

**Headquarters, U.S.
Marine Corps**

**MCO P5530.14
PCN 10208597900**



**MARINE CORPS
PHYSICAL SECURITY
PROGRAM MANUAL**

**COORDINATING DRAFT
(10 Jun 2004)**

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

IN REPLY REFER TO:
MCO P5530.14A
PS

MARINE CORPS ORDER P5530.14

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

Encl: (1) LOCATOR SHEET
(2) REFERENCES

1. Purpose. To establish policy, procedures, responsibilities, and uniform standards, per the references, for the Marine Corps Physical Security Program.

2. Cancellation: OPNAVINST 5530.13C, MCO 5510.15A, MCO 5500.18, MCO 1630.4A, MCO 4340.1, MCO 5500.14A, and MARADMIN 601-02.

2. Background. This Manual standardizes requirements for physical security aboard Marine Corps installations and organizations, as well as:

a. Provides commanders the authority and responsibility to protect personnel, facilities, property, and material under their command.

b. Identifies measures to safeguard personnel, facilities, property and material at all Marine Corps installations and activities.

c. Provides guidance for evaluating, planning and implementing Marine Corps command physical security programs.

d. Establishes uniform standards.

e. Assists those responsible for physical security in their efforts to carry out the assigned mission.

3. Discussion. To be effective, a physical security program must receive attention from all echelons within the chain of command.

Emphasis is placed on the commanding officer's responsibility to ensure that the command security posture is accurately assessed and security resources are appropriate to execute these programs.

DISTRIBUTION STATEMENT A: Approved for public release, distribution is unlimited.

4. Responsibilities. Marines, Sailors, and civilian employees must be involved in the physical security of U.S. Government and Marine Corps property.

a. Installation commanders/commanding officers are responsible for physical security within their commands.

b. The provost marshal is the installation commander's designated representative responsible for planning, implementing, enforcing and supervising the installation physical security program.

c. The security officer at each Marine Corps organization (battalion/squadron size and larger) is responsible for security matters within the organization. The security officer plans, implements, manages and directs the organization physical security program in coordination with the provost marshal.

5. Recommendations. Recommendations for changes to this Manual are encouraged. All recommendations will be forwarded via the chain of command to the Commandant of the Marine Corps (PS).

6. Action

a. The Deputy Commandant for Plans, Policies, and Operations (DC, PP&O) is assigned overall coordination and program responsibility for physical security within the Marine Corps and will:

- (1) Exercise overall staff cognizance for matters relating to physical security.
- (2) Develop physical security policy and oversee its implementation.
- (3) Provide guidance and assistance to commanders to enable them to develop and maintain effective physical security programs.
- (4) Manage a program to assess the level of security afforded installations and assets, and develop plans for security upgrades.
- (5) Program funds in support of specific Marine Corps physical security initiatives, to include:

(a) Marine Corps Electronic Security Systems (MCESS) for critical Marine Corps assets.

(b) Installation Physical Security Site Assistance Visits.

(6) Coordinate with the Deputy Commandant for Installations and Logistics (DC, I&L) for review of all Military Construction (MILCON) projects. This coordination will ensure that physical security and Antiterrorism/Force Protection (AT/FP) measures and costs are identified and incorporated in the cost estimates.

b. The Inspector General of the Marine Corps (IGMC) will:

(1) Coordinate with the DC, PP&O, PS regarding integration of the provisions of this Manual into the Automated Inspection Reporting System (AIRS) discrepancy listing.

(2) Conduct reviews as part of the Marine Corps Command Inspection Programs to determine compliance with the requirements contained herein.

c. DC, I&L will:

(1) Develop policy for installation master planning which factors in and documents physical security requirements.

(2) Provide programmed MILCON project documentation to DC, PP&O, PS for review.

(3) Coordinate with DC, PP&O, PS, to review all requests for Physical Security Structural Upgrade (R-2) funding.

(4) Coordinate with the Naval Facilities Engineering Command during the design of MILCON projects to ensure that the requested physical security and force protection measures are included in the design and construction of facilities.

d. Installation commanders will integrate security efforts to ensure continuity in providing an effective installation physical security program and posture.

e. Commanding officers (battalion/squadron and above) will implement the contents of this Manual and augment the guidance provided with local directives as required.

7. Reserve Applicability. This Manual is applicable to the Marine Corps Reserve, unless otherwise noted.

MCO P5530.14A

8. Records Disposition. Records required by this Manual will be maintained per part II, chapter 5, items 5500 through 5530 of SECNAVINST 5212.5.

9. Certification. Reviewed and approved this date.

J. C. HULY
Deputy Commandant for Plans,
Policies, and Operations

DISTRIBUTION: PCN 71000000000
71000000100

COPY TO: 7000110 (55)
8145005 (2)
7000099 (144)
8145001 (1)

LOCATOR SHEET

Subj: MARINE CORPS PHYSICAL SECURITY PROGRAM

Location: _____
(Indicate Location(s) of copy(ies) of this Manual.)

