordance with Military Personnel Security Program, COMDTINST M5520.12 (series).

U. Uniforms.

1. General.

a. Security and police personnel shall present themselves in a neat, sharp and professional manner. The patrol officer is often an outsider's first impression of the Coast Guard. However brief the contact, it should be one that makes the impression of total professionalism. The wearing of the uniform shall be a matter of pride. Each security or police force member is a representative of the Coast Guard; their appearance should reflect upon themselves and their unit.

b. The official uniform to be worn by military security and police force personnel shall be the working uniform/uniform of the day, as prescribed by the commanding officer. The official uniform to be worn by civil service security and police force personnel shall be at the discretion of the commanding officer. The official uniform to be worn by contract security force personnel shall be that which is specified in the contract.

c. All members of the security or police force must wear the same uniform. Only those insignia specifically authorized by Uniform Regulations, COMDTINST M1020.6 (series), and this chapter shall be worn.

d. The practice of designing and procuring local USCG law enforcement insignia for wear is specifically prohibited.

2. Headgear.

a. Ball caps may be worn in place of the Coast Guard combination or Garrison cap at the commanding officer's discretion. The words "SECURITY" or "POLICE" shall be in bold gold (yellow) print on the front of the cap. Alternatively, a smaller version (3 ½ X 2 ¾ inch) of the patch, as shown in Exhibit 10-1, may be permanently attached to the front of the cap. In the latter case, the stitching attaching the patch and the background color of the patch shall be the same dark blue material as the cap. These ball caps shall be procured by the unit and issued to security/police force personnel. Health considerations preclude designating these items as organizational clothing. Unit insignia, logos or other artwork is not permitted.

b. If, in the opinion of the command, safety considerations dictate the wearing of headgear which provides a greater measure of protection, during security/police operations, they may procure and issue protective helmets and optional face shields. These helmets shall have a white outer shell and be clearly marked with the USCG security/police force emblem.

c. All members of a security/police force shall wear the same headgear. The wearing of other headgear not specifically authorized is prohibited.

3. Footwear.

a. For many types of security activities the standard issue black steel-toed working boot is appropriate footware and shall be worn. As an option, security forces are authorized to wear a more flexible safety shoe meeting the following minimum criteria: black canvas/leather uppers; black non-marking/non-skid soles; steel-toed footware is highly recommended but is not mandatory; (no other color may be visible on the footware such as product labels, striping, etc.).

b. Health considerations preclude designating footware items as organizational clothing.

c. All members of a security/police force shall wear the same color and type of footware.

d. Whatever footware is worn, it must be free of unsightly paint, grime, scuff marks and other stains.

4. Uniform Insignia.

   a. Collar insignias shall be worn in lieu of rank insignias and in compliance with current, Coast Guard uniform policy. They shall be yellow/gold C.G.P.D or C.G.S.F letters, approximately ½ X 4 inches in size. Epaulets of all outer garments (winter reefer, windbreaker, rain coat, etc.) shall display the yellow/gold C.G.P.D or C.G.S.F letters. COMDT (G-CFI) can provide information on suggested source of supply upon request.

   b. In general, permanently assigned security and police personnel are not required to reveal their military rank or rating while conducting official business. Security and police personnel conduct business on behalf of the host commanding officer and shall be treated with the utmost respect and courtesy, regardless of their rank or rating. Conversely, any abuse of their authority will not be tolerated and shall result in disciplinary action and possible removal from security and police forces. If officials persist in questioning personnel about rank or rating, the matter should be referred to the CSO/CP.

5. Outer Garments. When normal uniform outer garments, as prescribed by the Uniform Regulations, are inadequate or inappropriate for wear during security or law enforcement activities due to inclement weather or climatic conditions, units shall procure and provide appropriate protective outer garments as organizational clothing, as authorized by the Uniform Regulations. All members of a security/ police force shall wear the same color and type of outer garments.

6. Coveralls. Coveralls are not normally authorized for use as a security/police uniform. However, commands may authorize the wear of coveralls when conditions exist that would likely soil or damage the normal uniforms.

7. Body Armor.

   a. The appropriate body armor shall be worn at all times while: (1) carrying a weapon in the performance of law enforcement and other security activities; and (2) while transporting weapons. All armed security and police force members, while enroute to or from, and during law enforcement operations, shall wear body armor.

   b. Body armor may be worn either under the uniform shirt or when supplied with a dark blue cover, over the uniform shirt and under an outer garment. If the outer garment is anticipated to be taken off at any time during the security/police operations, the body armor shall be worn under the uniform shirt. At no time, during normal operations, will body armor be worn over the uniform shirt without an outer garment.

c. Body armor is not required to be worn during routine patrol operations, however it must be immediately available to the patrolling security/police officer and be donned prior to the initiation of any law enforcement activity.

d. Any deviations from these body armor requirements must be approved in writing by the District/Area Commander.

e. No specific manufacturer of body armor is required. Any body armor which provides full front, side and back protection between the base of the neck and the belt line and provides Level IIa (IACP, NIJ-STD-0101.03) or greater protection against penetration and deformation may be worn. All new purchases of body armor must provide a minimum of Level IIa protection and be National Institute of Justice (NIJ) certified. This NIJ certification will be displayed on the body armor manufacturer's label.

8. Bicycle Patrol Uniforms. Units establishing a security/police bicycle patrol shall submit a proposal for modified uniform requirements to COMDT (G-CFI).

V. Patches, Badges and Credentials.

1. Exhibit 10-1 provides design specifications for Coast Guard standard issued badges and patches. Coast Guard issued badges shall be accountable and ordered via the cognizant SECMGR. No other patches/badges for security and police forces are authorized. Units are to curtail usage and dispose of all unauthorized patches/badges. Personnel not assigned to security or police force duty, as a Security Manager or Security Specialist, or Coast Guard Investigative Service (CGIS) duties shall not wear, display or represent themselves with any type of badge or patch not specifically authorized by Commandant (G-CFI or G-O-CGIS). Units may obtain armbands (brassards) for OODs, junior officer of the day (JOODs), Master at arms (MAAs), etc.

2. Police personnel shall wear the police patch and badge, as shown in Exhibit 10-1. Security personnel shall wear the security patch, as shown in Exhibit 10-1. Contractor personnel shall wear contractor issued patches and badges, as specified in the contract.

3. The patch shall be permanently attached to the left and right sleeves of all shirts and outer garments, positioned approximately two inches down from the upper most seam of the shirt, coat, etc. The six point star badge shall be worn centered ¼ of an inch above the left breast pocket. In the event service ribbons are worn, the badge is to be suspended or pinned centered ¼ of an inch below the lower edge of the left breast pocket flap.

4. Badges and credentials for police personnel should be carried on the person at all times while in the performance of official duties. Credentials (with photograph) should contain the following information:

   a. Personal Identification (name, height, weight, eye/hair color).

   b. Social Security Number.

   c. Badge/Credential Number.

   d. Bearer's Signature/Authorizing Signature.

   e. Appropriate Authority/Jurisdiction/Limitation.

5. The badge and credential shall be used only for official business and shall never be surrendered except when ordered by the CP. Personnel shall not use their official position, official identification, or badges:

   a. for personal or financial gain;

   b. <u>to gain privileges afforded Civil Police Authorities</u>, or other special privileges not otherwise available to them;

   c. for avoiding the consequences of illegal acts; or

   d. to obtain information outside their scope of duties which is not otherwise available to them.

6. The loss of a badge or credential shall be immediately reported to the CP who shall direct an investigation to determine the circumstances of the loss, and then notify Commandant (G-CFI) via the cognizant Security Manager. The CP shall also notify local Civil Police Authorities and the cognizant CGIS office.

7. Unissued badges and credentials shall be stored in a locked container of at least 12-gauge steel. Access and key controls shall be established in accordance with Chapter 2.

W. <u>Training</u>.

1. The effectiveness of security and police forces is influenced by the quality of its training program. Effective training depends on leadership, proper organization and efficient use of resources. Minimum training standards are essential to enable security and police force personnel to perform their duties in a professional manner.

2. The extent and type of training will vary, depending on the importance, vulnerability, size and other factors affecting a particular unit. Each member must complete a basic course of instruction and receive periodic training thereafter. Commanding officers shall establish the required training needed; however, a formal course of training is strongly recommended. One of the following federal government agencies may be used to achieve the basic course of instruction; quotas shall be obtained by Commandant (G-CFI):

   a. Police Training, Federal Law Enforcement Training Center, Glynco, GA.

   b. Military Police School, Ft. McClellan, AL.

   c. Navy Security Guard Course, Lackland AFB, San Antonio, TX.

   NOTE: Afloat units are not required to meet this training requirement due to limited resources and the burden of deployment schedules. However, if scheduling permits, it is highly suggested that they send key security personnel to training.

3. Exhibit 10-2 provides suggested periodic ”in service” training.

X. Equipment.

1. General.

   a. The types and quantities of equipment should be based on available resources, the mission being performed, and other unique situational requirements such as the assets being protected, local threat, etc.

   b. Specialized equipment should enhance the efficiency of security and police forces. Items in this category include, but are not limited to, warning lights, sirens, portable lights, night vision devices, flashlights, portable radios, first aid kits, traffic control devices and special clothing for health, comfort, or safety of security and police personnel.

   c. All security and police force individual equipment (rain slickers, cold weather reefers, wind breakers, radios, riot control gear, helmets, handcuffs, flashlights, etc.) other than clothing and footwear, should comply with the same standards as other federal and civilian security and police agencies.

2. Carrying of Equipment. There shall be no specific order of carrying or placing equipment on law enforcement or security belts, with the exception that the sidearm shall be placed on the strong side of the individual. Personnel shall be free to arrange equipment in whatever order of placement that they find appropriate

and convenient. The law enforcement belt, associated holster and storage pouches should be made of either black ballistic nylon material or black leather. The carrying of additional items of equipment on the law enforcement belt that are found convenient by security/police personnel, such as folding knives, key holders, etc., is authorized with command approval. The carriage of a straight-bladed (non-folding) knife is specifically not authorized. To the extent possible, the color, finish, and material of such items should match that of the law enforcement belt and associated holster.

3. Handcuffs. No specific type or manufacturer of handcuffs is required. Commands may procure and use any type of non-hinged (e.g., chain linked) handcuffs, with whatever nickel, blued or stainless steel finish, they determine useful and appropriate. For ease of operation, all types of handcuffs used by a unit should utilize the same type of key. The use of flexible handcuffs and similar devices for the temporary restraint of individuals is also authorized. All members of an authorized police force shall carry at least one pair of handcuffs.

4. Flashlights. All police force personnel should carry a flashlight, no larger than the three C-cell size, on the belt while conducting law enforcement operations. It is recommended that the flashlight have a minimum of 12,000 candlepower. When there is a need for a more powerful source of illumination, commands may procure and use lights possessing whatever illumination characteristics and other features they deem desirable. Flashlights are not intended for use as an impact weapon.

5. Holsters. The holster worn to carry the M9 personal defense weapon (PDW) shall be of the same material as the belt. It must be of the “standard ride”, “thumb break” type. “Standard ride” is defined as any belt mounted holster that when properly fastened to the belt and with the M9 PDW snapped in position, the PDW’s grip is no lower than 4 inches below the belt. “Thumb break” is defined as a holster with a retaining strap that passes over the back of the de-cocked PDW’s hammer and has a metal snap that requires thumb pressure towards the body to release the strap. It is recommended that a “high level of retention” style of holster be obtained for security and police forces with single officer response. Shoulder, leg, or thigh strapped type holsters are not authorized. Units shall procure and issue only one type of holster for wear. If the style of holster requires any action to remove the PDW other than a straight upward pull by the operator, then the unit will be responsible to provide training for personnel on the holster being used by the unit, and to ensure range training is conducted utilizing the holster carried by the unit.

Y. Weapons.

1. General.

a. Each commanding officer must undertake to conduct a comprehensive and continuous evaluation of their individual unit's threat environment and then to arm their security forces accordingly. The commanding officer's determination of the correct posture for their command shall be reflected in the unit's Standard Operating Procedures/Standing Orders/Post Orders and must be specific

b. While in the performance of official duties, military personnel may carry weapons, including concealed weapons, when expressly authorized to do so by appropriate authority, regardless of state or local laws. The inherent authority of the Coast Guard as to its military and law enforcement status has long been recognized by case law.

c. General Service police (GS-083) and security (GS-085) personnel may also be authorized to carry weapons in the performance of official duties. Personnel may have to obtain designation by the U.S. Marshals Service prior to use. If U.S. Marshal authority is limited, civilian personnel should apply to appropriate local civilian authorities for a permit to carry weapons.

d. All security and police personnel who carry and use weapons shall comply with current qualification standards as outlined in COMDTINST M8370.11 (series), Small Arms Manual.

2. Reporting Requirements.

a. Required Reports - Weapons Drawn or Used. Personal Injury. Property Damage, or Other Significant Use of Force Incident. Every law enforcement instance in which a weapon is drawn or used, personal injury or property damage results, or any other significant event occurs is a valuable learning opportunity for the entire service. However, it may also require an investigation and/or appropriate follow-up action. Accordingly, any of the following situations will warrant submission of a detailed letter report within 30 days, via the chain of command, to COMDT (G-CFI), with a copy to the cognizant Security Manager:

(1) whenever a firearm is drawn or discharged;

(2) whenever any other type of weapon is used (e.g., chemical irritants, expandable baton, etc.);

(3) whenever any other use of force involving physical contact is employed;

(4) whenever any law enforcement activity results in injury to USCG personnel or other persons, or significant property damage; or

(5) whenever any other incident involving the use or potential use of force is deemed noteworthy by the CO/CP.

b. The report should be short but thorough and include a summary of the facts, opinions, recommendations, and lessons learned. The Administrative Investigations Manual, COMDTINST M5830.l (series), and the Claims and Litigation Manual, COMDTINST M5890.9 (series), shall guide the preparation of these reports.

NOTE: (1) Separate reporting mechanisms exist and take precedence for incidents related to firearms training and accidental discharges (e.g., Ordnance Manua, COMDTINST M8000.2 (series)). (2) Special Agents are to comply with the USCG Investigations Manual, COMDTINST M5527.1 (series).

c. In the case of accidental discharge, a mishap report (MISREP) shall be completed in accordance with Safety and Environmental Health Manual, COMDTINST M5100.47 (series).

d. Policy Review. One of the primary purposes of the required reports is to provide the basis for continuous program-level policy review of the USCG approach to the use of force in law enforcement. The chief focus of such efforts is to examine current guidance, evaluate the training based thereon, and assess how well they worked in actual practice. This policy review will be coordinated by COMDT (G-CFI) and include participation by other CGHQ staff elements and the various training facilities, as appropriate.

3. Carriage of Weapons by USCG Police Forces. Except as provided in this manual, all USCG Police personnel participating in law enforcement or security activities shall be armed and equipped as follows:

a. A standard service pistol with a 15-round magazine inserted, round chambered, de-cocking lever up;

b. A minimum of one additional 15-round magazine;

c. An expandable baton;

d. The currently approved chemical irritant;
e. Chain linked handcuffs;

f. Flashlight;

g. Body armor;

h. An adequate means to communicate with the command center.

4. Impact Weapons. The expandable baton is the only impact weapon authorized for use by USCG security and police force personnel. All USCG security/police force personnel should be issued, trained in, and use as their primary impact weapon, an expandable baton with a polished chrome steel shaft, having no knurling or sharp edges, and a foam non-slip grip. It shall be rigid when deployed and have a length of 21 inches. The baton shall have no spring loaded or other triggering device.

5. Chemical Irritants. The carrying of chemical irritants by personnel engaged in security operations is not required but is optional at the member's discretion with the command's approval. If the security/police officer is outfitted with a standard weapons belt, then the carriage of the currently approved chemical irritant is mandatory. Oleoresin capsicum (OC) pepper spray is the only non-lethal force option, which can be used on multiple aggressors and at a safe distance. It has been shown in the Coast Guard and other law enforcement agencies, to be a highly effective and safe tool when properly used.

a. Any chemical irritant containing the active ingredient oleoresin capsicum (OC) may be used. The use of other type chemical irritants (CN or CS type) is not authorized. The OC aerosol must contain no greater than 10% and no less than 5% oleoresin capsicum concentration, have a water based carrier, be non-flammable, non-toxic, and be straight stream delivery (not fog). If a chemical irritant is carried by individual security/police force personnel, it shall be worn on the weapons belt with the expandable baton, not in place of it.

b. The belt carried OC containers should be no less than 3 oz. (net weight), and be thumb activated with a safety mechanism. Commands desiring to equip their security/police force with chemical irritants are to ensure sufficient quantities are available, and shall maintain on file a material safety data sheet listing all ingredients for all OC products used. Any first aid administered after the use of OC products shall conform to the product manufacturer's suggestions described for the product.

c. The use of OC aerosols in confined spaces and in windy environments may pose a hazard to USCG security/police personnel equal to its effectiveness against the intended target. Prior to using chemical irritants, law enforcement personnel should assess their location, the location of other law enforcement personnel, and the wind direction if in an open area. The use of OC shall be considered a level four use of force as described in Law

Enforcement Reference Manual, COMDTINST M16247.2. Chemical irritants should never be relied upon as an alternative to adequate training in the proper use of the non-deadly force techniques included in the USCG Use of Force Continuum.

d. USCG personnel must be qualified in the application and decontamination procedures of OC aerosol before being allowed to carry or use the product. All users of OC must receive training from a certified OC trainer. This training requires all users to experience a mandatory partial exposure to OC. This training shall be documented in the member's training record. Once the training has been successfully completed, a member does not have to recertify in the use of OC aerosol. OC trainers will be certified by a training program approved by Commandant. All personnel certified as OC trainers must experience mandatory full facial exposure to OC aerosol.

6. Standard Service Weapons. Commanding officers may decide to arm members of security and police forces based upon local needs. The standard service weapons (9mm pistol, riot shotgun, M-16 rifle) shall be carried in accordance with Small Arms Manual, COMDTINST M8370.11 (series), and the provisions of this instruction.

a. Qualification for Carriage. No security/police force personnel are authorized to carry or use a weapon unless they:

(1) have been adequately trained in the use of the weapon (proficiency and judgement) in accordance with current directives;

(2) are thoroughly familiar with the Use of Force Policy;

(3) have been determined by the unit commanding officer to possess the temperament, maturity and judgement to make reasonable and correct use of force decisions under pressure; and

(4) have been adequately trained and equipped to be able to use non-deadly force as necessary.

b. Standard Service Sidearm. The standard service pistol will be carried on the strong arm side of the weapons belt with a 15-round magazine inserted, round chambered, hammer forward, and de-cocking lever up. A minimum of one additional 15-round magazine will be carried on the weapons belt.

c. Shotguns. When there is an articulable reason to suspect that there is an increased threat to security/police force personnel safety, they may employ the use of a riot shotgun and the equipment necessary to support its use.

(1) Currently there is no USCG training for sidearm retention when carrying a shotgun; however, all police/security personnel who may be called upon to be so armed are required to attend applicable law enforcement training. Therefore, specific security/police force training from outside agencies should be arranged and authorized through Commandant (G-CFI).

(2) The shotgun will be loaded with four rounds of ammunition, with no rounds chambered. Extra rounds will be carried.

(3) Authorized shotguns when carried in a vehicle must be secured in an approved locking shotgun mount or secured in the trunk of the vehicle.

d. M-16 and Other Shoulder Fired Weapons. Security/police force personnel are not authorized to carry the M-16 or other shoulder fired weapons during normal law enforcement operations. These may be readily available, but not displayed, for immediate employment upon specific approval of the unit commanding officer.

7. All of the above weapons and equipment are to be carried and used in accordance with standard directives.

NOTE: The carrying of unloaded weapons by on-duty security/police personnel is prohibited, except for safety reasons while on the firing range or while participating in training exercises.

Z. Use of Force. This section prescribes a uniform use of force and weapons policy for the Coast Guard security and police forces. A more comprehensive Use of Force policy for Coast Guard security and police forces is included as Enclosure 6 to this manual.

1. There are varying degrees of force that may be justified in a law enforcement situation depending upon the gravity of the situation. However, the escalation of force by an officer must be consistent with the need for the lowest level of force required to effect the apprehension of a suspect or stop the particular criminal conduct.

2. In an enforcement situation, officers may use only that level of force necessary to control and terminate unlawful resistance, and to preclude any further physical confrontation against law enforcement personnel or other persons.

3. Besides self-defense, the use of this policy may arise in three USCG roles:

a. as a law enforcement agency;

b. as the custodian responsible for the security of government property; and

c. during peacetime as a branch of the armed forces, except when otherwise directed.

4. These roles may overlap in any given situation. Use of force is a sensitive issue and, like the exercise of any law enforcement authority, should be undertaken with caution and circumspection. This should not be construed as limiting the taking of quick action or using such force as is necessary to defend or protect one's self or others. Reckless, careless, or unnecessary use of force is never permitted. Exhibit 10-3 is a use of deadly force summary.

5. Whenever law enforcement personnel, while in the performance of official duties, inflict or are involved in an incident where death or serious bodily injury is inflicted upon another person as a result of some type of enforcement activity, they shall immediately notify the CSO/CP, who shall then notify the local CGIS Resident Agent's Office. Floating units shall notify their operational commander in lieu of CGIS.

6. The CSO/CP shall conduct an investigation into any report of weapons discharge (either accidentally or officially) and a detailed offense/incident report shall be prepared for review by the commanding officer. The CSO/CP shall then notify the local CGIS Resident Agent's Office. Floating units shall notify their operational commander and CGIS.

AA. Searches of Persons.

1. General.

a. This section provides policy guidance and procedures for conducting searches of persons while carrying out law enforcement operations. Such searches – including frisks, searches incident to arrest, strip searches and body cavity searches – are conducted for the protection of personnel, crime scene security, and the preservation or destruction of contraband or other evidence.

b. Body searches should be conducted in a manner to ensure that the dignity of the individual being searched is respected and should be conducted with the utmost tact. The search should be conducted in a professional manner and without comments about appearance, clothing, or character.

c. Except as provided in subparagraph 10.AA.4 of this section, body searches are to be conducted by a member of the same sex as the person being searched. However, primary concern is for the safety of USCG personnel.

The unavailability of a member of the same sex as the person being searched shall not deter an otherwise lawful body search.

d. Any article seized during a body search must be properly treated as evidence. Property not seized, but detained, should be safeguarded and properly inventoried during the course of the search.

e. Force may be used to compel compliance with the orders necessary to conduct a body search. The force used shall be the minimum reasonably necessary to achieve compliance. Absent circumstances requiring immediate compliance, the individual being searched should be given notice of the consequences for failure to comply, and a reasonable time for compliance.

NOTE: As per the section and enclosure on Use of Force, any use of force involving physical contact, will be the subject of a letter report within 30 days, forwarded via the chain of command and cognizant SECMGR to COMDT (G-CFI)

f. Searches are divided into two categories; those prior to and those subsequent to arrest. Pre-arrest searches are authorized for limited purposes requiring specific levels of suspicion. Searches subsequent to arrest are commonly referred to as field searches or searches incident to arrest. These are conducted for the purpose of discovering weapons, evidence, and means of escape.

2. Pre-Arrest Body Searches.

a. Frisk. A frisk search is the crushing and passing of hands over the outer clothing of a person, in search of weapons when an officer suspects that an individual may have a weapon and that either the officer or others may be endangered.

(1) When to conduct. Frisk searches are authorized for the purpose of the protection of the law enforcement officer. A person who is not under arrest may be frisked when reasonable suspicion exists that the individual may have a weapon secreted on their person, which could endanger the officer or others.

NOTE: A person under arrest may be frisked, however, a field search would be more appropriate for this circumstance.

(2) Scope. A frisk is done by firmly crushing and passing the hands over the subject's clothed body. The person may be requested to

remove an overcoat and similar outer garments to facilitate the search.

(3) Direct touching of the genitals or female breasts is to be avoided. Contact with such areas, which a reasonable person would find offensive, and might construe as fondling or caressing, is prohibited.

(4) The scope of a frisk may be extended to the "grab area" of an individual reasonably suspected to have a weapon (e.g., if someone is carrying a purse or bag and a weapon is suspected, the purse or bag may be searched to the extent necessary to rule out the existence of a weapon if the purse or bag is within the "grab area" of that person).

(5) Only weapons or items that could reasonably be construed as weapons may be confiscated during a frisk. If, in the course of a frisk, evidence of a violation of law, over which the officer has jurisdictional authority, is discovered and probable cause exists, that evidence may be seized and an arrest may be made.

b. Other Body Searches. Other searches more intrusive than frisk searches are authorized prior to arrest for the discovery of evidence of a crime. A person who is not under arrest may be searched if there is probable cause that the evidence of crime is secreted on the person to be searched. If possible, such searches should be delayed until after the person is arrested when, usually, a lesser degree of suspicion is required.

c. Persons Not Arrested, but Detained Onboard USCG Units. Individuals involuntarily detained on board USCG units for transfer or transport for other law enforcement agencies may be searched. This search is conducted to find weapons and/or means of escape.

(1) When to conduct. This search should be conducted as soon as practicable after the detainee is placed aboard the USCG unit. This search may be repeated when the detainee is transferred to another law enforcement agency.

(2) Scope. This search is done like the frisk search outlined above.

(3) This search may also be extended to the "grab area" of the individual being searched.

3. Post Arrest Body Search.

a. Field Search/Search Incident to Arrest. A field search is a detailed crush and feel search of an arrested individual's person and thorough search of outer clothing for weapons, evidence, or means of escape. Often referred to as a search incident to arrest, this type of search, while not a strip search, is more intrusive than a frisk search and is normally conducted at the point of arrest. Afield search will normally be distinguished from a strip search when removal of a layer of clothing will expose the undergarments (more than mere elastic waist bands, or back and arm straps) which cover male and female genitalia and female breasts. No suspicion or probable cause is required for the field search itself (although the underlying arrest must be lawful). Any weapon, item that might be used as a weapon, means of escape, contraband, or evidence should be seized. Items of value should be taken and safeguarded.

(1) When to conduct. A field search should be conducted as soon as practical after an arrest has been made. If circumstances permit, the field search should be conducted at the scene where the individual was arrested, immediately following the arrest. If circumstances do not allow the search to be conducted at the arrest scene, the search should be conducted as soon as practicable. A field search should be repeated after custody of an arrestee has been transferred from one law enforcement entity to another.

(2) Scope. This is a very thorough search of a person and their clothing. Outer garments, jackets, gloves, shoes, etc. may be removed and thoroughly inspected. Clothing which is not removed may be thoroughly searched by firmly pressing, with the flattened hand, along the body, arms, and legs. Search collars, waistlines, and seams of clothing by carefully turning them down a little at a time as you search. Turn all pockets inside out by pulling the pocket up a little at a time with the thumb and first finger. If the pocket will not turn inside out, search the pockets very carefully with two fingers.

(a) The mouth of the person being searched may be visually inspected as a part of a field search.

(b) To facilitate the search of the underarm and back of a female arrestee, she may be instructed to release the back clasp of her bra. This may be done even as the officer maintains control of the subject. If the bra has clasps in the front or no clasps at all, the bra would normally be left in place.

(c) There should be no direct (i.e., hands on) search of the female breast area, or groin area of either sex, unless:

(i) there is a reasonable suspicion that a weapon, contraband, or evidence which can be easily reached, is there; and

(ii) the possibility exists the arrestee may have to be released from direct control (i.e., an officer's hand on the suspect for control), before they can be searched by either medical personnel or a person of the same sex.

(d) The scope of a field search may also be extended to the area where an individual is arrested and the area where the individual is to be placed after arrest.

b. Strip Search. A strip search involves the intrusive removal of clothing and may be as extensive as visual examination of the nude body. As a rule of thumb, if there is reasonable likelihood that a search involving the removal of clothing would be offensive or cause embarrassment to the average person, then it should be considered a strip search.

(1) When to conduct. A strip search can be conducted when there is a reasonable suspicion that a weapon, evidence, or means of escape is secreted on a person. This suspicion may exist following a field search. An arrest standing alone does not necessarily justify a strip search; there must be a reasonable suspicion that the items sought are on the arrestee's person.

(2) Scope. A strip search will be conducted in a location free from outside observation, except for the personnel necessary to conduct the search.

(a) Strip searches should be conducted with a witness present. The witness should be of the same sex as the person being searched. If no witness of the same sex is available, then the witness should remain immediately outside the search location, but within hearing distance to closely monitor the progress of the search. Videotaping of strip searches is specifically prohibited.

(b) Most, if not all, clothing should be removed from the subject while they remain handcuffed. The handcuffs should be removed only when absolutely necessary and should be put back on as soon as practical.

(c) The removal of clothing exposing buttocks, genitalia, and/or female breasts is authorized when necessary to resolve specific suspicions related to those areas. Persons being searched should be requested to manipulate their own bodies as required to permit adequate visual examinations.

(d) Each item of clothing should be thoroughly searched and the contents placed in full view of the subject. If articles are detained, the subject should be informed and provided a receipt covering each item being seized or detained. The articles, and the person from whom removed, must be able to be identified at a later time.

c. Body Cavity Search. A visual or physical intrusion into a body cavity constitutes a cavity search. A visual inspection of the mouth during either a field search or a strip search is not considered a "body cavity search."

(1) When to conduct. Body cavity examinations other than by a physician are not authorized except by a visual examination. An anal or genital body cavity may be viewed when, after a strip search, reasonable suspicion exists that a weapon, evidence, or means of escape is secreted in the specific body cavity to be examined. Viewing of the mouth, ears, and nose does not require suspicion in addition to that, which justifies the arrest.

(2) Scope. Visual body cavity searches may be conducted when the necessary, specific suspicion exists. Persons being searched should be requested to manipulate their own bodies as required to permit adequate visual examination. If the examination reveals a suspicious object, the person being searched should be requested to remove the object. If they refuse, removal by the examiner is not authorized.

(3) Physical body cavity searches are to be conducted by a licensed physician under clinical conditions. Should suspicion exist that the individual has secreted a weapon, evidence, contraband or means of escape in a body cavity, then the individual should be kept under observation. If a search is immediately necessary due to medical reasons, it must be conducted by medical personnel using standard medical procedures.

4. Search by Members of the Opposite Sex.

a. When members of the same sex are unavailable, these additional procedures are applicable:

(1) Frisk searches and field searches may be conducted without making contact with or exposure of genitalia or female breasts.

(2) If a frisk, or field search requiring contact with genitalia or breasts, or a strip search is necessary, then the unit must document in the evidence package (regardless of any evidence found as a result of the search):

(a) reasonable suspicion justifying the search;

(b) the unavailability of trained members of the same sex to conduct the search; and

(c) the reason that other alternatives to conducting the search were unavailable to protect the government's interest in preserving evidence or the unit's security.

BB. Patrol Vehicle Standards.

1. Federal, state and local law enforcement agencies throughout the U.S. routinely use sedans equipped with heavy-duty components and equipment for safety and operational reasons. These sedans are designed for the special demands of the law enforcement mission. Years of testing and actual use have proven them to be safer and require less maintenance than the standard commercially procured sedan. Federal Standard 122 (as annually amended) provides specific standards for law enforcement sedans.

2. Various operational endeavors place the law enforcement vehicle and security and police personnel in a hazardous position requiring immediate identification and visibility. Therefore, these vehicles must be distinctively marked. Statistics reveal that distinctively marked law enforcement vehicles patrolling throughout a unit, including housing areas, parking lots, restricted areas and roadways, contribute significantly to reduced criminal activity.

3. Security and police forces shall be furnished with sufficient vehicles to maintain required patrol standards, response to alarms and emergencies, and to maintain effective supervision. These vehicles will be used solely by security and police personnel in the performance of official duties. Vehicles shall be:

a. Well-maintained.

b. Identified as a security or police vehicle.

c. Equipped with red, blue, amber, take down and alley emergency overhead lights (red over driver, blue over passenger and amber flashers to the rear), a rotating spotlight, electronic siren, mobile two way communications, speed detection device (radar), fire extinguishers, first aid kit and a locking shotgun mount with concealed release (where shotguns are carried). Video and audio equipment is highly recommended.

d. Equipped with additional operational lighting mounted to the grill or bumper area, if necessary. The CSO/CP may authorize certain vehicles to have lights on the inside dash and rear deck. Example of such vehicles, are unmarked vehicles used for investigations, or marked vehicles where the "police car silhouette" may be undesirable, such as traffic enforcement or radar use.

e. Equipped for transporting detainees, if no patrol wagon/van transport is available.

f. Equipped with seat and shoulder belts, which must be utilized whenever the vehicle is in motion.

g. Equipped with the following items: fire extinguishers, first aid kits, and highway warning signals, such as flares or reflective devices.

h. Equipped when necessary with approved locking shotgun mounts.

i. Sequentially numbered using the letter "P" for POLICE or "S" for SECURITY and the last three digits of the license plate. In the event the department uses scooters, the numbering system shall be "P-1", "S-2", etc.

j. Painted with the manufacturer's standard gloss white with two horizontally oriented, reflective stripes on the upper portion of the vehicle spaced one inch apart on each side and trunk of the vehicle. The top stripe shall be red, one inch wide and the bottom shall be blue, four inches wide. The word "SECURITY" or "POLICE" in four inch reflectorized white letters shall be on the top front vertical side of both front fenders placed over the blue stripe and centered on the rearward facing passenger portion of the trunk lid. The letters U.S.C.G. in four inch reflectorized white letters shall be centered on the rearward facing driver's portion of the trunk lid. The Coast Guard security or police logo (star) shall be applied to the front doors of the car. It is recommended that security or police emergency telephone numbers be placed in four inch reflectorized white letters over the blue stripe of the top rear vertical side of both rear fenders.

k. The above acquisition specifications and marking requirements also apply to Coast Guard leased vehicles.

CC. Emergency Vehicle Response.

1. Emergency vehicle response is the rapid movement of security and/or police personnel in reaction to a serious incident and shall be accomplished with the utmost caution. Emergency vehicle response generally involves the following factors:

   a. Use of flashing, rotating or steady burning warning lights on a moving security or police vehicle.

   b. Use of an audible air horn, siren on moving security or police vehicles.

   c. Operation of security or police vehicles in excess of posted speed limits.

   d. Violation of certain traffic regulations.

2. Emergency vehicle response is only necessary when there is a need to have security and police personnel at the scene of serious incident faster than one could arrive without emergency procedures and/or when it is necessary to pursue an individual suspected of violating the law.

3. The following examples are when emergency vehicle response may be authorized:

   a. Security or police personnel need assistance.

   b. When responding to a felony in progress, where the incident is serious and possibly life threatening.

   c. When responding to reports of “shots fired/person(s) with a gun/person screaming”, etc., or other calls where lives may be in danger.

   d. When responding to a scene where normal response may jeopardize investigative action.

   e. When responding to a traffic accident where injuries have been reported.

   f. When responding to fire and medical emergencies prior to the arrival of medical personnel, or when emergency response is requested by fire or medical personnel.

   g. When transporting injured personnel in the absence of medical personnel.

h. During protective service details when it is necessary to transport the protectee rapidly for his/her safety.

4. The use of an emergency vehicle to lead a non-emergency vehicle under emergency conditions is prohibited. This situation often occurs when a motorist is transporting a sick or injured person and seeks security or police assistance. Security and police personnel should call for medical assistance at the scene, transport the person in security or police vehicles, or provide non-emergency transport.

DD. Communications System.

1. A reliable communications system is essential for effective security and police forces. The system must be tailored to the requirements of security and police networks. Considerations include:

a. Flexibility.

b. Time sensitivity of information.

c. Vulnerability to interception.

d. Size of area to be covered.

e. Natural terrain obstructions.

f. Need for responsive reaction.

2. The communication system is largely subject to local determination, but essential characteristics include the following:

a. A system of radio communications netting all motor patrols, fixed posts and roving foot patrols.

b. Features such as an independent or emergency power source.

c. Capability to switch to an alternate frequency in the event the primary frequency becomes jammed or inoperable.

d. Self-contained multiple frequency capability for portable communications equipment.

e. Features such as voice encryption, scrambling and/or frequency agile radio systems.

f. Central communications and dispatch center.

3. Security and police forces shall have three dedicated frequencies (primary, tactical (used for specific operations) and a backup).

4. Security and police forces shall have continuous and reliable voice communications with local, state, county and CGIS offices during crisis situations.

5. A daily test of all communication circuits shall be conducted to ensure they are operating properly and a record/log maintained.

6. Quarterly inspections of all communication equipment shall be conducted by qualified electronics personnel under simulated emergency conditions and a record/log maintained.

EE. Evidence Procedures.

1. It is the responsibility of all security and law enforcement personnel to take every precaution to preserve the integrity of evidence in its original condition. This means that investigative personnel must enter evidence into the custodial system as soon as possible after its collection, seizure, or surrender.

2. Security and police forces shall establish a custodial system consisting of the following:

a. Evidence custodian (to be designated in writing).

b. Alternate evidence custodian (to be designated in writing).

c. Evidence locker (container, room, etc.).

d. Evidence log.

e. Active evidence custody record or file.

f. Final evidence disposition record or file.

3. The evidence custodian or alternate has responsibilities which cannot be further delegated to ensure the following:

a. Evidence is properly inventoried, tagged, packaged, and marked prior to acceptance for storage.

b. Evidence custody documents are properly completed by the one delivering the evidence for safekeeping, prior to acceptance for storage.

c. Evidence is properly safeguarded.

d. The evidence log, active evidence custody record and final evidence disposition records are properly maintained.

e. Inventories of evidence holdings are conducted as required by the CSO/CP.

f. Under the supervision of the CSO/CP, evidence is properly disposed of and recorded.

4. Any of a variety of configurations may be used to physically safeguard evidence in an "evidence locker". Depending on the needs of the unit, the evidence locker may be a field safe, security filing cabinet/container, or closet. Where large volumes of evidence are handled, the evidence locker may be a separate room.

a. When a closet or room is used for evidence, it shall be equipped with shelves, storage bins, lockers, storage cabinets, or other suitable means for storing a volume of evidence in an orderly and accessible manner.

b. Shelves, bins, lockers etc., shall be marked in a manner that facilitates the location of particular items of evidence.

5. Access to the evidence locker shall be strictly limited to the designated evidence custodian or alternate and the CSO/CP. In the event that the alternate custodian is not the CSO/CP, the CSO/CP shall be provided the combinations or keys in a sealed envelope. Under no circumstances shall personnel other than the above be granted unescorted access to the evidence locker.

FF. Security/Police Force Records Management.