Coordinating Draft for Review 10 June 2004

REFERENCES

- (a) SECNAVINST 5000.36; Department of the Navy Data Management and Interoperability
- (b) SECNAVINST 5510.36; Department of the Navy (DON) Information Security Program (ISP) Regulation
- (c) SECNAVINST 5510.30A; Department of Navy Personnel Security Program
- (d) DoDD 5210.41; Security Policy for Protecting Nuclear Weapons
- (e) SECNAVINST 5511.36A; Authority Of Military Commanders Under Internal Security Act Of 1950 To Issue Security Orders And Regulations For The Protection Or Security Of Property Or Places Under Their Command
- (f) DoD 5100.76-M; Physical Security of Conventional Arms, Ammunition and Explosives
- (g) DoDI 2000.16; DoD Antiterrorism Standards
- (h) MCO P11000.5F; Real Property Facilities Manual, Volume IV
- (i) UFC 4-010-01; Design: DoD Minimum Antiterrorism Standards for Buildings
- (j) FMFM 7-14; Combating Terrorism
- (k) DoD 5200.8R; Physical Security Program
- (l) MCO 5110.1C; Motor Vehicle Traffic Supervision
- (m) MIL-HDBK-1013/1A; Military Handbook Design Guidelines for Physical Security of Facilities
- (n) MCO 5500.6F; Arming of Security and Law Enforcement (LE) Personnel and the Use of Force

Coordinating Draft for Review 10 June 2004

- (o) MCO 3574.2J; Entry Level and Sustainment Level Marksmanship Training With The M16A2 Service Rifle and M9 Service Pistol
- (p) UFC 4-012-01; Security Engineering: Entry Control Facilities/Access Control Points
- (q) UFC 4-021-01; Design and O&M Mass: Notification Systems
- (r) DOD 6055.9-STD; DoD Ammunition and Explosives Safety Standards
- (s) NAVSUP OP 5 Vol 1; Ammunition and Explosives Ashore Safety Regulations for Handling, Storing, Production, Renovation and Shipping
- (t) MCO P8020.10A; Marine Corps Ammunition Management and Explosives Safety Manual
- (u) OPNAVINST 5530.13C; Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition and Explosives
- (v) NAVSUP P-724; Conventional Ordnance Stockpile Management (Rev 7)
- (w) DOD 5200.2-R; Personnel Security Program
- (x) DoD 5220.22-M; National Industrial Security Program Operating Manual
- (y) DoD 4140.1-R; DoD Material Management Regulation
- (z) DoD 4160.21-M; Defense Materiel Disposition Manual
- (aa) OPNAVINST 8015.2A; Conventional Ordnance Inventory Accountability
- (bb) MCO 8300.1C; Marine Corps Serialized Control of Small Arms System
- (cc) MCO 4400.150E; Consumer-Level Supply Policy Manual
- (dd) MCO 4400.151B; Intermediate-Level Supply Management Policy Manual
- (ee) DoD 4500.9-R; Defense Transportation Regulation

ENCLOSURE (2)

Coordinating Draft for Review 10 June 2004

- (ff) NAVSEA SW020-AG-SAF-010; Navy Transportation Safety Handbook for Ammunition, Explosives, and Related Hazardous Materials
- (gg) MCO 3302.1D; The Marine Corps Antiterrorism/Force Protection (AT/FP) Program
- (hh) MCO 1620.2C; Armed Forces Disciplinary Control Board and Off-Installation Liaison and Operation
- (ii) DoD 4160.21-M-1; Defense Demilitarization Manual
- (jj) MCO P5580.2A; Marine Corps Law Enforcement Manual
- (kk) MCO 4066.17; Marine Corps Exchange Security and Loss Prevention Manual
- (ll) NAVMED P-117; Manual of the Medical Department
- (mm) MCWP 3-34.1; Military Police in Support of the MAGTF
- (nn) DoDD 2000.12; DoD Antiterrorism (AT) Program
- (oo) UFC 4-010-02; Design (FOUO) DoD Minimum Standoff Distances For Buildings
- (pp) DoD 0-2000.12-H; DoD Antiterrorism Handbook

Coordinating Draft for Review 10 June 2004

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

TABLE OF CONTENTS

CHAPTER

1	INTRODUCTION
2	SECURITY PLANNING
3	SECURITY MEASURES
4	SECURITY FORCES
5	BARRIERS AND OPENINGS
▶ 6	PROTECTIVE LIGHTING ELECTRONIC SECURITY SYSTEMS
▶ 7	SECURITY OF OTHER CRITICAL RESOURCES
▶ 8	SECURITY OF ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)
▶ 9	CRIME PREVENTION PROGRAM
▶ 10	REPORTING
▶ 11	PHYSICAL SECURITY IN THE OPERATING FORCES