1. General. The Federal Records Act of 1950 requires that adequate controls over the creation of records be provided. Records documenting the organization, functions, policies, decisions, procedures and essential transactions of the Coast Guard security and police forces must be preserved to furnish information necessary to protect the legal and financial rights of the Coast Guard and persons affected by the activities of the Coast Guard. Correspondence, reports, forms, machine readable records with their supporting documentation, and directives are the principal types of records created. Programs, policies and procedures shall be adequately documented in directives and record copies of each directive (including those superseded) shall be maintained as part of the official files in accordance with the Coast Guard Directives System COMDTINST M5215.6.

2. Purpose. The following information gives amplifying guidance on the retention and disposition of some of the records relating to the measures taken for the

protection of Coast Guard owned facilities and privately operated facilities given security cognizance by Coast Guard security/police forces. The reports, forms, files, notices, records and other miscellaneous documents used by Coast Guard security/police or other protective forces to document enforcement actions and support program administration shall be maintained, stored and transferred for archiving in accordance with current paperwork management directives.

3. Retention Requirements/Limitations. Security and protective services records include the various files created by agencies to control and protect classified information; to protect Government facilities from unauthorized entry, sabotage, or loss; to ensure the adequacy of protective measures at privately-owned plants given security cognizance by the Government; and to develop and implement plans for the protection of life and property under emergency conditions. Included are files of offices having Government-wide or agency-wide responsibilities for security and protective services programs. Also included are files of security units, guard forces, and other organizational elements documenting the control of classified information, access to facilities, and like matters. Whenever information is not under the control of an authorized individual, it shall be stored under secure conditions such as a locked room, locked file cabinet, or locked desk.

a. These records should be maintained by the initiating security/police department for the periods specified:

(1) Law Enforcement Agreements. Coast Guard and State Law Enforcement Agreements such as Memorandums of Understanding (MOU) with local police departments; retain for 3 years after superseded or obsolete.

(2) Minor Traffic Accident Report case files. Incidents that involve no significant injury to personnel and only minor damage to property; retain for 1 year after final action.

(3) Major Traffic Accident Investigation/Report case files. Copies of traffic casualty case files including the record of proceedings and the investigative reports of Accident Boards of investigation, investigations of casualties involving death, investigations of traffic casualties and investigations of cases involving injuries; Retain for 5 years after case is closed.

(4) Parking Permit Controls. Information on the allotment of parking spaces, control of issuance and withdrawal of parking permits, and the recording of violations by holders of parking permits; Retain until transfer or separation of parking permit holder or when permit is superseded or revoked, whichever is first.

(5) Hearing records and associated unit case files. Retain for 5 years after final administrative action.

(6) Report of Violation, law and regulation violation cases and associated documents . Retain for 3 years after report is forwarded to hearing authority.

(7) Miscellaneous records. Routine administrative records of temporary value not provided for elsewhere; Retain for 2 years.

(8) Law enforcement case files. Includes cases referred to other agencies or departments for action consisting of investigation reports, violation reports, correspondence, and related documents; Retain for 1 year after final disposition of the case.

(9) Security and Protective Services Administrative Correspondence Files. Correspondence files relating to administration and operation of the facilities security and protective services programs, not specifically covered elsewhere; retain for 2 years.

(10) Survey and Inspection Files (Government-owned facilities). Reports of surveys and inspections of Government-owned facilities conducted to ensure adequacy of protective and preventive measures taken against hazards of fire, explosion, and accidents, and to safeguard information and facilities against sabotage and unauthorized entry; Retain for 3 years, until completion of the next survey of the same facility, or until discontinuance of facility, whichever is sooner.

(11) Survey and Inspection Files (leased facilities). Reports of surveys and inspections of privately owned/leased facilities assigned security cognizance by Government agencies, and related papers; Retain for 4 years or until security cognizance is terminated, whichever is sooner.

(12) Non-criminal Investigative Files. Investigative files accumulating from investigations of fires, explosions, and accidents, consisting of retained copies of reports and related papers when the original reports are submitted for review and filing in other agencies or organizational elements, and reports and related papers concerning occurrences of such a minor nature that they are settled locally without referral to other organizational elements; Retain for 2 years.

(13) Guard Assignment Files. Files relating to guard assignments and strength:

(a) Ledger records; Retain for 3 years after final entry.

(b) Requests, analyses, reports change notices, and other papers relating to post assignments and strength requirements; retain for 2 years.

(14) Police Functions Files. Files relating to exercise of police functions:

(a) Ledger records of arrest, cars ticketed, and outside police contacts; retain for 3 years after final entry.

(b) Reports about routine complaints, statements of witnesses, warning notices, and other case papers relating to arrest, commitments, and traffic violations (excluding criminal investigation reports); Retain for 2 years.

(c) Reports on contact of outside police with building occupants; Retain for 1 year.

(d) Police Journals. Information containing a chronological record of police activity developed from reports, complaints, incidents, information received and action taken, record of police radio traffic, desk blotters and police radio logs; Retain for 3 years.

(e) Criminal Investigation Files. Information compiled in support of case files, consisting of retained copies of reports and related papers when the original reports are forwarded to Coast Guard Investigative Service or other investigative agencies; Retain for 1 year after final disposition of the case.

(f) General Criminal Investigation Correspondence Files. Information relating to criminal investigation that are received for information only, on which no action is required. These include cards, listings, indexes, or other items which are created solely to facilitate or control work, extra copies of actions maintained by action officers, duplicate copies of actions accumulated by supervisory offices, and notes, drafts, feeder reports, and similar working information gathered for preparation of an action; Retain for 1 year after final disposition of the case.

(15) Police Property Files. Files relating to the receipt and release of property that is found, impounded, seized as contraband, prohibited, or safeguarded for detained personnel. This includes logs, receipts and releases, and related information; Retain for 5 years after return or release of property.

(16) Property Pass Files. Property pass files, authorizing removal of property or materials; Retain for 3 months after expiration or revocation.

(17) Personal Property Accountability Files. Files relating to accountability for personal property lost or stolen:

(a) Ledger files; Retain for 3 years after final entry.

(b) Reports, loss statements, receipts and other papers relating to lost and found articles; retain for 1 year.

(18) Key Accountability Files. Files relating to accountability for keys issued:

(a) For areas under maximum security; retain for 3 years after turn-in of key.

(b) For other areas; retain for 6 months after turn-in of key.

(19) Visitor Control Files. Registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers:

(a) For areas under maximum security; retain for 5 years after final entry or 5 years after date of document, as appropriate.

(b) For other areas; retain for 2 years after final entry or 2 years after date of document, as appropriate.

(20) Prisoner or Detained Person Receipts. Information showing the receipt of prisoners or detained persons; Retain for 3 years.

(21) Facilities Checks Files. Files relating to periodic guard force facility checks:

(a) Data sheets, door slip summaries, check sheets, and guard reports on security violations (except copies in files of agency security offices covered by regulations for the

safeguarding of national security information); Retain for 1 year.

(b) Reports of routine after-hours security checks which either do not reflect security violations, or for which the information contained therein is documented in the files covered by regulations for the safeguarding of national security information; Retain for 1 month.

(22) Guard Service Control Files.

(a) Control center key or code records, emergency call cards and building record and employee identification cards; Retain until superseded or obsolete.

(b) Round reports, service reports on interruptions and tests, and punch clock dial sheets; retain for 1 year.

(c) Automatic machine patrol charts and registers of patrol and alarm services; Retain for 1 year.

(d) Arms distribution sheets, charge records, and receipts; Retain for 6 months after return of arms.

(23) Logs and Registers. Guard logs and registers not covered elsewhere in this schedule:

(a) Central guard office master logs; Retain for 2 years after final entry.

(b) Individual guard post logs of occurrences entered in master logs; Retain for 1 year after final entry.

b. Extended Records Retention. Retention beyond the specified periods may be authorized by the CSO/CP on a case by case basis. Any retention beyond the specified limitations must contain a written explanation for the retention and be signed by the authorizing CSO/CP.

EXHIBIT 10-1

SECURITY BADGE AND PATCH DESIGN SPECIFICATIONS

KEY:

1. NAVY BLUE BACKGROUND
2. YELLOW BOARDER
3. YELLOW LETTERING
4. GOLD BADGE
5. ROYAL BLUE LETTERING
6. NAVY BLUE BACKGROUND
7. YELLOW LETTERING
8. RED, WHITE, AND ROYAL BLUE "CREST"
9. LIGHT BLUE BACKGROUND
10. ROYAL BLUE INNER CIRCLE WITH STARS

<u>NOTE</u>: ON BADGE, INSERT APPROPRIATE COMMAND NAME FOR "UNIT" AND SUBSTITUTE "SECURITY" FOR "POLICE" AS APPROPRIATE.

SIZE: PATCH - APPX. 3.5" x 4.5"; BADGE – APPX. 2.25" x 2.5" (2.5" TIP-TO-TIP)

EXHIBIT 10-2

SECURITY AND POLICE FORCE TRAINING

A. ADMINISTRATIVE
1. Area Overview/Orientation
2. Security and Police Force Duties
3. Standards of Conduct
4. Forms/Record Keeping/Report Writing

B. PHYSICAL SECURITY/LOSS PREVENTION
1. Vehicle & Personnel Movement Control
2. Crime Prevention
3. Restricted Areas
4. Perimeter Security
5. Intrusion Detection Systems
6. AA&E Storage Areas

C. LEGAL
1. Law and the UCMJ
2. Jurisdiction
3. Authority
4. Rules of Evidence
5. Search and Seizure
6. Apprehension and Arrest
7. Courtroom Testimony/Procedures

D. TRAFFIC LAWS AND ENFORCEMENT
1. Traffic Control
2. Speed Control Devices (RADAR)
3. Accident Investigation
4. Driving Under the Influence
5. Driving While Intoxicated
6. Alcohol and Drug Testing Procedure

E. PATROL
1. Crime Scenes
2. Preservation of Evidence
3. Crimes in Progress
4. Domestic Situations
5. Juvenile Offenses
6. Communications
7. Searches (Vehicle & Persons)
8. Drugs of Abuse Identification, Prevention & Control
9. Unarmed Self-Defense
10. Observation Skills
11. Interview/Interrogation Techniques
12. Human & Public Relations

EXHIBIT 10-2

SECURITY AND POLICE FORCE TRAINING

F. PROFESSIONAL SKILLS
1. Weapons Proficiency Training
2. Use of Force
3. Defense Tactics
4. Crime Computers (NCIC, EPIC, etc.)

G. UNUSUAL INCIDENTS
1. Crowd Control
2. Terrorist Activity
3. Hostage Negotiation
4. Threat Condition Levels
5. Bomb Threats/Searches
6. First Aid/CPR
7. Disaster & Emergency Plans

EXHIBIT 10-3

SECURITY AND POLICE FORCE USE OF DEADLY FORCE SUMMARY

For the following situation:[1]		Deadly force may be used if:
Self-Defense/Defense of Others		There is a reasonable belief of an imminent threat of death or serious bodily injury.
Prevention of a Crime		The felony, if not prevented, would pose an imminent threat of death or serious bodily injury.
Effecting an Arrest or Preventing an Escape[2]	*	There is probable cause that the suspect has committed a federal[3] crime involving the use of or threatened use of deadly force; and
	*	the suspect is armed or otherwise still poses a substantial threat of death or serious bodily injury; and
	*	the suspect has failed to obey an order to halt; and
	*	the use of force does not create an undue risk to any persons, other than the suspect.
Protection of Property		Normally never.[4]

Notes:

1. In any case, deadly force may only be used after USCG personnel:
   a. identify themselves as law enforcement officers (if feasible);
   b. issue an order to cease the dangerous activity (if feasible); and
   c. determine that, in view of the threat, the use of deadly force does not create an undue risk to others.
2. Disabling fire is a special method of effecting an arrest or preventing an escape of a vessel. It is not intended to be used as deadly force.
3. USCG commissioned, warrant, and petty officers normally have arrest authority only for federal crimes. The limitation to federal crimes does not apply if the USCG member has additional authority to arrest for the particular crime, such as by authorization of a flag State.
4. Deadly force may be used only when the specific property (including information) has been designated by COMDT as either (a) vital to the national security or (b) inherently dangerous to others.

Chapter 11 STORAGE OF CONTROLLED MEDICAL SUBSTANCES

A. Purpose. This chapter establishes standards for the storage of controlled medical substances and medically sensitive items as outlined in Medical Manual, COMDTINST M6000.1 (series).

1. Controlled medical substance storage and handling areas should be designated as restricted areas in accordance with Chapter 2 of this manual.

   NOTE: The mere existence of a container does not automatically require the location it is in to be a restricted area. For example, a room with a container that only stores controlled medical substances may not need restricted area controls, whereas a room with a container and where pharmacy transactions and controlled medical substance handling regularly occur would require restricted area controls. Areas where transactions only occur on an occasional basis would require the extra controls only during the transactions or handling and not at other times. Cognizant Security Managers should be consulted and compensatory measures established for proper control during all levels of activity.

2. Safeguarding measures include, but are not limited to the following:

   a. Ensuring that security responsibilities are assigned for the receipt, storage, issue, transportation, use, disposal, turn-in and accounting for all controlled medical substances.

   b. Providing specific instructions to individuals who are in the possession and control of, or who are responsible for, controlled medical substances.

   c. Ensuring the careful selection of personnel who are assigned duties that require access to controlled medical substances and sensitive item(s) storage areas or who have custodianship or possession of keys and combinations to locks used to secure these areas.

B. Storage Container Requirements.

1. The use of General Services Administration (GSA) approved security containers for all controlled medical substances is encouraged. However, there may be circumstances when it is not possible, e.g., due to cost and/or weight constraints. Your cognizant Security Manager should be consulted before making decisions affecting unit security.

2. For ashore units, bulk stocks (as defined in Medical Manual, COMDINST M6000.1 (Series)) of controlled medical substances shall be stored in a Class-5 GSA approved container.

3. For mobile units, bulk stock of controlled medical substances should be stored in a Class-5 GSA approved container; however, existing "built in," permanently mounted containers may be used.

4. Controlled medical substances shall not be stored with Arms, Ammunition and Explosives (AA&E), classified material, or funds and related instruments.

5. Containers shall be located inside a locked room where reasonable security measures can be effectively implemented.

6. Any container on casters or one that weighs less than 500 pounds shall be permanently secured to the premises unless it is protected by an IDS or located within a vault. It may be secured by bolts or heavy metal straps or, if it is intended to remain part of the structure, it may be secured by imbedding it in concrete.

7. Form SF 702, Security Container Check Sheet, shall be used to record the opening/closing of a container. Records shall be maintained for 3 months.

8. Form SF 701, Activity Security Checklist, shall be used to record area security checks at the close of each duty day. Records shall be maintained for 3 months.

Chapter 12 BOMB THREATS AND INCIDENTS

A. Purpose. Bomb threat planning is an important facet of any Physical Security Program. This chapter provides guidance in planning for and responding to bomb threats.

B. General. Bomb threats can be expected in the form of a telephone message, written message or suspicious package received through the mail, or found at the unit. A telephone or written bomb threat may or may not specify the location of the bomb, include the time for detonation/ignition, or contain an ultimatum related to the detonation/ignition or concealment of the bomb. Although most bomb threats are a hoax, each shall be treated seriously and action taken immediately to prevent personal injury.

C. Bomb Threats and Physical Security Planning. Bombing and the threat of being bombed are harsh realities in today's world. If there is one point that cannot be overemphasized, it is the value of being prepared. Do not allow a bomb incident to catch you by surprise. By developing a bomb incident plan and considering possible bomb incidents in your physical security plan, you can reduce the potential for personal injury and property damage.

1. Bombs

a. 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.

b. 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.

2. Bomb threats

a. 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.

b. 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.

c. Telephonic Bomb Threat. If a bomb threat is received by telephone, attempt to obtain as much information as possible to aid in locating the bomb and later investigating to determine culpability. Exhibit 12-1, Telephonic Bomb Threat Report, may be used to record and report such threatening calls. Periodically review the information in paragraph 12.D. "Responding to Telephonic Bomb Threats" as part of command training.

d. Written Bomb Threat. 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. 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.

e. Letter/Package Bombs. The construction and components of a letter or package bomb are limited only by the imagination of the bomber and the requirements of the postal process. Essential to the isolation of suspicious letters and packages is an awareness, by all personnel, of the normal types of items generally received by the unit. Exhibit 12-2 provides several peculiarities that may indicate a hazardous object. The information in this listing shall be placed in all mailrooms.

3. Why Prepare

a. 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.

b. Through proper preparation, you can reduce the accessibility of your command 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.

c. 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.

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

4. How to Prepare

a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

f. Contact your cognizant security manager 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.

g. 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 very important to organize and train an evacuation unit which will be responsive to the command center and has a clear understanding of the importance of its role.

h. It is critical that lines of communication be established between the command center and the search or evacuation teams. The center must have the flexibility to keep up with the search team progress. In a large facility, if the teams go beyond the communications network, the command center must have the mobility to maintain contact and track search or evacuation efforts.

5. Security Against Bomb Incidents

a. In dealing with bomb incidents or potential bomb incidents, two interrelated plans must be developed, the bomb incident plan and the physical security plan. Heretofore, we have primarily addressed the bomb incident plan. Now, before continuing with that plan, we will discuss security measures as they apply to "hardening" against the bomb attack.

b. Most commercial structures and individual residences already have some security in place, planned or unplanned, realized or not. Locks on windows and doors, outside lights, etc., are all designed and installed to contribute toward the security of a facility and the protection of its occupants.

c. In considering measures to increase security for your building or office, it is highly recommended that you contact your cognizant security manager for

guidance regarding a specific plan for your facility. There is no single security plan that is adaptable to all situations. The following are recommendations to be considered and are offered because they may contribute to reducing your vulnerability to bomb attacks.

(1) The exterior configuration of a building or facility is very important. Unfortunately, in most instances, the architect has given little or no consideration to security, particularly toward thwarting or discouraging a bomb attack.

(2) However, by the addition of fencing and lighting, and by controlling access, the vulnerability of a facility to a bomb attack can be reduced significantly.

(3) Bombs being delivered by car or left in a car are a grave reality. Parking should be restricted, if possible, to 300 feet from your building or any building in a complex. If restricted parking is not feasible, properly identified employee vehicles should be parked closest to your facility and visitor vehicles parked at a distance.

(4) Heavy shrubs and vines should be kept close to the ground to reduce their potential to conceal criminals or bombs. Window boxes and planters are perfect receptacles for the bomber. Unless there is an absolute requirement for such ornamentation, window boxes and planters are better removed. If they must remain, a security patrol should be employed to check them regularly.

(5) A highly visible security patrol can be significant deterrent. Even if this "patrol" is only one security guard/night guard, he/she is optimally utilized outside the building. If an interior guard is utilized, consider the installation of closed-circuit television cameras that cover exterior building perimeters.

(6) Have an adequate burglar alarm system installed by a reputable company that can service and properly maintain the equipment. Post signs indicating that such a system is in place.

(7) Entrance/exit doors with hinges and hinge pins on the inside to prevent removal should be installed. Solid wood or sheet metal-faced doors provide extra integrity that a hollow-core wooden door cannot provide. A steel doorframe that properly fits the door is as important as the construction of the door.

(8) The ideal security situation is a building with no windows. However, bars, grates, heavy mesh screens, or steel shutters over

windows offer good protection from otherwise unwanted entry. It is important that the openings in the protective coverings are not too large. Otherwise, a bomb may be introduced into the building while the bomber remains outside. Floor vents, transoms, and skylights should also be covered. Please note that fire safety considerations preclude the use of certain window coverings.

(9) Controls should be established for positively identifying personnel who are authorized access to critical areas and for denying access to unauthorized personnel. These controls should extend to the inspection of all packages and materials being taken into critical areas.

(10) Security and maintenance personnel should be alert for people who act in a suspicious manner, as well as objects, items, or parcels which look out of place or suspicious. Surveillance should be established to include potential hiding places (e.g., stairwells, rest rooms, and any vacant office space) for unwanted individuals.

(11) Doors or access ways to such areas as boiler rooms, mail rooms, computer areas, switchboards, and elevator control rooms should remain locked when not in use. It is important to establish a procedure for the accountability of keys. If keys cannot be accounted for, locks should be changed.

(12) Good housekeeping is also vital. Trash or Dumpster areas should remain free of debris. A bomb or device can easily be concealed in the trash. Combustible materials should be properly disposed of, or protected if further use is anticipated.

(13) Install detection devices at all entrances and closed-circuit television in those areas previously identified as likely places where a bomb may be placed. This, coupled with the posting of signs indicating such measures are in place, is a good deterrent.

(14) 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.

(15) 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.

D. Responding to Telephonic Bomb Threats.

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

2. It is always desirable that more than one person listens 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.

3. 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.

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

a. Keep the caller on the line as long as possible.

b. Ask him/her to repeat the message.

c. Try to keep a word for word record of the conversation. Record every word spoken by the caller.

d. If the caller does not indicate the location of the bomb or the time of possible detonation, ask him/her for this information.

e. 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.

f. Attempt to keep the caller talking and elicit further information if possible.

g. Attempt to obtain the caller’s name, address, and telephone number. Point out to the caller that by giving these details they are indicating the validity of the warning.

h. Summon assistance (through a telephone exchange) to trace the call and to corroborate facts and opinions.

i. Comply with the caller's request to be connected with another extension. Monitor the call if possible. Alert security and designated personnel.

j. 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.

k. 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.

l. **DON'T HANG UP!** After the caller hangs up, place your line on hold or leave it off hook if hold is not available. From another phone or line, call the operator and advise them you've just received a bomb threat and would like a "lock on" for phone line _____ (phone number call was received on). Many people have been caught this way, even from pay phones if done quickly enough. The operator can assist in trying to determine the type of telephone call.

(1) Was the call operator-connected?

(2) If the call was operator connected, identify the call source?

(3) Was it from a pay phone?

(4) If dialed from a pay phone, was it direct dialed?

m. Report the information immediately to the chain of command, police department, fire department, ATF, FBI, and other appropriate agencies. The sequence of notification should be established in the bomb incident plan.

n. After the call is complete, make a full written record of the conversation and your impressions based on the information annotated on the Telephonic Bomb Threat Report (Exhibit 12-1).

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

E. Countermeasures. In order to effectively handle a bomb threat situation, certain procedures must be developed in advance of the threat. The ultimate goal is to provide early detection of an explosive device and to minimize disruption at the unit.

1. Preplanning considerations

   a. Preplanning is an essential prerequisite for developing a workable bomb threat plan. In the preplanning phase, provision shall be made for communication channels and support organizations (primary and alternate).

   b. Communication equipment. Do not operate radio transmitters in the vicinity of the bomb. They could detonate it.

2. The following shall be considered in the bomb threat/incident plan:

   a. Control of the operation.

   b. Evacuation.

   c. Search.

   d. Action to be taken upon finding the bomb or suspected bomb.

   e. Disposal - Explosives Ordnance Disposal (EOD).

   f. Detonation and damage control. Barricade material around the device to guide fragments upward.

   g. Control of publicity.

   h. Erection of barriers.

   i. Fire and medical service standby.

   j. Disconnection of utilities.

   k. Removal of flammables/explosives.

   l. Establishment of temporary morgue facilities.

   m. Pre-designation of hospitals and emergency medical service (EMS) ambulance services that will provide support.

   n. After action report.

3. Evaluate the threat.

4. Activate the plan.

F. Decision Time.

1. The most serious of all decisions to be made by the command 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.

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

   a. Ignore the threat.

   b. Evacuate immediately.

   c. Search and evacuate if warranted.

3. 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.

4. 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 the mission. 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 command/mission to a standstill. An employee, knowing that the policy is to evacuate immediately, may make a threat in order to get out of work. 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.

5. 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.

G. Conducting a Search.

1. General. The choice of search techniques will depend on whether the threat is overt or covert. The following decisions must be made before the proper techniques can be applied.

   a. Will the search be conducted prior to, after, or without evacuation?

   b. Will supervisors, occupants, or a special team conduct the search, i.e.; those personnel most familiar with the area to be searched (those personnel most likely to be able to identify unusual or unfamiliar objects).

   c. What portions of the building will be searched? Uncontrolled common areas shall always be searched; restricted areas, where access is controlled, may not require a search.

2. Search Teams

   a. It is advisable to use more than one individual to search any area or room, no matter how small. Searches can be conducted by supervisory personnel, area occupants or trained explosive search teams. There are advantages and disadvantages to each method of staffing the search teams.

   b. Using supervisory personnel to search is a rapid approach and causes little disturbance. There will be little loss of employee working time, but a morale problem may develop if it is discovered that a bomb threat has been received and workers were left unaware. Using a supervisor to search will usually not be as thorough because of his/her unfamiliarity with many areas and his/her desire to get on with business.

   c. Using area occupants to search their own areas is the best method for a rapid search. The occupants' concern for their own safety will contribute toward a more thorough search. Furthermore, the personnel conducting the search are familiar with what does or does not belong in a particular area. Using occupants to search will result in a shorter loss of work time than if all were evacuated prior to search by trained teams. Using the occupants to search can have a positive effect on morale, given a good training program to develop confidence. Of course, this would require the training of an entire work force, and ideally the performance of several practical training exercises. One drawback of this search method is the increased danger to non-evacuated workers.

d. The search conducted by a trained team is the best for safety, morale and thoroughness, though it does take the most time. Using a trained team will result in a significant loss of production time. It is a slow operation that requires comprehensive training and practice.

e. The decision as to who should conduct searches lies with the command, and should be considered and incorporated into the bomb incident plan.

3. Search Techniques.

a. The following room search technique is based on the use of a two-person searching team. There are many minor variations possible in searching a room. The following contains only the basic techniques.

b. When the two-person search team enters the room to be searched, they should first move to various parts of the room and stand quietly with their eyes closed and listen for a clockwork device. Frequently, a clockwork mechanism can be quickly detected without use of special equipment. Even if no clockwork mechanism is detected, the team is now aware of the background noise level within the room itself.

c. Background noise or transferred sound is always disturbing during a building search. If a ticking sound is heard but cannot be located, one might become unnerved. The ticking sound may come from an unbalanced air-conditioner fan several floors away or from a dripping sink down the hall. Sound will transfer through air-conditioning ducts, along water pipes, and through walls. One of the most difficult buildings to search is one that has steam or hot water heat. This type of building will constantly thump, crack, chatter, and tick due to the movement of the steam or hot water through the pipes and the expansion and contraction of the pipes. Background noise may also include outside traffic sounds, rain, and wind.

d. The individual in charge of the room searching team should look around the room and determine how the room is to be divided for searching and to what height the first searching sweep should extend. The first searching sweep will cover all items resting on the floor up to the selected height.

e. You should divide the room into two virtually equal parts. This equal division should be based on the number and type of objects in the room to be searched and not on the size of the room. An imaginary line is then drawn between two objects in the room; e.g., the edge of the window on the north wall to the floor lamp on the south wall.

(1) First Room-Searching Sweep

(a) Look at the furniture or objects in the room and determine the average height of the majority of items resting on the floor. In an average room, this height usually includes table or desktops and chair backs. The first searching height usually covers the items in the room up to hip height.

(b) 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.

(c) 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.

(2) 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 bookcases, and tall table lamps.

(3) 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.

(4) 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.

f. 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.

g. 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 speaker's 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.

h. 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 wails and proceed toward the center of the room.

4. Vehicle Bomb Search. Exhibit 12-5 outlines a step-by-step guide for conducting a vehicle bomb search.

H. Suspicious Object Located

1. 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:

   a. 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.

   b. If absolutely necessary, place sandbags or mattresses, never metal shields, around the suspicious object. Do not attempt to cover the object.

   c. Identify the danger area, and block it off with a clear zone of at least 300 feet, including floors below and above the object.

d. Check to see that all doors and windows are open to minimize primary damage from blast and secondary damage from fragmentation.

e. Evacuate the building/area.

f. Do not permit re-entry into the building until the device has been removed/disarmed, and the building declared safe for re-entry.

I. Evacuation Procedures. If a threat is received and a bomb is found, the following must be considered:

1. An evacuation unit consisting of management personnel should be organized and trained. The organization and training of this unit should be coordinated with the development of the bomb incident plan.

2. The evacuation unit should be trained in how to evacuate the building during a bomb threat. You should consider priority of evacuation, e.g., evacuation by floor level. Evacuate the floor levels above and below the danger area in order to remove those persons from danger as quickly as possible.

3. You may also train the evacuation unit in search techniques, or you may prefer a separate search unit. Volunteer personnel should be solicited for this function. Assignment of search wardens, team leaders, etc., can be employed. To be proficient in searching the building, search personnel must be thoroughly familiar with all hallways, rest rooms, false ceiling areas, and every location in the building where an explosive or incendiary device may be concealed. When police officers or firefighters arrive at the building, the contents and the floor plan will be unfamiliar to them if they have not previously reconnoitered the facility. Thus, it is extremely important that the evacuation or search unit be thoroughly trained and familiar with the floor plan of the building and immediate outside areas. When a room or particular area is searched, it should be marked or sealed with a piece of tape and reported to the supervisor of that area.

4. The evacuation or search unit should be trained only in evacuation and search techniques and not in the techniques of neutralizing, removing or otherwise having contact with the device. If a device is located, it should not be disturbed. However, its location should be well marked and a route back to the device noted.

5. Evacuation Plan. An evacuation plan should contain the following

a. Authority to order evacuation.

b. The signal to evacuate.

c. What the evacuation procedures are.

d. Who will be on the evacuation team.

e. Responsibilities of the occupants during evacuation.

f. Priorities for personnel removal.

g. Predesignated guides.

h. Predesignated routes of evacuation.

i. Designating evacuating occupants.

j. Designated location to evacuate to.

k. Decision to permit reentry to building.

J. Handling the News Media

1. 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.

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

K. Training As mentioned throughout this chapter, thorough planning, preparation and training is essential to how your unit will respond to a bomb threat or incident. Periodic planning and response drills will help to identify and resolve deficiencies prior to actual need. Commands should ensure that all personnel receive training in response and evacuation measures. Particular training should be provided to security/police force personnel about their specific roles in providing leadership and protection during incidents. Commands should periodically conduct joint training with the outside agencies that will be expected to provide support during a bomb threat/incident aboard the government facilities. Remember, your unit and personnel will have a tendency to respond to a real crisis in the same way that they train to respond. **BE PREPARED!**

L. Summary

1. This information 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 commanding officer for the threatened facility.

2. Develop a bomb incident plan (Exhibit 12-3). Draw upon any expertise that is available to you from your cognizant security manager, police departments, government agencies, and security specialists. Don't leave anything to chance. **BE PREPARED!**

This page intentionally left blank

EXHIBIT 12-1

TELEPHONIC BOMB THREAT REPORT

EXACT WORDING OF THREAT:_____
_____
_____
_____
_____
_____
_____

ASK CALLER:

WHEN IS THE BOMB GOING TO EXPLODE?_____
WHERE IS IT RIGHT NOW? _____
WHAT DOES IT LOOK LIKE? _____
WHAT KIND IS IT?_____
WHAT WILL MAKE IT EXPLODE?_____
WHAT ORGANIZATION DO YOU REPRESENT?_____
WHERE ARE YOU CALLING FROM?_____
WHY WAS IT PLANTED?_____

CALLER'S VOICE:

___CALM	___SOFT	___DISTINCT	___LISP	___DEEP BREATHING
___ANGRY	___LOUD	___SLURRED	___RASPY	___CRACKLING VOICE
___EXCITED	___LAUGHTER	___WHISPER	___DEEP	___DISGUISED
___SLOW	___CRYING	___NASAL	___RAGGED	___ACCENT
___RAPID	___NORMAL	___STUTTER	___FAMILIAR	___CLEARING THROAT

THREAT LANGUAGE:

___FLUENT	___INCOHERENT	___RATIONAL
___PRECISE	___ARTICULATE	___IRRATIONAL
___BROKEN	___REPEATING	___READING STATEMENT

ACCENT:

___SOUTHERN	___NEW ENGLAND	___BRITISH	___MIDDLE EAST
___NORTHER	___EUROPEAN	___ORIENTAL	OTHER:_____

BACKGROUND SOUNDS:

___TRAFFIC	___CHILDREN	___CLEAR	___OTHER (LIST)
___MACHINERY	___ANIMALS	___STATIC	_____
___OFFICE	___MUSIC	___LOCAL	_____
___PA SYSTEM	___MOTOR	___LONG DISTANCE	_____

ADDITIONAL INFORMATION:

_____
_____
_____
_____
_____

IMMEDIATELY REPORT CALL TO:_____

RECIPIENT OF CALL:_____

DATE:_____ TIME:_____ AT PHONE MUMBER:_____

DON'T HANG UP

This page intentionally left blank

EXHIBIT 12-2

LETTER AND PACKAGE BOMB RECOGNITION SIGNS

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.

The following information is useful in detecting the presence of letter or package bombs sent through the U.S. or international mails. While by no means a complete or foolproof list, letters and packages exhibiting the characteristics below should be viewed with extreme caution.

1. Delivery:

    a. The item does not have to be delivered by a postal carrier. Most bombers set up and deliver the bomb themselves.

    b. If delivered by carrier, inspect for lumps, bulges, or protrusions, without applying pressure.

    c. If delivered by carrier, conduct a balance check to see if it is lopsided or heavy sided.

    d. Packages or letters hand delivered or dropped off for a friend.

    e. Any letters or packages arriving before or after a phone call from an unknown person asking if the item was received.

2. Packaging:

    a. Leaks, stains, or moisture. Possibly from the "sweating" of plastic explosives.

    b. Inks, particularly reds or blues, may bleed, staining envelope.

    c. Use of extra sealing material.

    d. Packages wrapped in string are automatically suspicious, as modern packaging materials have eliminated the need for twine or string.

    e. Wires, string or foil are sticking out or attached.

EXHIBIT 12-2

f. Inner sealed enclosure.

g. Peculiar odor.

h. Feeling of springiness in its top, bottom, or sides.

i. Unexpected sounds generating from the package.

3. Weight:

a. Weight is unevenly distributed.

b. Heavier than usual for its size.

4. Thickness/Rigidity:

a. Not uniform or has bulges.

b. Greater than normal, particularly along its center length.

c. For medium size envelopes, the thickness of a small book and fairly rigid.

d. For large envelopes, bulkiness, an inch or more in thickness and fairly rigid.

5. Address:

a. Poorly typed or handwritten address.

b. Handwritten addresses or labels from companies are improper. Check to see if the company exists and if they sent a package or letter.

c. Addressed to a high ranking recipient either by name, rank, title, division, or department within the organization.

d. Title or rank of the recipient is incorrect.

e. Any unexpected foreign addresses, or postage.

f. Improper spelling of common names, places, or titles.

g. Generic or incorrect titles.

h. No return address or nonsensical return address.

EXHIBIT 12-2

6. Writing:

   a. Marked (handwritten notes or stamped)such as: “PERSONAL,” “PRIVATE,” “For _____ eyes only,” "To Be Opened in the Privacy of_____," "CONFIDENTIAL," "Your Lucky Day is Here," "Prize Enclosed," etc.

   b. Marked (written or stamped) “Air Mail,” “Registered,” “Certified” or “Special Delivery” unnecessarily.

   c. Misspelled words, particularly those in common military usage.

   d. Style of writing is foreign.

7. Postage:

   a. More than enough postage for the piece. (Excess postage on small packages or letters indicates that the object was not weighed by the Post Office.)

   b. No postage

   c. Non-canceled postage.

   d. Unexpected foreign postage

8. Postmark:

   a. From unusual city or town in the United States.

   b. Unexpected foreign postmarks.

   c. Multiple postmarks.

If you have a suspicious letter or package
Call: 911 - ISOLATE - EVACUATE

EXHIBIT 12-3

Bomb Incident Plan

1. Designate a chain of command.

2. Establish a command center.

3. Decide what primary and alternate communications will be used.

4. Establish clearly how and by whom a bomb threat will be evaluated.

5. Decide what procedures will be followed when a bomb threat is received or device discovered.

6. Determine to what extent the available bomb squad will assist and at what point the squad will respond.

7. Provide an evacuation plan with enough flexibility to avoid a suspected danger area.

8. Designate search teams.

9. Designate areas to be searched.

10. Establish techniques to be utilized during search.

11. Establish a procedure to report and track progress of the search and a method to lead qualified bomb technicians to a suspicious package.

12. Have a contingency plan available if a bomb should go off .

13. Establish a simple-to-follow procedure for the person receiving the bomb threat.

14. Designate and establish a temporary morgue facilities.

15. Activation plan for Emergency Medical Service (EMS) ambulance services that will respond and transport, and pre-designated medical facilities that will provide victim support.

16. Review your physical security plan in conjunction with the development of your bomb incident plan.

EXHIBIT 12-4

Bomb Threat Command Center Plan

1. Designate a primary location and an alternate location.

2. Assign personnel and designate decision making authority.

3. Establish a method for tracking search teams.

4. Maintain a list of likely target areas.

5. Maintain a blueprint of floor diagrams and facility plans in the center.

6. Establish primary and secondary methods of communication.
   (Caution-the use of two-way radios during a search can cause premature detonation of an electric blasting cap.)

7. Formulate a plan for establishing a command center, if a threat is received after normal work hours.

8. Maintain a roster of all necessary telephone numbers.

EXHIBIT 12-5

VEHICLE BOMB SEARCH

The following information is intended to provide a step-by-step guide that can be used by every driver to carefully and thoroughly inspect government and personal vehicles for the presence of improvised explosive devices.

1. Prevention:

   a. Be suspicious.

   b. Check your vehicle at irregular intervals and times.

   c. Always lock your vehicle.

   d. Let a fine coat of dust remain on the vehicle surface or apply talc powder to help detect tampering.

   e. Secure transparent tape to vehicle doors, trunk, and hood to help detect tampering.

   f. Install two bolts in an X pattern through the open end of the exhaust pipe. This is one place a terrorist can easily and quickly place an explosive device.

   g. Another favorite spot is the fuel tank. Use a locking gas cap and install or have installed a mesh strainer in the mouth of the filler tube.

   h. Don't wait for passengers in an idling or parked vehicle. Get outside where you can see everything that's happening.

2. Exterior Search:

Know your vehicle inside and out so you can quickly recognize something wrong. Unless your vehicle has been under continuous positive control, always assume that it has been tampered with. Here's how you can search your vehicle to find that bomb.

NOTE. If you do find a bomb, **DO NOT TOUCH IT!**
Call the police/security forces, isolate the device, and evacuate the area.

   a. If possible, search in pairs. Start by searching the area around the vehicle.

   b. Examine the exterior surfaces of the vehicle. Look for signs of tampering: wires hanging down; doors, hood, or trunk left ajar; anything different.