APPENDIX

A	DEFINITIONS
B	PHYSICAL SECURITY PLAN (FORMAT)
▶ C	INSTRUCTIONS FOR PREPARATION OF A MISSING, LOST, STOLEN, AND RECOVERED (MLSR) REPORT
D	INSTRUCTIONS FOR PREPARATION OF PHYSICAL SECURITY SURVEY

- ▶ E WAIVER AND EXCEPTION REQUEST (FORMAT)
- ▶ F KEY AND LOCK CONTROL FORMS
- ▶ G SEIWG DATA FORMAT
- ▶ H SECURITY RISK CATEGORIES
- ▶ I AA&E SCREENING PACKAGE
- ▶ J MLSR AA&E REPORTING QUANTITIES
- ▶ K EXAMPLE ATF Form 3270.19
- ▶ L INSTRUCTIONS FOR PREPARATION OF THE LAW
ENFORCEMENT AND PHYSICAL SECURITY ACTIVITY
REPORT

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 1

INTRODUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
SCOPE	1000	1-3
THE SECURITY CHALLENGE	1001	1-3
SECURITY RESPONSIBILITIES	1002	1-5
SECURITY OF MARINE CORPS INSTALLATIONS AND RESOURCES	1003	1-5
DEPUTY COMMANDANT FOR PLANS, POLICIES AND OPERATIONS	1004	1-6
COMMANDER MARINE FORCES	1005	1-6
INSTALLATION COMMANDER	1006	1-6
COMMANDING OFFICER	1007	1-7
PROVOST MARSHAL	1008	1-7
► PHYSICAL SECURITY CHIEF	1009	1-9
COMMAND/ORGANIZATION SECURITY OFFICER . .	1010	1-10
PHYSICAL SECURITY OF ORGANIZATIONS NOT LOCATED ABOARD MARINE CORPS INSTALLATIONS	1011	1-11
PHYSICAL SECURITY OF TENANT AND CIVILIAN AGENCIES/ORGANIZATIONS ABOARD MARINE CORPS INSTALLATIONS	1012	1-12
PHYSICAL SECURITY COUNCIL	1013	1-12
WAIVERS AND EXCEPTIONS	1014	1-13

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
HOST NATION CONFLICT	1015	1-15
ACTIVITY UPGRADE PROJECTS	1016	1-15
FACILITY MODIFICATIONS	1017	1-16
MILITARY/MINOR CONSTRUCTION	1018	1-16

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 1

INTRODUCTION

1000. SCOPE. This Manual directs the application of physical security programs **for Marine Corps commands and ~~aboard Marine Corps installations, Marine Forces, and battalions/squadrons and above~~. Included are Marine Corps organizations not located aboard a Marine Corps installation, and tenant and civilian agencies/organizations aboard Marine Corps installations.**

Definitions applicable to this Manual are contained in Appendix A. This Manual further:

1. Identifies responsibilities for physical security. It classifies various security vulnerabilities, details protective measures and management actions that must be employed to provide an acceptable physical security posture.

2. Establish **uniform ~~minimum~~** physical security requirements. The language separates recommended physical security measures from required measures and eliminates conflicting guidance.

3. Identifies physical security requirements that are not covered by other specialized security programs. Protection of classified material, automated data processing (ADP) systems, and ~~sensitive conventional arms, ammunition and explosives (AA&E)~~ nuclear weapons security are specifically addressed in references (a) through (d), respectively. Those requirements augment the basic guidance provided by this Manual.

4. Establishes policy and procedures for Marine Corps commanders authorized to issue regulations for the protection or security of property or places under their command as specifically addressed in reference (e).

1001. THE SECURITY CHALLENGE

1. Protection of personnel and property is accomplished by:

1001 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- a. Identifying the personnel or property requiring protection.
- b. Determining jurisdiction and boundaries.
- c. Assessing the threat.
- d. Committing resources.
- e. Establishing perimeters, barriers, and access control.
- f. Providing the means to detect efforts to wrongfully remove, damage or destroy property.
- g. Employing a security force sufficient to protect, react to, and control situations and circumstances that threaten personnel and property.

2. The security challenge is influenced partially by the geographic location, size, type, jurisdiction, and mission of the property. Further, the procedures, plans, policies, agreements, systems and resources committed to safeguard personnel, protect property, and prevent losses also impact security. The physical security portion of the program is concerned with means and measures designed to achieve a strong physical security and antiterrorism/force protection (AT/FP) posture. The program goal is to safeguard personnel and protect property by preventing, detecting, and confronting unauthorized acts. These unauthorized acts include but are not limited to terrorism, espionage, sabotage, wrongful destruction, malicious damage, theft, and pilferage.