EXHIBIT 12-5

c. Check the film of dust or powder. Is it undisturbed? Has another layer of dust appeared?

d. Has the transparent tape been removed or broken?

e. Has the hood or trunk lock been jimmied? Look; do not lift it. Are there any other signs of forced entry? Broken windows, scratched paint, bent or damaged metal?

f. Look closely for any bits of tape or wire lying around inside or outside of the vehicle.

g. Look for any unusual marks on the ground surrounding the vehicle.

h. Examine the ground near the tires for any signs of digging.

i. Check the gas tank. Remove the cap and look inside.

j. Check in and around the exhaust pipe(s).

k. Check the undercarriage. If you can, use a long handled mirror to help in your search. Look for disturbed dirt, suspicious tapes or wires, or objects that don't belong there.

l. Look in the wheel wells and behind the bumpers.

m. Use extreme caution when searching any external compartments. Open just a crack first, look, and then gently feel for a trip wire. If none is found, the compartment may be safe to open all the way.

n. Look everywhere: steps, handholds, even the canvas tops of vehicles.

3. Interior Search:

a. Use extreme caution! Always <u>look</u> inside before you move inside.

b. Looking through the windows, do you see anything out of place? Has anything been moved?

c. Has anything been added: a package or briefcase that doesn't belong there?

d. Do you see tapes or wires hanging down?

e. Is the door ajar?

EXHIBIT 12-5

f. Are there any wires protruding from beneath any doors? If all is clear, open the door.

g. **DON'T TOUCH ANYTHING YET**. Make a visual search of the interior. Look under and around the seats. Never rest your weight on the seats until you've looked.

h. Look at the carpet or floor mats for any suspicious bulges. Look as far as you can under the seats and around them.

i. Now slip into the seat and check the ashtray, adjustable head rests, and seatbelts.

j. In a sedan, pay special attention to the right rear passenger seat.

k. Carefully check the glove compartment.

l. Look under the dash, checking especially for strange tapes or wires.

m. Use a flashlight to check the air conditioning ducts and other cavities.

n. Carefully examine the sun visors and mirrors for signs of tampering.

4. Engine and Trunk Search:

a. Now exit the vehicle and open the hood, a quarter inch at first. Be very thorough in gently feeling for wires along the entire length of the hood.

b. Raise the hood and make a thorough search of the engine compartment and firewall.

(1) First, look for any strange or new looking wires attached to the battery, to the clutch, coil, accelerator, or any power operated equipment.

(2) Check in the cavities for anything that looks like it doesn't belong and anything out of place.

(3) Open the air filter and look inside. Pay special attention to the spark plug wires, the distributor, the ignition area, and the exhaust manifold.

c. Open the trunk just a quarter inch and feel for wires along the edges. Then open it to check all the items inside. Anything rearranged? Anything new?

d. Check the spare tire to ensure it is filled with air, and nothing else.

EXHIBIT 12-5

5. Careful Start:

   a. If everything looks Ok so far, get into the driver's seat and check the dashboard.

   b. Does anything on the steering column appear unusual?

   c. Look at the turn signal and light controls for anything unusual, then turn them on. Do the same – look, then try – with the wipers and washer, radio, and horn.

   d. Start the vehicle, letting it run for about 2 minutes before moving.

   e. Move slowly at first, testing the steering and brakes, then go on about your business.

6. Summary:

   Try to develop a sixth sense about potential danger in your area.

   Search your vehicle at irregular times, but always use the same routine so you don't overlook anything.

   Know your vehicle inside and out so you can recognize any thing different.

   The minutes spent searching your vehicle can mean a lifetime for you and your passengers.

If you find a suspicious device
Call: 911 - ISOLATE - EVACUATE

GLOSSARY OF TERMS AND ACRONYMS

PART I GLOSSARY OF TERMS

Access. Entry to a specified area or unit.

Ammunition. A device charged with explosives, propellants, pyrotechnics, riot control agents, chemical herbicides, smoke and flame for use in connection with defense or offense, including demolition. Ammunition includes cartridges, projectiles, bombs, missiles, grenades, mines, pyrotechnics, bullets, shot, primers, propellants, fuses and detonators.

Annunciator. A visual or audible signaling device that indicates conditions of associated circuits. Usually, this is accomplished by activation of a signal lamp or audible sound.

Antiterrorism/Counterterrorism.. Actions and measures to deter, detect, and respond vigorously to all terrorist attacks against Coast Guard facilities, ships, aircraft, resources or personnel (PDD-39) (Element of the Physical Security Program).

Armed Guard. An individual equipped with a firearm and ammunition whose primary function is to protect property, and who has qualified in an approved weapons qualification course. The guard is considered "armed" when the firearm and ammunition are readily available for immediate use.

Armory. An arms storage area, i.e., compartment, room or building specifically designed and designated to store AA&E.

Arms. A weapon which will, or is designed to, expel a projectile or flame by the action of an explosive, and the frame or receiver or metal parts of any such weapon from which a complete weapon could be constructed.

Arms Racks. Storage of arms that meet the security criteria outlined in Chapter 3.

Automated Data Processing Security Officer. An individual designated in writing to manage the AIS Security Program.

Automated Data Processing System Security Officer. An individual designated in writing, who has been assigned responsibility for the security of an AIS.

Badge. A mechanism for positively identifying personnel and establishing authorization for personnel movement and control.

Balanced Magnetic Switch. A magnetically operated switch designed to detect the opening of secured doors, windows, etc.

Bomb. A device capable of producing damage to material and injury or death to personnel when detonated or ignited. Bombs are classified as explosive or incendiary. An explosive bomb causes damage by fragmentation, heat and blast wave. The heat produced often causes a secondary incendiary effect. An incendiary bomb generates fire-producing heat without substantial explosion when ignited. Bombing occurs when an explosive bomb detonates, or an incendiary bomb ignites.

Bomb Incident. Involves any occurrence concerning the detonation/ignition of a bomb, discovery of a bomb, or receipt of a bomb threat.

Bomb Threat. A message delivered by any means, which may or may not

- Specify location of the bomb
- Include the time for detonation/ignition
- Contain an ultimatum related to the detonation/ignition or concealment of the bomb.

Burglary Resistant Safe. A safe certified by Underwriters' Laboratories and manufactured under certain classifications.

Clear Zone. An area on one or both sides of a perimeter barrier which provides an unobstructed view of the barrier and the ground adjacent to it.

Closed Circuit Television. A system normally consisting of a television camera, monitor, and electrical circuitry that is frequently used to complement an IDS.

Cognizant Security Manager. An individual designated in writing to manage the overall area and district Security Program for specific district units (all those within their geographic boundaries, except for area units) or specific area units (all those within the area, except for district units).

Command Security Officer. An individual designated in writing to manage the overall unit Security Program.

Commanding Officer. Any commander, officer-in-charge, or other title assigned to command status.

Compensatory Measure. An alternative physical security measure employed to provide a degree of security equivalent to or exceeding the provisions of this manual.

Continuous 24 Hour Live Watch. The continuous observations by awake and alert personnel. For rooms or office spaces, the individual need not be physically in the room or space; however, the individual must be in a position to prevent access or maintain continuous observation of the room or space. This does not include personnel who are asleep.

Control Unit. The terminal box that receives alarm and tamper signals and transmits these signals to the local audible alarm and/or monitor unit. It provides the primary and backup power for all sensors and activates and
deactivates the system.

Criticality. A measure of importance to a unit mission or national security. Examples of protection for critical functions include alternate sources of supply and backup/redundant capabilities.

Critical Infrastructure. Those physical and information systems essential to the minimum operations of the Coast Guard. They include, but are not limited to, financial systems, electrical power systems, fuel storage and transportation, water supply systems, telecommunications, and emergency services (including medical, police/security forces, fire and rescue). Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence.

Defense Readiness States (DEFCON). These are mobilization and deployment states of the entire U.S. defense establishment including but not limited to DoD Components, other U.S. Government Agencies and Departments assigned specific responsibilities to assist DoD during times of war, and elements of the Defense Industrial Base. DEFCONs refer to wartime postures. DEFCONs are declared by the National Command Authority.

Delay. The effect achieved by physical features, technical devices, or security measures and forces that impede an adversary from gaining access to a target. Normally expressed as a function of time, it is a major consideration in the design and development of security systems.

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

Duress Alarm System. The combination of duress alarms, fixed, portable, and duress code procedures by which personnel can covertly communicate the existence of a threat situation to other operating or security personnel. Duress alarms are normally installed to protect those who may come under a threat, and they read out at the alarm control center. Duress code procedures normally are used to protect authorized personnel in face-to-face threat situations, and should be changed frequently to prevent compromise.

Espionage. Overt, covert or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used for the injury of the U. S. or to the advantage of a foreign nation.

Exception. A written permanent deviation from a specific provision of this manual. The authority for which is based upon the implementation of better or equivalent protection and an established configuration or process.

Explosives. Any chemical compound, mixture or device, the primary or common purpose of which is to function by explosion. This includes, but is not limited to, individual land mines, demolition charges, and blocks of explosives (dynamite, TNT, C-4, etc.).

GSA Approved Container. A container that has been approved and manufactured under certain federal specifications, as specified by the General Services Administration.

Hardened Structure. A structure housing critical or sensitive assets, constructed so that it will delay a forcible entry attempt for sufficient time to assure that the adversary will be observed and appropriate countermeasures taken.

High-Risk Personnel. Individuals or groups who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets.

Intrusion Detection System. A system consisting of sensors, signal media, annunciators and an energy source for signaling the entry or attempted entry into the protected area.

Jurisdiction. Federally mandated control in which a commanding officer exercises judicial and other authority over an area under his/her cognizance. Three types of jurisdiction are exclusive, concurrent and proprietary.

Key and Lock Control System. A system encompassing all keys and locks used to safeguard assets and information.

Key Control Officer. An individual designated in writing by the commanding officer to manage the unit key control system.

Loss Prevention. That part of an overall security program dealing with resources, measures and tactics devoted to the care and protection of government property.

Magazines. Storage of ammunition that meets the security criteria outlined in Chapter 3.

Mission Essential/Vulnerable Areas. Areas or activities, which, by virtue of their function, are essential to successful accomplishment of the Coast Guard, mission. Also included are areas not essential to the operational mission, but which by nature of the unit are vulnerable to espionage, sabotage, theft, or other criminal activity.

Mobile Units. Those commands and assets, not personnel, that are characterized by design and application as having the capability of self-propelled movement. This would include ships, boats and aircraft. Other uses must be approved in writing by the cognizant Security Manager. It does not include temporary dwellings and structures being utilized as a fixed facility.

Monitor. A device that senses and reports on the condition of an alarm system, commonly used interchangeably with the terms monitor unit, monitor panel, status indicator module, annunciator, etc.

National Command Authorities. The President and the Secretary of Defense or their duly deputized alternates (or successors).

Net Explosive Weight. A measure of the total static weight of the explosives in a round. They are listed for each NALC in SW020-AC-SAF-010/020/030, Transportation and Storage Data for Ammunition.

Network Security Officer. An individual assigned responsibility for the security of a network.

Non-restricted Area. An area in which access is either minimally controlled or uncontrolled.

Nuisance Alarm. The result of a sensor activation caused by accident, neglect, malfunction, or natural causes, such as wind, lightning or thunder. Often improperly called a false alarm.

Physical Security. That part of security concerned with tangible measures designed to safeguard personnel; to prevent unauthorized access to equipment, property, materiel and documents; and to safeguard them against espionage, sabotage, damage, pilferage and theft.

Physical Security Evaluation. A formal recorded assessment of physical security measures to determine compliance with physical security policy.

Physical Security Plan. A comprehensive written plan providing proper and economical use of personnel and equipment to prevent or minimize loss or damage from theft, espionage, sabotage and other criminal or disruptive activity.

Physical Security Program. The interrelationship of various security devices (structural standards, locks, IDS, etc.) that complement each other to produce a comprehensive approach to physical security matters. These components include, as a minimum, the physical security plan, physical security evaluations and surveys, and a continuing assessment of the unit physical security posture.

Physical Security Survey. A specific on-site evaluation by the CSO to determine vulnerabilities and compliance with physical security policy. Survey results are used primarily as a management tool by the surveyed unit.

Pilferable Items. Material having a ready resale value, civilian utility or personal application and which is, therefore, subject to theft.

Protective Lighting. Lighting, during hours of darkness, that provides a continuing degree of protection similar to that maintained during daylight hours.

Restricted Area. A designated area under Coast Guard control into which persons may not enter without specific authorization. The area contains information or material vital to the Coast Guard mission requiring special security measures to protect the resources contained therein from

sabotage, espionage, damage or theft. Restricted areas are designated as exclusion, limited, or controlled.

Sabotage. An act or acts with intent to injure, interfere with, or obstruct the national defense by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources.

Salvage Value. The value of equipment which can be readily removed and installed elsewhere.

Seals. A device to show whether the integrity of an asset has been compromised. Seals are numbered serially, are tamper proof and must be safeguarded while in storage.

Security Check. A check conducted by security personnel to ensure the integrity of the security interest involved. Physical checks of locking devices includes examination to ensure closure, by manual means, i.e., shaking, pulling and pushing locking devices installed on doors, windows, magazines, buildings, gates, etc.

Security Force. That portion of security at a unit, comprised of either active duty military, civilian police/guard personnel, contract guard personnel, or a combination tasked with providing physical security and law enforcement services.

Security Hazard. An act or condition which may result in the compromise of information, loss of life, damage, loss or destruction of property, or disruption of the mission of the unit. Security hazards are categorized into two types: natural and manmade. Natural hazards are usually the consequence of natural phenomena, such as floods, storms or winds. Manmade hazards are acts of commission or omission, both covert and overt, which could disrupt or destroy the operation or mission of a unit. Examples of manmade hazards include sabotage, pilferage, carelessness, accidents and civil disturbances.

Security Risk Categories. A division of the most sensitive AA&E into four categories based upon factors such as attractiveness for theft, portability, and magnitude of effect of their misuse, etc. They assist in directing the application of security measures commensurate with the gravity of loss.

Selvage. The edge on either side of a woven fence fabric so finished as to prevent raveling.

Self-Defense Force. That portion of personnel at a unit, comprised of active duty military and/or Security Force personnel tasked with providing armed response to hostile assault.

Sensitive Items. Material which requires a high degree of protection and control due to regulatory requirements such as controlled medical substances, funds and negotiable instruments, hazardous items, AA&E, etc.

Sound Masking. A system that provides programmed cover music to effectively mask electronic eavesdropping techniques.

Sound Transmission Class. A term used in architectural acoustics to describe the transmission attenuation afforded by various wall materials and other building components.

Supervised Line. A conductor, which if cut, broken, shorted or otherwise tampered with, will cause a change in status indicated at a monitoring unit.

Technical Security Countermeasures. Specialized counterintelligence techniques and measures employed to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to National Security Information and/or sensitive but unclassified information.

TEMPEST. The study and control of compromising emanations emitted from electrical equipment.

Terrorism. The calculated use or threatened use of unlawful force or violence against individuals or property to inculcate fear, with the intention of coercing or intimidating governments or societies, in the pursuit of goals that are generally political, religious, or ideological.

Terrorists. Individuals or groups of individuals who may be sponsored by sovereign states or political organizations and who use violence, terror, and intimidation to pursue ideological, criminal, national, personal, religious, or political objectives.

Terrorist Threat Conditions. Program standardizing the Military Services' identification of and recommended responses to terrorist threats against U.S. personnel and facilities. This program facilitates inter-Service coordination and support for antiterrorism activities. Consisting of a series of four graduated categories describing progressive levels of countermeasures implemented to protect facilities, assets, and personnel from attack.

Theft. A common name for larceny and pilferage. It is the taking of property without the owner's consent, with intent to deprive the owner of the value of the same, and to appropriate it to the use or benefit of the person taking it.

Threat Level. A five-step scale of standardized terms used to describe the severity of terrorist threats on a country-specific basis as judged by intelligence analysts. These five steps from highest to lowest are: CRITICAL, HIGH, MEDIUM, LOW, AND NEGLIGIBLE.

Visitor. Any individual not under official orders to the unit, or otherwise employed by the unit.

Visitors Bill. Written directives containing procedures on the control and movement of visitors.

Vulnerability. A measure of susceptibility to damage, destruction or loss by virtue of location or state of being/readiness. Examples of protection for vulnerable functions include relocation of the function, diversion of attention away from the function, and improved security measures.

Waiver. A written temporary relief from specific standards imposed by this manual, pending actions or accomplishment of actions that will result in conformance with the standards required. Interim compensatory security measures are required.

Workmanlike Manner. In construction, all cracks, holes and openings on the interior and exterior of an area permanently sealed, properly finished, or painted.

PART II GLOSSARY OF ACRONYMS

AA&E.	Arms, Ammunition and Explosives
A&E.	Ammunition and Explosives
ADP.	Automated Data Processing
ADPSO.	Automated Data Processing Security Officer
ADPSSO.	Automated Data Processing Systems Security Officer
AIS.	Automated Information Systems
AOR.	Area of Responsibility
ATF.	Alcohol, Tobacco and Firearms
BMS.	Balanced Magnetic Switch
CCTV.	Closed Circuit Television
CEU.	Civil Engineering Unit
CGHQ.	Coast Guard Headquarters
CGIS.	Coast Guard Investigative Service
CMCO.	Classified Material Control Officer
COMMCEN.	Communication Center
COMSEC.	Communication Security
CP.	Chief of Police
CSO.	Command Security Officer
CT.	Counterterrorism
DEFCON.	Defense Readiness Condition

DOD.	Department of Defense
DOT.	Department of Transportation
DSCO.	Document Station Control Officer
E.	Exception
ENTNAC.	Entrance National Agency Check
EOD.	Explosives Ordnance Disposal
FBI.	Federal Bureau of Investigations
FD&CC.	Facility Design and Construction Center
FOUO.	For Official Use Only
GSA.	General Services Administration
IDS.	Intrusion Detection System
ISOO.	Information Security Oversight Office
MILHDBK.	Military Handbook
MLC.	Maintenance and Logistics Command
MPC.	Military Personnel Command
MOU.	Memorandum of Understanding
MSF.	Motorcycle Safety Foundation
MSO.	Marine Safety Office
NAC.	National Agency Check
NACLC.	National Agency Check with Local Check
NAVFAC.	Naval Facility Engineering Command
NAVCIVENGRLAB.	Naval Civil Engineering Laboratory
NEW.	Net Explosive Weight

NIJ.	National Institute of Justice
NSN.	National Stock Number
NSO.	Network Security Officer
OCE.	Army Office of Chief of Engineers
OPCEN.	Operations Center
PDW.	Personal Defense Weapon
POV.	Privately Owned Vehicle
RF.	Radio Frequency
SDF.	Self Defense Force
SECMGR.	Security Manager
S&G.	Sargent and Greenleaf
SLTG.	Shoulder Line Throwing Gun
SN.	Stock Number
SOP.	Standard Operating Procedure
SSBI.	Single Scope Background Investigation
SSIC.	Standard Subject Identification Code
SSO.	Special Security Officer
STC.	Sound Transmission Class
STU III.	Secure Telephone Unit
THREATCON.	Threat Condition
TISCOM.	Telecommunications and Information Systems Command
TS.	Top Secret

TSCM.	Technical Security Countermeasures
TSCO.	Top Secret Control Officer
TSG.	Telephone Security Group
UCMJ.	Uniform Code of Military Justice
UL.	Underwriters Laboratory
VP.	Vulnerable Points
W.	Waiver

PHYSICAL SECURITY PLAN

1. Purpose and Scope. State purpose and scope of plan.

2. Area Security. Define the areas, buildings, and other structures considered critical and establish priorities for their protection.

3. Control Measures. Define and establish restrictions on access and movement into critical areas. These restrictions can be categorized as to personnel, material and vehicles.

   a. Personnel Access.

      (1) Establish controls pertinent to each area or structure.

         (a) Authority for access.

         (b) Access criteria for:

            (I) Unit personnel.

            (II) Visitors.

      (2) Identification and Control.

         (a) Describe the system to be used in each area. If a badge system is used, include display requirements, identification and control procedures, standards for passes and badges, etc.

         (b) Describe who the system applies to.

            (I) Unit personnel.

            (II) Visitors to restricted areas.

            (III) Visitors to non-restricted areas.

            (IV) Vendors, tradesmen, etc.

            (V) Contractor personnel.

            (VI) Maintenance or support personnel.

            (VII) Emergency response personnel.

b. Material Control.

(1) Incoming.

(a) Requirements for admission of material and supplies.

(b) Search and inspection of material for possible sabotage hazards.

(c) Special controls on delivery of supplies and/or personal shipments in restricted areas.

(2) Outgoing.

(a) Documentation required, e.g., property pass.

(b) Controls, as outlined in (1) (a), (b) and (c), above.

c. Vehicle Control.

(1) Policy on search of government and privately owned vehicles.

(2) Parking regulations/restrictions.

(3) Controls for entrance into restricted and non-restricted areas.

(a) Privately owned vehicles.

(b) Government vehicles.

(c) Emergency vehicles.

(d) Commercial vehicles.

d. Vehicle Registration.

4. Aids to Security. Indicate the manner in which the following listed aids to security will be implemented on the unit.

a. Protective barriers.

(1) Definition.

(2) Clear zones.

(a) Criteria.

(b) Maintenance.

(3) Signs.

(a) Types.

(b) Posting.

(4) Gates.

(a) Hours of Operation.

(b) Security requirements.

(c) Lock security.

b. Protective Lighting System.

(1) Use and control.

(2) Inspection.

(3) Action to be taken in the event of commercial power failure.

(4) Action to be taken in the event of a failure of alternate source of power.

(5) Emergency lighting systems.

(a) Stationary.

(b) Portable.

c. Intrusion Detection Systems.

(1) Testing.

(2) Inspection.

(3) Use and monitoring.

(4) Action to be taken in event of "alarm" conditions.

(5) Maintenance.

(6) Alarm logs or registers.

(7) Sensitivity settings.

(8) Fail-safe and tamper-proof provisions.

(9) Monitor panel location.

(10) Areas protected.

d. Communications (primary and alternate sources).

(1) Locations.

(2) Use.

(3) Tests.

(4) Authentication.

(5) Emergency communications.

5. Security Forces. Include general instructions that would apply to all security force personnel. Detailed instructions such as Special Orders and SOPs should be attached as annexes. An SOP should be written for each post.

a. Composition and organization.

b. Authority and jurisdiction.

c. Tour of duty.

d. Essential posts and routes.

e. Weapons and equipment.

f. Training.

g. Use of sentry/patrol dogs.

h. Emergency Response Force.

(1) Composition.

(2) Mission.

(3) Weapons and equipment.

(4) Location.

(5) Deployment concept.

6. Contingency Plans. Indicate required actions in response to various emergency situations. Detailed plans such as Unit specific Threatcon Measures, bomb threats, hostage negotiation, natural disaster, fire, hurricanes, earthquakes, mass casualties etc., should be attached as annexes.

a. Individual actions.

b. Emergency Response Force actions including casualty evacuation.

c. Security Force actions.

7. Use of Air Surveillance.

8. Coordinating Instructions. Indicate matters which require coordination with other agencies including any mou/moa's in place.

a. Integration with plans of host or nearby military installations.

b. Liaison and coordination.

(1) Local and state authorities.

(2) Federal agencies.

(3) Military organizations.

Annexes (as appropriate):

A – Intelligence including Threat Assesment

B - Unit Security Status Map

C - Key and Lock Control Procedures

D - Contingency Plans

E - Special Instructions to Security Force and Officers of the day

F - Special Orders for Guard Posts.

G - AA&E Security

H – Robbery Prevention Plan

I – Loss Prevention Plan

J – Bomb Threat/Incident Plan

K – Coast Guard Exchange System tenant activities Security Plans

L – Vulnerability Assesment

PHYSICAL SECURITY CHECKLIST

UNIT _____ **DATE** _____

CSO _____ **EVALUATOR** _____

PART I . PROGRAM IMPLEMENTATION	**REF PARA**	**YES**	**NO**
1. Does the unit hold the current Physical Security Manual and changes?		[ ]	[ ]
2. Has a Command Security Officer (CSO) been designated in writing?	1.C.2	[ ]	[ ]
3. Have biennial evaluations of subordinate units been conducted?	1.D.2.h	[ ]	[ ]
Date of last evaluation _____			
4. Have any waivers or exceptions been granted?	1.E	[ ]	[ ]
5. Has a Physical Security Plan been developed?	1.F	[ ]	[ ]
6. Is the plan reviewed and updated annually?	1.F	[ ]	[ ]

Comments: _____

_____

_____

PART II . PHYSICAL PROTECTION MEASURES	**REF PARA**	**YES**	**NO**
Section A . Restricted Areas			
Does the unit have any restricted areas? (If "NO" skip to next section)		[ ]	[ ]
List Areas:			
_____			
_____			
_____			
1. Have restricted areas been designated in writing by a SECMGR?	2.B.1.b	[ ]	[ ]
2. Do restricted areas have a clearly defined and protected perimeter?	2.B.2.d	[ ]	[ ]
3. Do restricted areas use personnel identification and control systems, including access lists and entry/departure logs when required?	2.B.2.d	[ ]	[ ]
4. Are perimeters and points of entry posted with the required signs?	2.B.2.d	[ ]	[ ]
5. Are entry/exit points controlled by guards or cleared personnel?	2.B.2.d	[ ]	[ ]
6. Are periodic checks conducted by security/police force personnel?	2.B.2.d	[ ]	[ ]
7. Are administrative inspections conducted?	2.B.2.e	[ ]	[ ]

Comments: _____

_____

Section B . Physical Barriers	REF PARA	YES	NO
1. Is the perimeter of the unit clearly defined and posted?	2.C.1.c	[ ]	[ ]
2. Are water boundaries adequately protected?	2.C.4.d	[ ]	[ ]
3. Do fences meet the minimum standards?	2.C.5	[ ]	[ ]
4. If building walls and roofs form a part of the perimeter barrier, do they provide a degree of security equivalent to chain link fencing?	2.C.6	[ ]	[ ]
5. Are appropriate clear zones maintained?	2.C.8	[ ]	[ ]
6. Are security barriers inspected at least monthly?	2.C.10	[ ]	[ ]
7. Are gates locked when not in use and frequently inspected?	2.C.12.b	[ ]	[ ]
8. Are locks rotated or rekeyed at least annually?	2.C.12.b	[ ]	[ ]
9. Are openings (in restricted areas) greater than 90 square inches properly protected?	2.C.13 & 14	[ ]	[ ]
10. Are utility poles, signboards, trees at least 14' away from the perimeter?	2.C.15	[ ]	[ ]
11. Are warning signs appropriately posted?	2.C.16	[ ]	[ ]
12. Are exterior signs legible from 50' during daylight?	2.C.16.h	[ ]	[ ]

Comments: _____

Section C . Protective Lighting	REF PARA	YES	NO
Does the unit use any protective lighting? (If “NO” skip to next section)		[ ]	[ ]
1. Is the concept of glare projection used?	2.D.3.a.(1)	[ ]	[ ]
2. Is lighting checked daily for proper operation and are defective lights immediately reported?	2.D.6.a	[ ]	[ ]
3. Are restricted areas sufficiently illuminated?	2.D.6.b	[ ]	[ ]
4. Are gates/exterior doors sufficiently illuminated?	2.D.6.d & e	[ ]	[ ]
5. Is emergency power supplied to lighting in restricted areas?	2.D.7	[ ]	[ ]
6. Are battery powered lights available?	2.D.7	[ ]	[ ]
7. Are emergency power systems tested monthly and a record retained for 1 year?	2.D.7	[ ]	[ ]
8. Is protective lighting independent of the unit's primary lighting or power system?	2.D.8.a	[ ]	[ ]
9. Are controls and switches for protective lighting located inside the protected area and locked or guarded at all times?	2.D.8.b	[ ]	[ ]

Comments: _____

_____

Section D . Intrusion Detection Systems	**REF PARA**	**YES**	**NO**
Does the unit have any installed Intrusion Detection Systems? (If "NO" skip to next section)		[ ]	[ ]
1. Is the IDS supported by a prompt security/police force response?	2.E.1	[ ]	[ ]
2. Are signal transmission lines constantly monitored at one central annunciator?	2.E.3.c	[ ]	[ ]
3. Does the IDS incorporate fail-safe features that alert for abnormal operating conditions?	2.E.3.e	[ ]	[ ]
4. Does the IDS incorporate tamperproof features?	2.E.3.f	[ ]	[ ]
5. Are balanced magnetic switches used on doors?	2.E.4.a	[ ]	[ ]
6. Does the IDS have line supervision?	2.E.4.b	[ ]	[ ]
7. Does the backup power source sustain the system for 4 hours?	2.E.4.c	[ ]	[ ]
8. Are on/off switches located within the protected area?	2.E.4.d	[ ]	[ ]
9. Are emergency power sources tested monthly and a record retained for 1 year?	2.E.6.a	[ ]	[ ]
10. Is repair maintenance service available on a 24 hour basis?	2.E.6.c.(2)	[ ]	[ ]
11. Are IDS plans and diagrams properly marked and protected?	2.E.6.d	[ ]	[ ]
12. Are alarm history records retained for 1 year?	2.E.7.d	[ ]	[ ]
13. Are identity verification/duress codes used?	2.E.7.e	[ ]	[ ]
14. Are they properly marked, protected, and changed semi-annually?	2.E.7.e.(4)	[ ]	[ ]
15. Are IDS and duress systems tested monthly and the record retained for 1 year?	2.E.8.a	[ ]	[ ]
16. Is periodic testing conducted to test security force response time?	2.E.8.b	[ ]	[ ]

Comments: _____

_____

_____

_____

_____

_____

_____

Section E . Key and Lock Control	**REF PARA**	**YES**	**NO**
Does the unit use any security locks? (If "NO" skip to next section)		[ ]	[ ]

1. Has a key and lock control system been established?	2.F.2.a	[ ]	[ ]
2. Has a key control officer been designated in writing?	2.F.2.c	[ ]	[ ]
3. Are locking devices inspected after hours?	2.F.2.f.(3)	[ ]	[ ]
4. Is the number of personnel authorized to draw/retain keys kept to a minimum?	2.F.4.a	[ ]	[ ]
5. Are keys properly stored in a 20 gauge steel container and secured to the structure?	2.F.4.e	[ ]	[ ]
6. Is the repository locked & under surveillance during working hours?	2.F.4.e	[ ]	[ ]
7. Is an index maintained for each repository?	2.F.4.g	[ ]	[ ]
8. Are separate registers used for each repository?	2.F.4.h.	[ ]	[ ]
9. Are registers maintained for 6 months after final entry?	2.F.4.h	[ ]	[ ]
10. Are semiannual inventories conducted by serial number and records maintained?	2.F.4.k	[ ]	[ ]
11. Are padlocks rotated or rekeyed at least annually?	2.F.4.l	[ ]	[ ]
12. Are Grand Master keys appropriately protected and stored?	2.F.5.b	[ ]	[ ]
13. Are locks immediately replaced in the event of lost, misplaced, or stolen keys?	2.F.6	[ ]	[ ]

Comments: _____

_____

_____

Section F . Security Containers	**REF PARA**	**YES**	**NO**
Does the unit have any security containers? (If "NO" skip to next section)		[ ]	[ ]
1. Are combinations to all security containers changed as required?	2.G.1	[ ]	[ ]
2. Is the SF 700 used and appropriately stored?	2.G.2	[ ]	[ ]
3. Is an SOP affixed to the outside of the container?	2.G.2	[ ]	[ ]
4. Is the SF 701 used and retained for 3 months?	2.G.3	[ ]	[ ]
5. Is the SF 702 used and retained for 3 months?	2.G.4	[ ]	[ ]

Comments: _____

_____

_____

Section G . Visitor Control	**REF PARA**	**YES**	**NO**
1. Has a visitors bill been developed?	2.H.2	[ ]	[ ]
2. Are reports being properly submitted for incidents of visitors who express an unusual or persistent interest in classified or otherwise sensitive information?	2.H.3	[ ]	[ ]

Comments: _____

_____

_____

Part III . ARMS, AMMUNITION AND EXPLOSIVES	**REF PARA**	**YES**	**NO**
Does the unit hold any AA&E? (If "NO" skip to next section)		[ ]	[ ]
1. What categories of Arms are stored at the unit?	3.G.1	I II	III IV
2. What categories of A&E are stored at the unit?	3.G.2	I II	III IV
3. Are privately-owned weapons properly stored at the unit?	3.A	[ ]	[ ]
4. Have any AA&E waivers or exceptions been granted?	3.D	[ ]	[ ]
5. Has the unit issued appropriate written policies to cover all phases of AA&E security, including armed response forces?	3.F.2	[ ]	[ ]
6. Is access to AA&E storage areas limited only to designated persons and an access list posted inside the area?	3.I.1	[ ]	[ ]
7. If more than one unit stores weapons in the same area, are the weapons properly segregated?	3.I.2	[ ]	[ ]
8. Are keys to AA&E storage areas and IDSs maintained separately from other keys, and limited to only those names appearing on the access list?	3.J.1	[ ]	[ ]
9. Are keys to AA&E storage areas properly protected when unattended?	3.J.1.b	[ ]	[ ]
10. Has an AA&E key control officer been designated in writing?	3.J.2	[ ]	[ ]
11. Are key control registers retained for 6 months?	3.J.3	[ ]	[ ]
12. Is an armed security/police force capable of responding to an IDS alert within 15 minutes?	3.L.2	[ ]	[ ]
13. Are security/police response personnel provided with efficient primary and backup communications equipment?	3.L.3	[ ]	[ ]
14. Are AA&E storage areas designated as restricted areas and posted?	3.M.1	[ ]	[ ]
15. Is fencing used to protect AA&E?	3.N	[ ]	[ ]
16. Is protective lighting provided as required?	3.O	[ ]	[ ]
17. Are Category I - IV arms properly stored?	3.P.1	[ ]	[ ]
18. Are Category I and II arms supported by an IDS or live watch?	3.P.1	[ ]	[ ]
19. Are containers on casters or those weighing less than 500 pounds secured to the structure?	3.P.2	[ ]	[ ]
20. Are Arms Racks properly maintained and secured?	3.P.3	[ ]	[ ]
21. Is AA&E stored in non-Coast Guard environments?	3.P.4	[ ]	[ ]
22. If so, has a written support agreement/MOU been established?	3.P.4.a	[ ]	[ ]

23. Are receipts and proper physical security maintained?	3.P.4.b	[ ]	[ ]
24. Are A&E properly stored in an approved container or magazine?	3.Q.1	[ ]	[ ]
25. Do armories meet the required construction specifications?	3.R	[ ]	[ ]
26. Do Weapons Spaces meet the required specifications?	3.S	[ ]	[ ]
27. Do shipboard doors and hatches meet the required standards?	3.T	[ ]	[ ]

Comments: _____

_____

_____

_____

PART IV . TECHNICAL SECURITY COUNTERMEASURES	**REF PARA**	**YES**	**NO**
1. Does the unit <u>require</u> the utilization of TSCM?	4	[ ]	[ ]
2. Have any of the units spaces been surveyed?	4	[ ]	[ ]
3. Have survey discrepancies been corrected?	4	[ ]	[ ]

Comments: _____

_____

_____

PART V . SECURITY THREAT CONDITIONS	**REF PARA**	**YES**	**NO**
1. Are the CO, CSO and security/police force personnel continually aware of the counterterrorism threat condition levels?	5	[ ]	[ ]
2. Has the unit generated local procedures adapting the THREATCON measures to meet local command structure and operational environment?	5.B.3	[ ]	[ ]
3. Has liaison been established with local, state, and federal law enforcement agencies whereby early warning of a threat situation will be provided?	5.B.4	[ ]	[ ]

Comments: _____

_____

_____

PART VI . FUNDS FACILITIES	**REF PARA**	**YES**	**NO**
Does the unit have any funds handling or storage areas? (If "NO" skip to next section)		[ ]	[ ]
1. Have dedicated funds storage/handling areas been designated as restricted areas?	6.A.3	[ ]	[ ]
2. Have command specific control, safeguarding and emergency procedures been developed and published?	6.B.1.c & d	[ ]	[ ]
3. Are funds stored in the required container in a locked room?	6.E.1	[ ]	[ ]

4. Are funds stored in the same container as prohibited material?	6.E.3.a	[ ]	[ ]
5. Are containers on casters or those weighing less than 500 pounds secured to the structure?	6.E.3.b	[ ]	[ ]
6. Are storage containers illuminated as appropriate?	6.E.3.c	[ ]	[ ]
7. Are storage container records properly used and maintained?	6.E.4	[ ]	[ ]
8. Are recorded money packs (for ashore units) kept in security containers for funds in excess of $2K?	6.F	[ ]	[ ]
9. Is the record stored in a separate container?	6.F.2	[ ]	[ ]
10. Is the combination/key envelope appropriately stored in a GSA approved container?	6.G.1	[ ]	[ ]
11. Are the combinations and keys to containers changed as required?	6.G.3 & 4	[ ]	[ ]
12. Is security lighting adequate?	6.H	[ ]	[ ]
13. If an IDS is used, are warning signs posted?	6.I.1	[ ]	[ ]
14. Are escorts or a contract armored car service used for funds transport?	6.J.1	[ ]	[ ]
15. Are routes and times of funds transport detail's departure varied?	6.J.3	[ ]	[ ]
16. Are Penalty Postage Meters being properly safeguarded?	6.K	[ ]	[ ]
17. Are Government Credit Cards being properly safeguarded?	6.L	[ ]	[ ]
18. Are Travelers Checks being properly safeguarded?	6.M	[ ]	[ ]
19. Does the Physical Security Plan include a robbery plan that is coordinated with local law enforcement agencies and/or host facility?	6.N.1	[ ]	[ ]
20. Is the plan tested annually for funds in excess of $2K?	6.N.3	[ ]	[ ]
21. Is annual robbery prevention training presented to funds handlers?	6.N.4	[ ]	[ ]

Comments: _____

_____

_____

_____

_____

PART VII . PRIVATE MOTOR VEHICLE REGISTRATION	**REF PARA**	**YES**	**NO**
Does the unit issue or require the CG-4801 for access? (If "NO" skip to next section)		[ ]	[ ]
1. Has the unit been properly designated as an Issuing Authority?	7.C.2	[ ]	[ ]
2. Does the unit issue the CG-4801 only to those personnel accessing their facilities?	7.C.4	[ ]	[ ]
3. Are POVs properly registered?	7.D	[ ]	[ ]
4. Are decals and expiration tabs properly displayed?	7.D.9	[ ]	[ ]

5. Are records of issued decals retained for 4 years from date of initial issue or 1 year after expiration?	7.F.1	[ ]	[ ]
6. Are unissued decals inventoried (by an individual with no direct interest) annually and a record retained for 1 year?	7.F.1	[ ]	[ ]
7. Are unissued decals and expiration tabs stored in a locked container of at least 12 gauge steel?	7.F.2	[ ]	[ ]