3. Terrorist activity worldwide against U.S. military and business concerns poses a clear and persistent danger to Marine Corps interests. While such activity is principally targeted against commands overseas, prudence dictates recognition of the potential threat to activities within the continental United States. Additionally, military activities located within leased space facilities have unique challenges in addressing physical security issues (commercial firms and contractors located in same building(s), public facilities, shared entranceways and common spaces). Security officers shall use the guidance and

policies contained in this Manual in determining security and/or protective measures deemed essential for their particular spaces, areas and/or buildings. Liaison with appropriate authorities (General Services Administration (GSA), building administrators, lessors, etc.) is essential to outline specific security measures that are necessary for protection of lives and property and tailored to the individual characteristics of the leased space. Commands should address physical security in all lease agreements, ~~as appropriate.~~

1002. SECURITY RESPONSIBILITIES. Security is the direct responsibility of all Marines, Sailors, and civilian employees. Specific responsibilities are established in the following paragraphs.

1003. SECURITY OF MARINE CORPS INSTALLATIONS AND RESOURCES.

Installation commanders are authorized to issue regulations for the protection or security of property of places under their command pursuant to the provisions of reference (e), and to provide guidance relative to the enforcement of the laws that prohibit unlawful entry.

1. Security regulations or orders must be conspicuously and appropriately posted. Reference (e) provides penalties for violations of such regulations or orders as have been promulgated or approved by the installation commander for the protection or security of Department of Defense (DoD) property or places.

2. Installation commander's authority, per references (e), is limited to property and places "under their command" and requires installation commanders to comply with the implementing policies and procedures established by the Department of Defense.

3. Penalties for persons who unlawfully enter or reenter a military installation are addressed in reference (e).

1004 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

1004. DEPUTY COMMANDANT FOR PLANS, POLICIES AND OPERATIONS (D/C PP&O). The D/C PP&O is responsible for formulation and dissemination of Marine Corps physical security policy. As such, the D/C PP&O has cognizance for implementation of this policy. All correspondence concerning physical security matters will be addressed to the CMC(PS).

1. Plan, program, and budget requisite resources to ensure that AA&E in Marine Corps custody is protected in accordance with reference (f).

2. Prescribe security requirements for AA&E that are outside the scope of reference (f).

1005. COMMANDER, MARINE FORCES. The Commander of Marine Forces Atlantic, Pacific, and Reserves (COMMARFORLANT, COMMARFORPAC, and COMMARFORRES) will implement and oversee requirements of this Manual within their headquarters and subordinate commands.

1006. INSTALLATION COMMANDER. The installation commander is inherently responsible for the overall command security posture to include perimeter and area security and protection of personnel and property aboard the installation. As such, the installation commander is responsible for:

1. Establishing an installation physical security program, to include a physical security plan that is included as an appendix of the installation AT/FP plan. An example format of a physical security plan is provided in Appendix B. The purpose of a physical security plan is to identify day to day physical security applications and operations. This plan must incorporate the physical security plans of all tenant commands as required in reference (f).

2. Appointing a physical security officer in writing to ensure that requirements of this Manual are implemented. The installation physical security officer should be the installation provost marshal, due in part to the unique security assets (military police, military working dogs, physical security specialists, military police investigators, etc.) under his/her operational command.

3. Publishing a consolidated list of all restricted areas aboard the installation, including those of tenant commands. This list will be published annually, and will specify whether or not these areas are vital or substantial to national security. Figures 7-1 & 2 contain the Department of Defense asset prioritization chart and physical security threat matrix, which can assist commanders in prioritizing asset protection efforts.

1007. COMMANDING OFFICER. Each commanding officer (battalion/squadron and higher) is responsible for physical security within his/her organization. As such, he/she is responsible for:

1. Establishing and maintaining a command physical security program that encompasses all requirements of this Manual.

2. Appointing a command security officer in writing and providing him with sufficient resources, staff assistance and authority to implement, manage and execute an effective physical security program. It is recommended that the command security officer also be appointed as the command antiterrorism/force protection (AT/FP) officer, as these two programs complement one another.

3. Identifying and designating, in writing, all restricted areas within his/her command to include specifying whether or not these areas are vital or substantial to national security. This information will be provided in writing to the installation commander annually.