Comments: _____

_____

_____

_____

_____

PART VIII . SECURITY IDENTIFICATION BADGE SYSTEM	**REF PARA**	**YES**	**NO**
Does the unit issue or require the CG-5439 for access? (If "NO" skip to next section)		[ ]	[ ]
1. Is CG-5439 used as the security identification badge?	8.A	[ ]	[ ]
2. Is CG-5439E used for visitors?	8.A	[ ]	[ ]
3. Are badges properly worn by personnel?	8.C.3	[ ]	[ ]
4. Is CG-5448 properly safeguarded and retained by the CSO?	8.E.3	[ ]	[ ]
5. Are records of issued badges retained for 4 years?	8.F.1	[ ]	[ ]
6. Are unissued badges inventoried annually and a record retained for 1 year?	8.F.1	[ ]	[ ]
7. Are unissued badges stored in a locked container of at least 12 gauge steel?	8.F.2	[ ]	[ ]
8. Are badges returned to the CSO upon transfer from the unit?	8.F.3	[ ]	[ ]
9. Is the CSO immediately notified of a lost or stolen badge?	8.F.3	[ ]	[ ]

Comments: _____

_____

_____

PART IX . LOSS PREVENTION	**REF PARA**	**YES**	**NO**
1. Is a Loss Prevention Program in effect?	9.A	[ ]	[ ]
2. Does the Physical Security Plan include loss prevention measures?	9.C.1.d	[ ]	[ ]
3. Are losses properly reported?	9.D.2	[ ]	[ ]
4. Are reports of recovery sent to all addresses initially notified of the loss?	9.D.3	[ ]	[ ]
5. Are AA&E losses reported in accordance with COMDTINST M8370.11, Small Arms Manual?	9.D.6	[ ]	[ ]
6. Are proper inventory controls established?	9.G	[ ]	[ ]

7. Are random inspections conducted and the results submitted to the Commanding Officer?	9.H	[ ]	[ ]

Comments: _____

_____

_____

PART X . SECURITY/POLICE FORCES	REF PARA	YES	NO
Does the unit have a security/police force? (If "NO" skip to next section)		[ ]	[ ]
1. Is the security/police force responsible to the CSO/CP?	10.C.4 & 5	[ ]	[ ]
2. Has appropriate authority been established?	10.G	[ ]	[ ]
3. What type of jurisdiction has been established? _____	10.H.2		
4. Are security/police force standing orders published and signed by the current CO?	10.J	[ ]	[ ]
5. Do security/police force personnel meet the general qualifications?	10.K	[ ]	[ ]
6. Are contract guard services coordinated with the SECMGR?	10.K.7	[ ]	[ ]
7. Are other means of communication used to supplement the supervision of the security/police force?	10.M	[ ]	[ ]
8. Are the number and type of posts sufficient?	10.N	[ ]	[ ]
9. Is the present security force strength and composition commensurate with the degree of security protection required?	10.Q	[ ]	[ ]
10. Does the unit have an auxiliary security/police force?	10.S	[ ]	[ ]
11. Do personnel have the required security investigation?	10.T	[ ]	[ ]
12. Do personnel wear the required type of uniform?	10.U.1.b	[ ]	[ ]
13. Are ball caps and collar insignias properly worn?	10.U.2 & 4	[ ]	[ ]
14. Are patches and badges of the standard type?	10.V.1	[ ]	[ ]
15. Are patches properly worn?	10.V.3	[ ]	[ ]
16. Do police personnel carry the badge and credential at all times?	10.V.4	[ ]	[ ]
17. Are badges and credentials being used only for official business?	10.V.5	[ ]	[ ]
18. Are lost badges or credentials immediately reported to the CSO/CP?	10.V.6	[ ]	[ ]
19. Do personnel receive a basic course of instruction?	10.W.2.a – c	[ ]	[ ]
20. Do personnel receive periodic/in service training?	10.W.2 & 3	[ ]	[ ]
21. Do personnel maintain the required equipment?	10.X.1	[ ]	[ ]
22. Is the "high level of retention" holster used?	10.X.5	[ ]	[ ]
23. Do personnel carry weapons?	10.Y	[ ]	[ ]

24. Are the proper reports promptly made anytime a weapon is drawn or discharged?	10.Y.2	[ ]	[ ]
25. Is Use of Force and General Weapons Policy being appropriately applied by security/police force personnel?	10.Z Exhibit 10-3 Enclosure (6)	[ ]	**[ ]**
26. Are Body Searches of persons being appropriately conducted?	10.AA	[ ]	**[ ]**
27. Do patrol vehicles comply with Federal Standard 122?	10.BB.1	[ ]	[ ]
28. Are patrol vehicles distinctively marked and do they contain the required equipment?	10.BB.2 & 3	[ ]	[ ]
29. Is the communication system sufficient for operations?	10.DD.1 & 2	[ ]	[ ]
30. Does it include the required frequencies?	10.DD.3	[ ]	[ ]
31. Are the required tests/inspections conducted of circuits and equipment to ensure proper operation and records maintained?	10.DD.5 & 6	[ ]	[ ]
32. Has an evidence custodian and alternate been designated in writing?	10.EE.2	[ ]	[ ]
33. Is evidence properly stored and access strictly limited?	10.EE.4 & 5	[ ]	[ ]
34. Are security/police force documents, records, and files appropriately maintained and properly disposed of after required retention periods?	10.FF	[ ]	[ ]

Comments: _____

_____

_____

_____

_____

_____

_____

_____

PART XI . CONTROLLED MEDICAL SUBSTANCES	**REF PARA**	**YES**	**NO**
Does the unit handle or store any controlled medical substances? (If “NO” skip to next section)		[ ]	[ ]
1. Have dedicated controlled medical substance storage/handling areas been designed as restricted areas?	11.A.1	[ ]	[ ]
2. Are controlled medical substances stored in the required container in a locked room?	11.B.2 & 3	[ ]	[ ]
3. Are controlled medical substances stored in the same container as prohibited material?	11.B.4	[ ]	[ ]
4. Are containers on casters or those weighing less than 500 pounds secured to the structure?	11.B.6	[ ]	[ ]

5. Are storage container records properly used and maintained?	11.B.7 & 8	[ ]	[ ]

Comments: _____

_____

_____

_____

PART XII . BOMB THREATS	REF PARA	YES	NO
1. Does the unit's Physical Security Plan include a Bomb Threat/Incident Plan?	12.C	[ ]	[ ]
2. Is the plan available for use by all supervisors and key personnel?	12.C	[ ]	[ ]
3. Are mail handling personnel able to recognize letter bombs?	12.C.2.e	[ ]	[ ]
4. Does the plan include the following:			
a. Activation of a command post?	12.C.4	[ ]	[ ]
b. Emergency communications plan?	12.C.4	[ ]	[ ]
c. Predesignated routes of evacuation?	12.C.4	[ ]	[ ]
d. Predesignated safety perimeters around all buildings?	12.C.4	[ ]	[ ]
e. Predesignated evacuation re-assembly areas 300 feet from affected areas and buildings?	12.C.4	[ ]	[ ]
f. Plan for notification of surrounding commands/activities?	12.C.4	[ ]	[ ]
g. Search procedures for occupied and evacuated buildings?	12.C.4	[ ]	[ ]
5. Is a form similar to the Telephonic Bomb Threat Report used?	12.D	[ ]	[ ]
6. Does the command plan identify temporary morgue facilities?	12.E	[ ]	[ ]
7. Does the command plan have designated hospitals and ambulance services?	12.E	[ ]	[ ]
8. Does the command conduct bomb threat planning/drills periodically?	12.K	[ ]	[ ]
9. Is training provided to command personnel (non-security) in the handling of bomb threats/incidents?	12.K	[ ]	[ ]
10. Is training provided to security force personnel in the handling of bomb threats/incidents?	12.K	[ ]	[ ]
11. Does the command conduct joint training with outside agencies that may be called upon to assist during a bomb threat/incident?	12.K	[ ]	[ ]

Comments: _____

_____

_____

Overall Comments: _____

PRELIMINARY INFORMATION FOR TSCM SECURITY REVIEW

A. Here is a list of preliminary information required for a comprehensive physical/technical security review by our staff as related to chapter 4.

1. Requests must include, as a minimum, the following facility information:

a. Complete identification of the area requiring TSCM support, to include:

(1) Name of the area

(2) Room number

(3) Building number

(4) Address

(5) Floor plan

(6) Electrical and telephone wiring diagrams.

(7) Air conditioning and heating duct diagrams.

(8) "As built" construction blueprints.

(9) List of adjacent tenants, bordering the entire perimeter of the area to be inspected (including those above and below).

(10) Square footage of the area.

b. Identity and telephone number of the command point of contact and an alternate.

c. Clearance requirements for the TSCM support personnel.

d. Date of last TSCM report and the status of previous recommendations provided, if any.

e. Information that may impact on the scheduling, i.e., date scheduled construction will commence, completion date of construction in progress, etc. Should unexpected events which could interfere with a TSCM survey occur after support has been scheduled, the requester should notify the program manager as soon as possible to prevent unnecessary expenditures of manpower and funds.

2. What follows is a detailed list of required information to be sent to (G-CFI) prior to a comprehensive survey.

   a. Architectural Drawings

   b. Assembly Drawings

   c. Detail Drawings

   d. Section drawings

   e. Bill of Materials and Specifications

   f. Mechanical Drawings

   g. Floor Plans

   h. Electrical Drawings, and

   i. Site Plan

   j. "As Built" Drawings

3. These drawings should detail both Services and Equipment as follows:

   a. Electrical services & equipment.

   b. Gas services & equipment

   c. Plumbing services & equipment

   d. Sewage/Drainage system service and equipment

   e. Heating service and equipment

   f. Ventilation & Air conditioning (HVAC) service and equipment

   g. Telephone & Telecommunication service and equipment

   h. TV & Video cable system service and equipment

   i. Intrusion Detection System (IDS) alarm service and equipment

   j. Fire alarm & safety service and equipment

4. Copies of the following administrative paperwork:

a. Standard Operating Procedure (SOP)

b. Emergency Action Plan (EAP).

c. Information Security Plan (May be part of SOP).

d. Security Servicing Agreements.

e. Physical Security Plan and Physical Security Checklist

f. Latest copy of the SECMGR security inspection report.

g. Unit/Facility telephone book

h. Basic emergency egress/evacuation Floor Plan.

i. Automated Information System (AIS) security plan.

j. Any and all facility accreditation paperwork for any system or equipment located within the facility.

k. Provide a copy of all administrative waivers/exceptions needed for each facility requiring the waiver/exception.

5. In addition, either ensure the following items are clearly identified in the above information package, and/or provide a brief description as needed:

a. A basic "block diagram" outlining the perimeter of each "Physically Protected Space" (PPS) and or "classified space".

b. A brief description of the following for each space to be evaluated:

(1) Identify highest classification level of material either discussed, displayed or stored in space.

(2) Identify whether "open" or "closed" storage is authorized.

(3) Identify physical locks and locking devices used to protect proprietary/sensitive/classified material/space.

(4) Identify/List the technical specifics of IDS equipment.

(5) Identify all computer/telephone/IDS systems within the PPS.

(a) Include technical information on Operating System. (Including software version numbers)

(b) Include Wiring diagrams of PBX/LAN/WAN for AIS or telephone systems. (Including unclassified AIS systems)

(c) Briefly describe the purpose/mission for each room/office/space.

c. Provide a local detailed (scaled down) "road map" showing the location of the facility to be reviewed. Include any areas of interest that may be of concern or threat. (Internal & or External)

d. Provide a basic "block diagram" of the entire facility, showing specifically the location of the external boarder/fence-line to public areas. Also include the following items on this diagram:

(1) Identify where the facility plant electrical/phone/power/IDS and other wires that enter/egress the facility and each specific "classified" space to be reviewed.

(2) Identify points of entry/exit for personnel. Include brief description of current policy for access controls in place.

(3) Identify common barriers/walls and identify who, externally share these common walls?

(4) Identify PPS's on your overall facility floor plan.

(5) List the percentage of classified/sensitive discussions likely to take place in each room/area for each classification level.

(6) Identify areas where classified/sensitive information is stored.

B. Obviously, putting together this amount of information will take time. It may be wise to plan ahead when thinking about requesting services.

C. In order to facilitate the security review teams time "on-site" and to improve the security review teams over-all effectiveness, we require as much information as you can possibly muster and as much lead-time as you can possibly give.

D. In order to avoid OPSEC concerns when associated with the timing and location of the teams arrival, adhere to guidance provided in chapter 4. Discussions and purpose for collection of the above information should not be associated with the pre-planned arrival of a security review team.

E. Adhere to the "classification guidance" outlined in chapter 4 while collecting the above information. Just by compilation, the information you gather is "sensitive" and may even be considered classified. Classification will depend upon the "guide" you use and by the information's association with the security review teams arrival.

F. Please avoid telling other personnel the real reason why you are collecting this information. The true knowledge of why you're collecting the above information should remain limited to a "need to know" basis, particularly when the teams arrival is expected soon.

APPROVED LOCKING DEVICES FOR AA&E STORAGE

NOMENCLATURE	NSN	MIL-SPEC
HIGH SECURITY LOCKS		
S&G 833C	5340-00-799-8248	MIL-P-43607
S&G 831B	5340-01-188-1560	MIL-P-43607
HI SHEAR LK1200	5340-00-799-8248	MIL-P-43607
TUFLOC 60-1XR	5340-00-144-7310	(none)
TUFLOC 60-2XR R.H.	5340-00-144-7311	(none)
TUFLOC 60-2XR L.H.	5340-00-145-0293	(none)
TUFLOC 60-3XR	5340-00-144-7359	(none)
HIGH SECURITY HASPS		
MARK II MOD VIII (NAPEC)	5340-01-196-2547	MIL-H-29181
MARK II MOD IX (NAPEC)	5340-01-235-6907	MIL-H-29181
1300 SERIES-RIGID	5340-01-281-7938	MIL-H-24653
1300 SERIES-HINGED	5340-01-282-8275	MIL-H-24653
NATICK	(various)	(various)
MEDIUM SECURITY LOCKS		
S&G 826D	5340-00-799-8016	MIL-P-43951
LOW SECURITY (SECONDARY) LOCKS		
Padlock without chain, steel case and shackle	5340-00-158-3805*	A-A-1927D
Padlock with chain, steel case and shackle	5340-00-158-3807*	A-A-1927D

*Note: Other padlocks that meet MIL-P-17802D are also acceptable.

USE OF FORCE AND GENERAL WEAPONS POLICY FOR COAST GUARD SECURITY AND POLICE FORCES

A. Use of Force. This enclosure prescribes a uniform use of force and weapons policy for Coast Guard security and police forces.

1. General.

a. There are varying degrees of force that may be justified in a law enforcement situation depending upon the gravity of the situation. However, the escalation of force by an officer must be consistent with the need for the lowest level of force required to effect the apprehension of a suspect or stop the particular criminal conduct.

b. In an enforcement situation, officers may use only that level of force necessary to control and terminate unlawful resistance, and to preclude any further physical confrontation against law enforcement personnel or other persons.

c. Besides self-defense, the use of this policy may arise in three USCG security roles:

(1) as a law enforcement agency;

(2) as the custodian responsible for the security of government property; and

(3) during peacetime as a branch of the armed forces, except when otherwise directed.

d. These roles may overlap in any given situation. Use of force is a sensitive issue and, like the exercise of any law enforcement authority, should be undertaken with caution and circumspection. This should not be construed as limiting the taking of quick action or using such force as is necessary to defend or protect one's self or others. Reckless, careless, or unnecessary use of force is never permitted.

2. Definitions. The following definitions apply to this section (and to any references to the use of force throughout this manual):

a. "Felony" means any crime which is punishable by imprisonment for more than one year or by death.

b. "Misdemeanor" means any crime other than a felony.

c. "Non-deadly force" means any force other than deadly force.

d. "Self-defense" means the act of defending one's self or another person from harm by using force.

e. "Deadly force" means any force which is intended to cause death, or which creates a substantial risk of death or serious bodily injury; Exhibit 10-3 is a use of deadly force summary.

f. "Serious bodily injury" means actual physical injury to the body that results in: (a) unconsciousness; (b) protracted and obvious disfigurement; or (c) protracted loss or impairment of the function of a bodily member, organ, or mental faculty.

g. "Military situation" is one involving any action by a foreign military or subversive force which intentionally poses a clear and present danger to the security of the United States or any of its forces, territories, or possessions. The hostile forces must use, have used, or threaten to use deadly force.

h. "Foreign military or subversive force" includes foreign military or governmental units and the operations of organized paramilitary or terrorist elements sponsored by a foreign government.

i. "Standing Rules of Engagement (SROE)" provides implementation guidance on the inherent right of self-defense and the application of force for mission accomplishment. SROE were promulgated by the National Command Authorities (NCA) to the Unified Commanders (CINCs) and adopted by the Coast Guard.

3. General USCG Use of Force Policy. Only such force as is reasonably necessary under the circumstances may be used. Excessive force may never be used. Normally, deadly force is only appropriate in meeting deadly force or dealing with a crime involving the use of, or threatened use of deadly force. Force shall not be used where assigned duties can be discharged without it. Even when use of force is permitted, the force used must be limited to the minimum necessary and must be designed to achieve the desired result with minimum injury to persons and property. Even when concurrence from higher authority is not required, if time and circumstances permit, consultation with superiors before using force is encouraged. However, when prompt action is necessary, personnel are expected to make appropriate use of force decisions in a timely manner according to their own best judgment without prior consultation with higher authority. Consistent with the foregoing, use of force is permissible in the following circumstances:

a. for self-defense (including defense of others);

b. to prevent a federal crime, or where authorized, a serious state or foreign crime;

c. to effect a lawful arrest;

d. to protect property that USCG personnel have the authority to protect; and

e. to compel compliance with an order the USCG has authority to issue.

NOTE: More than one of the above grounds for using force may be available in any particular situation since they overlap.

4. Minimum Force Necessary. This phrase means that while USCG personnel are enforcing laws or regulations, they may use the minimum amount of force necessary to enforce those laws and regulations. This includes the use of deadly force when authorized in accordance with this policy.

5. No Duty to Retreat. USCG personnel performing law enforcement activities do not have a duty to retreat. However, while USCG personnel are not required to retreat to avoid situations justifying the use of force, including deadly force, retreat is an alternative and in some cases may be the most reasonable decision under the circumstances.

6. Military Situations. The use of force policy for military situations is contained in the standing rules of engagement (SROE). Standing ROE are an application of the right of self-defense, but they can be less restrictive than self-defense rules in non-military incidents. The applicable rules of engagement for USCG units are promulgated by the USCG Area Commanders based upon those promulgated by the Joint Chiefs of Staff. The determination of when a military situation exists rests with the senior commissioned officer in command on-scene. If there is reasonable doubt that a military situation exists, it shall be treated as a non-military incident and the USCG Use of Force Policy will apply.

7. Prevention of a Crime. Non-deadly force may be used to prevent the commission of a misdemeanor only if the crime involves the intentional use of force. Deadly force may be used to prevent the commission of a felony, which if not prevented, would pose an imminent threat of death or serious bodily injury to any person.

8. Effecting an Arrest. Use of force to arrest or to prevent an escape is limited to federal crimes, unless (a) the member has additional arrest authority for the particular crime, or (b) the member is acting at the direction of someone who has arrest authority for the crime. Reasonable non-deadly force may be used to arrest or to prevent the escape of a suspect when there is probable cause that the suspect committed a crime. As a last resort, deadly force may be used after the suspect

has failed to obey an order to halt, only if:

a. the use of deadly force does not create any undue risk to others; and

b. there is probable cause that the suspect has committed a crime involving the use or threatened use of deadly force; and,

c. you know that the suspect is armed, or otherwise poses a substantial threat - whether or not imminent - of death or serious bodily injury to any person.