► **4. Report Missing, Lost, Stolen, and Recovered (MLSR) reportable items to CMC (PS/LPC), per chapter 10, and in the format provided by Appendix C.**

1008. PROVOST MARSHAL. The installation provost marshal serves as the staff officer responsible for coordinating the installation physical security and law enforcement programs. As such, the provost marshal is responsible for ensuring that those programs complement the overall installation security effort. In this capacity, the provost marshal will:

1. Conduct law enforcement operations and crime prevention efforts in support of the installation physical security program, including measures to enhance security during periods of increased threat and crisis situations.
2. Determine the adequacy of the installation physical security posture with a physical security survey program. Physical security surveys identify areas requiring improvements and direct corrective measures to the responsible commanding officer. The surveys may also provide recommended actions for an improved organization security posture. Physical security surveys will be conducted as prescribed in Chapter 3.
3. Maintain liaison with installation/regional Naval Criminal Investigative Service (NCIS) personnel in support of criminal investigations aboard the installation. Maintain liaison with federal, state, local, other military activities, and host nation officials regarding law enforcement/physical security concerns. These concerns will include mutual physical security responsibilities as applicable and according to Memorandums of Agreement (MOAs), Memorandums of Understanding (MOUs), Status of Forces Agreements (SOFAs), and Host Nation Agreements.
4. Provide commanders with technical assistance and recommend equipment, procedures, and methods to enhance physical security.
5. Support the installation commander in developing and maintaining a comprehensive installation physical security plan.
- ▶ 6. ~~Provide guidance and support to~~ **Support the installation commander in developing and chairing** the installation Physical Security Council as described herein.
7. Review and endorse all requests for physical security waivers and exceptions from command and tenant organizations.
8. Ensure law enforcement and physical security programs complement the installation AT/FP program. These programs are key elements of the AT/FP effort and the installation provost marshal will not be assigned as the AT/FP officer, as his/her focus is law enforcement and physical security functions.

9. Assist command/organization security officers in physical security and AT/FP efforts.

▶ 10. Act as the manager of ~~the all~~ the **CMC(PS)** centrally managed Marine Corps Electronic Security Systems (MCESS) aboard the installation ~~and develop policy and procedures for MCESS operation.~~

▶ 11. Investigate MLSR incidents when appropriate or, where warranted, refer to NCIS for investigation.

▶ 1009. PHYSICAL SECURITY CHIEF. The physical security chief serves as the provost marshal's resident protection professional responsible for establishing, implementing, and managing the installations physical security and loss/crime prevention programs. As such, the physical security chief is responsible for ensuring that the provost marshal's programs encompass the security efforts of tenant activities, while ensuring tenant activities have security programs that complement the overall installation security effort. In this capacity, the physical security chief will:

1. Supervise the provost marshal's physical security unit.

2. Support the installation commander by establishing, implementing, and maintaining:

a. Physical security programs that utilize active and passive security measures and management protocol designed to prevent unauthorized access to personnel, equipment, material and documents, and safeguards against espionage, sabotage, damage, and theft.

b. Crime and loss prevention programs that increase personal safety, protect government and personal property from theft, misuse and unlawful destruction, while focusing on reducing manpower, time, and cost expended by the government in the investigation, pursuit, and prosecution of criminal activities. See Chapter 9 for further information on crime and loss prevention programs.

c. Procedures for timely submission of required reports (LEPSAR, etc.).

3. Assist the Installation AT Officer with physical security related matters that affect the AT/FP Program, however, physical security specialist will not be assigned AT Officer responsibilities as an additional/collateral duty, as their focus is physical security.

4. Provide testing, preventive maintenance, and troubleshooting to the installation's MCESS in protection of AA&E, flight lines, and other critical assets.

5. Assist commands in physical security related training.

6. Track all MLSR reports submitted by commands located aboard the installation, and determine if the loss was due to a physical security deficiency.

1010. COMMAND/ORGANIZATION SECURITY OFFICER. The command/organization security officer serves as the focal point for physical security matters and will report directly to the commanding officer in matters pertaining to physical security. Each security officer will be appointed in writing. Additionally, separate organizations such as Marine Corps Community Services (MCCS) activities, and tenant organizations will designate a security officer. Individuals assigned as security officers may be assigned such duties on a collateral basis and will be a commissioned officer, staff non-commissioned officer or equivalent civilian employee grade. In this capacity, the security officer will:

1. Plan, manage, implement, and direct the organization physical security program.

2. Establish physical security requirements for the command with assistance from the installation provost marshal, public works officer and facilities engineer as appropriate.

3. Develop, implement and maintain an organization physical security plan. This plan should be incorporated into the organization AT/FP plan.

4. Develop and maintain an organization security education program.

5. Identify assets (property and structures) requiring protection by priority and location. Particular attention will be paid to those areas **housing personnel and** storing government property.

6. Coordinate identification of restricted areas with the provost marshal. Ensure these areas are designated in writing by the Commanding Officer, and provided to the installation commander/commanding officer for inclusion in the installation order/directive that identifies all restricted areas.

7. Determine and identify resources (e.g., personnel, materials, funds, etc.) required to implement physical security measures.

8. Assist the commanding officer in specifying facility, training, construction, and equipment requirements necessary to comply with this Manual.

9. Program and budget fiscal resources necessary to support physical security requirements and correct deficiencies.

10. Serve as the organization point of contact for all requests for physical security and loss prevention to include exceptions/waivers, MLSRs, etc.

11. Coordinate all ~~AT/FP~~ and physical security matters with the installation provost marshal.

12. Attend quarterly Physical Security Council meetings.

1011. PHYSICAL SECURITY OF ORGANIZATIONS NOT LOCATED ABOARD MARINE CORPS INSTALLATIONS. At all Marine Corps organizations not located aboard a Marine Corps installation, the commanding officer will:

1. Establish a command physical security program.

2. Appoint a command security officer in writing.

▶ 3. Establish a command physical security survey program. (Note: Personnel conducting these evaluations need not possess MOS 5814 (~~Crime Prevention~~/Physical Security Specialist)). **Surveys will be completed using NAVMC 11121 per Appendix D.** Completed surveys at the organization will be retained for a period of three years. ~~or until the next Commanding General/Inspector General of the Marine Corps inspection, whichever occurs last.~~

4. Additionally, those organizations located aboard other Department of Defense service/agency sites will coordinate physical security requirements with the host. Marine Corps organizations are encouraged to establish Inter Service Support Agreement (ISSA)/MOUs/MOAs/SOFAs with the host service or nation. Topics which should be addressed include property boundaries, intrusion detection system monitoring, available response forces, deadly force training and issues, physical security support, etc. Commanding officers are required to coordinate all such agreements through higher headquarters, to include Judge Advocate/legal offices.

1012. PHYSICAL SECURITY OF TENANT AND CIVILIAN AGENCIES/ ORGANIZATIONS ABOARD MARINE CORPS INSTALLATIONS. Tenant and civilian organizations aboard Marine Corps installations will maintain an active physical security program that complements the installation's program. Host installations will establish a MOU/MOA/SOFA/ISSA, and/or Host Nation Agreement where applicable and as directed, with tenant and civilian agencies that

▶ incorporate or recognize a physical security **survey inspection** program. Agreements will be coordinated with all special staff offices, particularly the Judge Advocate/Legal office. Tenant organizations will be made aware of all physical security initiatives to include the installation physical security council and antiterrorism contingency drills to be conducted by the host installation.

1013. PHYSICAL SECURITY COUNCIL. The installation commander will establish, in writing, a Physical Security Council (PSC) which will meet on a quarterly basis. The installation commander or a designated representative will chair the PSC. The PSC assists the commander by coordinating and implementing

▶ initiatives that support the installation's physical security, **Critical Infrastructure Protection (CIP)**, and AT/FP program. The PSC provides a means for the commander to gain maximum participation from organizations on the installation in support of physical security interests.

1. The PSC will consist of those personnel who are able to materially assist the installation commander in the physical security effort. Examples of personnel who will attend are the provost marshal, operations officer, facilities officer, comptroller, and a representative from the Judge Advocate office.

2. PSC subject matter is focused on, but not limited to, the installation's physical security, CIP, and AT/FP posture. The council will conduct a review of physical security, CIP, and AT/FP deficiencies and recommend corrective action, which may include fiscal and/or logistical solutions.

3. When agenda items directly impact their command, tenant or unit commanders/command security officers will attend PSC meetings.

▶ 4. Council minutes will be recorded for accuracy and distributed to attendees for review. These minutes will be maintained on file for a period of ~~one~~ **three** years.

▶ 1014. WAIVERS AND EXCEPTIONS. CMC(PS) serves as the sole authority for waivers and exceptions to physical security requirements. Requests for waivers/exceptions will be originated by the commanding officer of the affected organization. **Waivers, exceptions, or extension requests will be assigned a waiver or exception number**, and completed in the applicable prescribed format outlined in Appendix E. ~~The initiating command will assign a waiver or exception number per the prescribed format. All information must be provided in waiver and exception requests, to include extension requests.~~ Additionally, the following guidance is provided:

a. All requests for waivers or exceptions will contain an organization plan of action and milestones (POA&M).

b. Non-applicable elements shall be noted as N/A.

c. Requests will contain an analysis of the problem and a detailed description of compensatory ~~equivalent~~ security measures ~~in effect~~, which the commanding officer ~~will ensure that compensatory measures have been~~ **has** implemented ~~and that such measures are identified within the request.~~

d. The installation provost marshal will endorse all requests and ensure that the most recent physical security survey for that facility is attached. **Additionally**, the provost marshal will identify if and/or how the waiver or exception may impact the overall installation security posture.

1. Waiver or exception requests will be forwarded via the chain of command, including **the installation commander, to the cognizant COMMARFOR** ~~=Commanding General/Commanding Officer, and higher headquarters to CMC(POS)~~ for approval/disapproval.