9. Warning Shots - Prohibited. A warning shot, as practiced by the USCG, is a signal not a use of force. In view of the higher risk of hitting unintended targets, the firing of warning shots is generally prohibited over land. Warning shots for crowd control are not authorized. Warning shots fired by land based law enforcement or security personnel using personal defense weapons are prohibited.

10. Disabling Fire - Prohibited. Disabling fire, as practiced by the USCG, does not constitute the use of deadly force. Such fire is a special method of stopping a vessel. Disabling fire is only used against vessels, not automobiles, aircraft, or persons. Disabling fire by land based law enforcement or security personnel using personal defense weapons is prohibited.

11. Protection of Property. The minimum amount of non-deadly force necessary may be used to prevent the theft of, intentional damage to, or destruction of property (including information) in the custody of the U.S. The use of deadly force is normally not authorized solely for the purpose of protecting property from theft, sabotage, intentional damage, or destruction. (Note: Such criminal activity in certain circumstances may also lead to the right of self-defense, prevention of a crime, or an arrest.) However, in special situations, Area and District Commanders may request COMDT to authorize the use of deadly force in limited circumstances for the protection of property which is either vital to the national security or inherently dangerous to others (i.e., certain nuclear material, explosives, operable weapons, or ammunitions). The designation of property and the specific use of force policy to protect it must be approved by COMDT. (If protecting or assisting in the protection of property in the custody of Department of Defense (DOD) military services, the DOD use of force policy applies.)

B. General Weapons Policy.

1. Carriage and Use of Weapons by USCG Police and Security Personnel. USCG police forces and security activities shall be armed as necessary to carry out their duties. USCG personnel (except special agents) will be armed with standard service weapons and ammunition only. The use of personal or privately owned weapons and ammunition is prohibited. In an emergency self-defense situation, however, if a standard service weapon malfunctions, is lost, or is insufficient

protection, any weapon available may be used.

a. Except in extremis or urgent circumstances, no member is authorized to carry and use a weapon unless:

(1) the member has been adequately trained in the use of the weapon (i.e., proficiency and judgment) in accordance with current directives;

(2) the member is thoroughly familiar with this chapter;

(3) the member has been adequately trained/equipped to be able to use non-deadly force as an alternative; and

(4) the member's CO/CP has determined that the member possesses the proper temperament, maturity and judgment to make reasonable and correct use of force decisions under pressure. Such determinations must be certified in writing unless an emergency situation precludes doing so.

b. A side arm may be drawn from its holster or a long gun shouldered for firing (or in preparation for firing) only if deadly force is warranted or there is a reasonable possibility that its use will be necessary to protect life or safeguard property vital to the national security.

c. The chambering (racking) of a round in a riot shotgun is a method used to communicate (both visually and aurally) USCG preparedness to use deadly force. This action is a signal and does not itself constitute a use of force.

2. Reporting Requirements and Policy Review.

a. Required Reports - Weapons Drawn or Used. Personal Injury. Property Damage, or Other Significant Use of Force Incident. Every law enforcement instance in which a weapon is drawn or used, personal injury or property damage results, or any other significant event occurs is a valuable learning opportunity for the entire service. However, it may also require an investigation and/or appropriate follow-up action. Accordingly, any of the following situations will warrant submission of a detailed letter report within 30 days, via the chain of command, to COMDT (G-CFI), with a copy to the cognizant Security Manager:

(1) whenever a firearm is drawn or discharged;

(2) whenever any other type of weapon is used (e.g., chemical irritants, expandable baton, etc.);

(3) whenever any other use of force involving physical contact is employed;

(4) whenever any law enforcement activity results in injury to USCG personnel or other persons, or significant property damage; or

(5) whenever any other incident involving the use or potential use of force is deemed noteworthy by the CO/CP.

b. The report should be short but thorough and include a summary of the facts, opinions, recommendations, and lessons learned. The Administrative Investigations Manual, COMDTINST M5830.l (series), and the Claims and Litigation Manual, COMDTINST M5890.9 (series), shall guide the preparation of these reports.

NOTE: (1) Separate reporting mechanisms exist and take precedence for incidents related to firearms training and accidental discharges (e.g., Ordnance Manual, COMDTINST M8000.2 (series)). (2) Special Agents are to comply with the USCG Investigations Manual, COMDTINST M5527.1 (series).

c. In the case of accidental discharge, a mishap report (MISREP) shall be completed in accordance with Safety and Environmental Health Manual, COMDTINST M5100.47 (series).

d. Policy Review. One of the primary purposes of the required reports is to provide the basis for continuous program-level policy review of the USCG approach to the use of force in law enforcement. The chief focus of such efforts is to examine current guidance, evaluate the training based thereon, and assess how well they worked in actual practice. This policy review will be coordinated by COMDT (G-CFI) and include participation by other CGHQ staff elements and the various training facilities, as appropriate.

3. Facilitating Foreign Law Enforcement. In the absence of interagency concurrence, USCG personnel are not permitted, as a matter of policy, to interfere with or facilitate foreign law enforcement. However, with certain limitations, USCG personnel may assist another nation in the enforcement of its laws, and may use the minimum force reasonably necessary to do so. USCG security/police personnel should be fully aware of the foreign law enforcement force's use of force policy, but only employ the USCG Use of Force Policy.

a. Combined Operations. Combined operations (i.e., those operations where USCG and foreign law enforcement personnel work together) greatly increase the possibility that USCG personnel will face the situation where

they can facilitate or interfere with foreign law enforcement or have foreign authorities interfere with USCG law enforcement. Owing to this increased potential, OPORDERs contemplating combined operations should be reviewed and scrutinized on an interagency basis prior to the conduct of such operations.

b. The USCG Use of Force Policy applies to USCG participation in combined operations. Units may not apply foreign use of force policies. While foreign law enforcement personnel are on board USCG units they must abide by the USCG Use of Force Policy and are subject to the direction, in this regard, of the CO/CP. Before any law enforcement action is undertaken, all participants should have a thorough understanding of the USCG Use of Force Policy.

4. Joint Operations. The USCG Use of Force Policy shall apply to all law enforcement operations involving USCG personnel. However, when the USCG acts only in support of another U.S. federal, state, or local agency, the operational commander may allow application of the other agency's use of force policy.

INDEX

PAGE(S)

- A -

Access Control…….…… 2-37, 3-6
Access Lists, Personnel……..……..…… 2-4
Accountability.
Badges.……...……..……8-3
Decals…….……..……7-9
Weapons…….……..……3-5
Acronyms..……...…… Enclosure (1)
Air Vents…….…… 3-14, 3-15
Alarm Systems (See Intrusion Detection Systems)
Ammunition……...…….……. 3-4
Ammunition Storage Requirements……..…….……. 3-12
Annunciators……..…….……. 2-21
Apprehension…….…….……. 10-3, 10-4
Area Designation……...……..……2-1
Armed Response…….……. 3-8
Armored Car Service...……..…….. 6-8
Armory……...…….……3-7, 3-9, 3-12
Arms Racks…….……. 3-10
Arms Storage Requirements…….…….…….. 3-9
Arrest…….……..……10-3, 10-4
Authority
Security/Police Force…….…….. 10-4
Title 18 U.S.C. 1382…….…….……..2-2, 2-39
Auxiliary Security/Police Force……..……. 10-14

- B -

Backup Power
Intrusion Detection Systems……2-22
Lighting……..……..……2-19
Badge Expiration..……..…….…….8-3
Badge Inventory.……..…....8-3
Badge, Security/Police Force…….....…..10-18, 10-45
Balanced Magnetic Switch……...……2-21
Ball Caps……...…... 10-16
Barriers
Inspection…….…….….…..2-12
Physical…….….….. 2-7
Temporary…….….…..2-11
Board of Survey…….….. 9-3

Bomb Incident……..…..…..12-1, 12-4, 12-24
Bomb Threat……...…..12-1, 12-7, 12-19
Bomb Threat Plans
Countermeasures…….…....12-9
Evacuation Procedures……..…...12-15
Search Techniques……...…….…... 12-12
Bombs…….…. 12-1
Boundaries
Perimeter…….……..…….…..2-10
Water…….…….…..2-8
Briefings……...……..…..9-1

- C -

Call-in Boxes…….……...……....10-11
Cashiers Cage…….……..……....6-6
Ceilings…….…….…….. 3-13, 3-15
Central Annunciator…….……..…..2-21
Chain Link Fencing…….……..... 2-9
Checks, Security……...……... 2-5
Checklists…….……....Enclosure (3)
Civil Service Security Forces……...…… 10-2, 10-11
Classified Material Control Officer…….… 1-2, 8-1
Clear Zones…….. 2-11
Closed Circuit Television……...…….. 2-9, 10-12
Combinations…….….. 2-36, 6-7
Command Security Officer
Duties…….……..1-4, 2-32, 9-1, 10-1
Qualifications…….…….. 1-1
Communications Security……..…….. 1-1, 1-4
Communications, Security/Police Force…….. 3-8, 10-11, 10-36
Compensatory Measures…….. 1-5
Concurrent Federal Jurisdiction…….…….. 10-7
Conditions, Threat……..……..5-1
Confinement……...…..10-4
Collar Insignias……..…….. 10-17
Construction Specifications
Arms Racks……..3-10
Armory……3-12
Containers (See Security Containers)
Weapons Spaces……...……3-14
Continuous Lighting……...……..2-17
Contract Security Force…….…….. 10-2, 10-11
Control Units……..……..2-21
Controlled Areas…….……..2-3

Controlled Lighting…….. 2-17
Controlled Medical Substances……..…….. 11-1
Credentials
Police Force……..……10-18
Security Manager……..1-2
Culverts…….……2-10
Custodians
Evidence……...10-37
Funds……6-7
Key……...2-32

- D -

Decals, Vehicle…… 7-1
Deficiencies…….. 1-5
Definitions …….. Enclosure (1)
Doors……2-13, 3-13, 3-15
Drugs (See Controlled Medical Substances)
Duress Alarms/Codes…….. 2-29
Duties
Command Security Officer…….. 1-4, 2-32, 9-1, 10-1
Security Manager……1-2

- E -

Emergency Lighting……. 2-17
Emergency Power…… 2-19
Emergency Vehicle Response…….. 10-35
Equipment, Security/Police Force……... 10-20
Escorts, Funds……..6-8, 10-13
Evacuations…….. 12-15
Evaluations……...1-3
Evidence……...10-37
Exceptions……1-4, 3-2, 3-10, 3-12
Exclusion Areas……... 2-2
Exclusive Federal Jurisdiction……. 10-6
Expiration Tabs…… 7-10, 7-12

- F -

Fences……...2-9, 3-9
Fire Protection……. 10-1, 10-14
Firearms (See Weapons)
Floors……3-13, 3-15

Foreign Security/Police Force…….. 10-2
Forms……2-36, 7-9, 8-1
Funds Escorts……...6-8, 10-13
Funds, Storage of……6-1

- G -

Gates
Inspection……2-12
Pedestrian……2-13
Vehicular……..2-13
Glare Projection……... 2-17
Glossary
Acronyms……Enclosure (1)
Terms……... Enclosure (1)
Government Owned Vehicles…….. 7-4
GSA Approved Security Container……. 2-36, 3-10, 6-3, 11-1
Guards
Civilian……. 10-2
Contract……10-2
Military…… 10-2

- H -

Hasps……Enclosure (5)
Hatches…….3-16
Hinges…….. 2-13, 3-14, 3-15

- I -

Identification Badges……... 8-1
Incidents, Bomb……... 12-1, 12-24
Inspections
Administrative……..2-6
Barriers…….2-12
Clear Zones……..2-11
Gates…… 2-12
Personnel……..9-4
Vehicles……9-4, 12-26
Intrusion Detection Systems
Capacitance……..2-26
Electric Circuit……2-22
Light Beam……...2-23
Maintenance……2-27

Microwave……... 2-26
Motion……..2-25
Sound……... 2-24
Testing……..2-29
Ultrasonic……2-25
Vibration…….. 2-24
Inventory
Badges……..8-3
Decals……...7-9
Keys……. 2-35
Weapons……...3-5
Investigations……... 9-2, 10-15

- J -

Jurisdiction……... 10-6
Exclusive…….. 10-6
Concurrent……10-7
Proprietary……10-7
Territorial……. 10-7

- K -

Key Control……. 2-31, 3-6
Key Control Officer……. 2-32, 3-7
Key Control Register……... 2-34, 3-7
Key Custodian……..2-32
Key Repository…… 2-34, 3-6
Keys……. 2-31, 3-6, 6-7, 6-10

- L -

Letter Bombs……12-2, 12-21
Lighting (See Protective Lighting)
Lighting, Emergency…… 2-17
Limited Areas……...2-2
Line Supervision…….. 2-21
Lock Control……2-33
Locks……Enclosure (5)
Loss Prevention……9-1
Loss Prevention Program……9-1
Loss Reporting……9-1, 9-5
Lost Badge Reporting……..8-3, 10-19

- M -

Magazines…… 3-12
Maintenance
Intrusion Detection Systems…… 2-27
Lighting…… 2-19
Man-Made Barriers…….. 2-8
Measures, THREATCON…… 5-4
Memorandum of Understanding…….. 3-8, 3-11
Military Security/Police Force……. 3-8, 10-1
Money Packets……. 6-6
Motorcycle Safety Requirements……. 7-8
Movable Lighting……. 2-17

- N -

Narcotics (See Controlled Medical Substances)
Natural Barriers……2-8
Negotiable Instruments…… 6-1
Non-Restricted Areas……...2-6

- O -

Officer of the Customs……. 10-3
Openings, Perimeter……. 2-12
Orders, Security/Police Force…….. 10-9

- P -

Padlocks……... 2-35,3-10, Enclosure (5)
Patches, Security/Police Force……. 10-2, 10-18, 10-45
Patrol Craft……...2-8
Patrol Roads……2-12
Pedestrian Gates……...2-13
Perimeter Boundaries……...2-14
Perimeter Openings…….. 2-12
Personnel Access Lists……. 2-4
Personnel Inspections……...2-6, 9-4
Personnel Movement Control…….. 3-8
Physical Barriers…….. 2-10
Physical Security Checklist…….. 1-3, Enclosure (3)
Physical Security Plan.....……..1-6, 3-2, Enclosure (2)
Physical Security Survey…… 1-3, Enclosure (3)
Pilferage……... 9-3
Police……10-1

Posse Comitatus Act…… 10-8
Posts……10-12
Post Orders……...10-9
Posting of Boundaries…….. 2-14
Power, Emergency……... 2-19
Private Motor Vehicle Registration……. 7-1
Privacy Act Statement……..8-3, 8-5
Privately Owned Vehicles…… 7-1
Privately Owned Weapons……... 3-1
Property Management……..9-1
Proprietary Jurisdiction…… 10-7
Protective Lighting……...2-16, 3-9, 6-8

- Q -

Qualifications
Security Personnel……... 1-1
Security/Police Forces……. 10-9
Quarterdeck Watch…….. 3-9

- R -

Racks……3-10
Radio Communications…… 3-8, 10-11, 10-36

Recorded Tour Systems……...10-11
Recovery…….. 9-2
References……Enclosure (7)
Registration of Privately Owned Vehicles……... 7-1
Reporting Losses……..9-1, 9-5
Repository Containers……. 2-34
Repository Index……..2-34
Response Force…… 3-8

Responsibilities
All Employees…….…… 1-1, 9-1
Chief of Police……..10-1
Command Security Officer……...1-4, 2-32, 9-1, 10-1
Security Manager……..1-3
Restricted Areas
Designation Criteria……. 2-2
Types……2-2
Roads
Patrol……2-12
Perimeter……..2-12

Robbery Plans…….. 6-11
Roofs……3-13

- S -

Searches
Bomb Threat…….……... 12-11
Vehicles……9-4, 10-3, 12-26
Security Checks……... 2-36
Security Clearances…….…..… 8-1
Security Containers……...……... 2-36, 3-10, 6-3, 11-1
Security Identification Badge……... 8-1
Security Investigations……. 9-2, 10-15
Security/Police Force……... 3-8, 10-1
Security/Police Force Equipment……10-20
Security/Police Force Training……10-19, 10-46
Security Manager
Duties……... 1-2
Qualifications……... 1-1
Security Risk Categories…….. 3-3
Sensitive Compartmented Information Facilities…… 1-1
Sensors.....……..2-21
Sewers.....……..2-13
Shipments.....……3-16
Single Scope Background Investigation.....……1-2
Signs, Warning.....…….2-14
Signboards.....……2-13
Skylights.....…….2-13
Small Arms (See Weapons)
Standard Forms.....……2-36
Standard Operating Procedures.....……1-7, 2-37
Standby Lighting.....……2-17
Standing Orders.....……10-9
Storage
Arms, Ammunition and Explosives.....……..3-9, 3-12
Badges.....…….8-3
Controlled Medical Substances.....……...11-1
Decals.....……..7-9
Evidence.....……..10-37
Funds.....……..6-4
Supervision of Security/Police Force.....……10-11
Support Agreement.....……3-8, 3-11
Survey.....……1-3, Enclosure (3)

- T -

Tabs, Expiration.....7-7, 7-10, 7-13
Taut Wire.....2-9
Telephonic Bomb Threat Report.....12-2, 12-19
Television, Closed Circuit.....2-9, 10-12
Temporary Barriers.....2-11
Terms.....Enclosure (1)
Territorial Jurisdiction.....10-7
Terrorism.....5-1
Terrorist Incidents.....5-1
Tests
  Emergency Power.....2-19
  Intrusion Detection System.....2-29
  Lighting.....2-19
Terrorist Threat Conditions.....5-1
Theft.....9-1
Threat, Bomb.....12-1, 12-4, 12-19
Threat Conditions.....5-4
THREATCON NORMAL.....5-4
THREATCON ALPHA.....5-4
THREATCON BRAVO.....5-4
THREATCON CHARLIE.....5-4
THREATCON DELTA.....5-4
THREATCON Measures.....5-4 through 5-23
Title 18 U.S.C. 1382.....2-2, 2-39
Top Guard.....2-10
Training, Security/Police Training.....10-19, 10-46
Transmission Lines.....2-21
Trees.....2-13
Tunnels.....2-13

- U -

Uniforms.....10-15
Utility Openings.....2-13
Utility Poles.....2-13

- V -

Vehicle Decals.....7-1
Vehicle Gates.....2-13
Vehicle Inspections.....9-4, 10-3
Vehicle Movement Control.....3-8
Vehicle Patrol Standards.....10-33

Vehicle Response.....10-35
Vehicle Searches.....10-3, 12-26
Vehicles
  Government Owned.....7-4
  Privately Owned.....7-1
Visitor Control.....2-37
Visitors.....2-37
Visitors Bill.....2-37

- W -

Waivers.....1-4, 3-2
Walls.....2-11, 3-13, 3-15
Warning Signs.....2-14
Watch, Quarterdeck.....3-9
Water Boundaries.....2-8
Water Patrol Craft.....2-8
Weapons.....3-3, 9-3, 10-21
Weapons Containers.....3-10
Weapons Space..... 3-9, 3-12, 3-4
Windows.....2-13, 3-14, 3-15
Wire, Taut.....2-9

- X, Y & Z -

Zones, Clear.....2-11