2. **Requests for a waiver or exception to an AA&E structural deficiency will be forward via the chain of command, including the installation commander and cognizant COMMARFOR, to CMC (PS) for approval/disapproval.**

3. Waivers are granted for a one-year period when corrective action of a security **deficiency requirement** may be accomplished by the organization **in the near-term**. Exceptions are granted for three years when corrective action of a security **deficiency requirement** is beyond the capability of the organization, or the condition necessitating the request cannot be corrected in the near-term. ~~Requests for extensions will be completed in the format prescribed in Appendix E and will be processed for approval in the same manner as the original request. Additionally, all extension requests must be accompanied by the latest physical security survey conducted for that site. Waivers and exceptions to security criteria contained in reference (SECNAVINST 5510.30A, SECNAVINST 5510.36 through (d) satisfy requirements of this Manual.~~

4. Permanent waiver/exceptions will not be granted.

► 5. Blanket waivers and exceptions listing several different facilities which have the same deficiencies will not be granted.

6. Approval of waivers and exceptions does not relieve commanding officers of the security responsibility, compensatory security measures, and a POA&M to correct the identified deficiency.

7. Waivers and exceptions are self-canceling at the end of the allocated time.

~~1015. WAIVER AND EXCEPTION CANCELLATION. Waivers and exceptions are self-canceling at the end of the allocated time. Request for renewal must be submitted prior to the expiration date.~~

8. Commands are directed to notify **the approving authority** ~~CMC(POS)~~ once the waiver/exception deficiency(ies) has been corrected and the requirement no longer exists.

1015. HOST NATION CONFLICT. Organizations located outside of the United States (OCONUS) may not be able to implement certain requirements of this Manual. In those instances, commanders must address physical security requirements in Host-Nation or Status of Forces Agreements (SOFAs).

1016. ACTIVITY UPGRADE PROJECTS

1. Upgrades or modifications to existing facilities must conform to standards contained in this Manual.

2. Physical Security Upgrade Project (R-2) Funding. This funding is awarded annually in support of installation physical security upgrade projects. Consideration for funding requires the installation to initiate correspondence to CMC(LFF-2) in accordance with the procedures outlined in reference (h). Once received at CMC(LFF-2), the project will be reviewed and validated by CMC(LFF-2 and PS) and will compete for funding against security projects initiated throughout the Marine Corps. Projects approved will be awarded design funds and installations

will be notified via Naval message traffic. Construction projects are evaluated and approved based on initial correspondence; therefore installations are not required to send an additional request. Request for authority to advertise the project for execution will be submitted on the installation's contract advertisement forecast in accordance with reference (h).

3. It is the installation's responsibility to contact LFF and/or POS to identify the status of the request.

1017. FACILITY MODIFICATIONS. Physical security and force protection enhancement modifications to existing buildings, facilities, sites, etc., must be reviewed by the provost marshal or designated representative, security officer and AT/FP officer during the design process, all review phases and final (100%) drawings. Modification requests will be forwarded to the facility/public works officer via the provost marshal and/or security officer who will ensure that changes are consistent with applicable security criteria. Contract for bid will not be processed without documentation of review by security and AT/FP representatives.

1018. MILITARY/MINOR CONSTRUCTION

1. All military construction projects will be reviewed at CMC(I&L and PS) to ensure physical security and force protection requirements have been addressed. Installation facility engineers, antiterrorism/force protection officers, and physical security personnel will review all military/minor construction projects to ensure that physical security and force protection requirements have been addressed.

2. Military/minor construction shall comply with the requirements of this and other appropriate physical security design/technical manuals. All plans for new construction must incorporate physical security and force protection features and must be reviewed by the provost marshal or designated representative, security officer, and the AT/FP officer during the design process, all review phases and final (100%) drawings.

A review will be conducted during the design process and all review phases. Contract for bid will not be processed without documentation of review by security and AT/FP representatives.

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 2

SECURITY PLANNING

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	2000	2-3
▶ PHYSICAL SECURITY CREDENTIALS	2001	2-3
PHYSICAL SECURITY PLAN	2002	2-5
EVALUATION	2003	2-5
COST OF SECURITY	2004	2-7
COORDINATION	2005	2-8
SECURITY CONSIDERATIONS	2006	2-8
CALCULATED RISK	2007	2-9

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 2

SECURITY PLANNING

2000. GENERAL. Security planning is a continuous process carried out in advance of, and concurrent with, security operations. Normally, planning for security operations will fall within the patterns used by military planners, i.e., the estimate, the plan, and implementation in the administrative plan or annexes. The security estimate with its analysis of the mission and situation (courses of action and decision) provide the basis for the security plan. Each installation and organization (battalion/squadron and above) will develop and publish a physical security plan as part of its AT/FP plan. Tenant activity physical security plans will be integrated into the installation plan. Classification of the plan will be established per reference (b).

► 2001. PHYSICAL SECURITY CREDENTIALS. In the performance of their assigned duties, school-trained military police personnel possessing the additional MOS 5814 must be permitted access to all designated restricted areas, Mission Essential Vulnerable Areas (MEVAs), and other facilities containing critical assets. Accordingly, physical security specialists must possess an official means to identify themselves to unit commanders with facilities that are subject to the requirement for a physical security survey as prescribed herein.

1. CMC(PS) will maintain strict accountability of Marine Corps physical security inspector credentials by central issuance. Only school-trained military police personnel currently assigned to the Provost Marshal's Physical Security Unit, and performing the duties of a physical security specialist will be issued credentials.

2. Installation Provost Marshals will request issuance of physical security credentials in the format prescribed in Figure 2-1. Each individual requiring credentials will enclose an identification photograph, approximately 1-1/4 inches square, and a copy of the U.S. Army Conventional Physical Security Course Completion Certificate with each request.

(HEADING)				
Code)				5512 (Orig. (Date)
From:	Provost Marshal, (Base or Station)			
To:	Commandant of the Marine Corps (POS-20)			
Subj:	REQUEST FOR ISSUANCE OF PHYSICAL SECURITY SPECIALIST CREDENTIALS			
Ref:	(a) MCO P5530.14A			
Encl:	(1) U.S. Army Conventional Physical Security Course Completion Certificate (2) Identification Photographs			
1. In accordance with the instructions contained in reference (a), request physical security specialist credentials be issued for the following Personnel:				
<u>NAME</u>	<u>GRADE</u>	<u>SSN/MOS</u>	<u>BILLET ASG.</u>	<u>SCTY. CLNC</u>
2. All personnel identified above have attended the U.S. Army Conventional Physical Security Course.				
3. Upon completion of physical security specialist duties or reassignment, Credentials will be returned to the Commandant of the Marine Corps (POS-20) For voidance.				
(SIGNATURE)				

Figure 2-1.--Request for Issuance of Physical Security Credentials Format.

Installation Provost Marshals must certify that the individual meets each of the following criteria:

- a. Successive completion of the U.S. Army Conventional Physical Security Course at Fort Leonard Wood.
 - b. Entry of course completion certificate into the Service Record Book (SRB), and assignment of the additional MOS 5814.
 - c. Assignment to the physical security unit, and performing the duties of a physical security specialist.
3. Upon receipt of credentials, an acknowledgement of responsibilities, See Figure 2-2, will be completed. This document will be promptly returned to CMC(PS).
4. It is the responsibility of the physical security chief to ensure that credentials are returned to CMC(PS) for voidance when individuals are no longer assigned to the physical security unit or performing the duties of a physical security specialist.

2002. PHYSICAL SECURITY PLAN. A model physical security plan format is provided in Appendix B. The intent of the plan is to clearly identify how the command conducts day-to-day security as well as how it responds to security incidents. The plan should reflect the detailed implementation of Marine Corps policy at the installation/activity and should not be philosophical or a verbatim reiteration of this Manual. The physical security plan will be included as an annex or appendix in the installation antiterrorism/force protection (AT/FP) plan, which is detailed in reference (g). The physical security plan is not intended to replace the AT/FP plan, it will complement the plan with detailed information concerning daily application of access control, material control, barriers, etc., aboard the installation. The physical security plan will be reviewed annually in conjunction with the AT/FP plan.

2003. EVALUATION. In evaluating the type and extent of physical protection required, the following factors should be considered in planning:

(HEADING)	
Code)	5512 (Orig. (Date)
From: _____	
(Rank, Full Name, SSN/MOS, Duty Station)	
To: Commandant of the Marine Corps (POS-20)	
Subj: RECEIPT FOR PHYSICAL SECURITY SPECIALIST CREDENTIALS, AND ACKNOWLEDGEMENT OF RESPONSIBILITIES	
Ref: (a) MCO P5530.14A	
1. I hereby acknowledge receipt for physical security specialist credentials, serial number _____. I agree to safeguard these credentials, and to prevent their loss.	
2. I recognize that the issued credentials will only be used in the furtherance of official physical security specialist duties. Under no circumstances are they to be used for personnel benefit.	
3. I recognize that these credentials are the property of the U.S. Government, and are to be returned to Commandant of the Marine Corps (POS-20) for voidance upon completion of physical security specialist duties described in reference (a).	
(SIGNATURE)	

Figure 2-2.—Acknowledgement of Receipt of Physical Security Credentials.

1. Overall importance/criticality of the command.
 - a. Mission of the command.

b. Importance of the command to essential installation operations.

2. Overall susceptibility/vulnerability of the command to threats.

a. The threat to a specific command as defined by military intelligence and investigative agencies.

b. Ease of access to vital equipment and material.

c. Location, size, deployment and vulnerability of facilities within the activity and the number of personnel involved.

d. Need for tailoring security measures to mission critical operating constraints and other local considerations.

e. Legal jurisdiction.

f. Mutual aid and unilateral assistance agreements.

g. Local political climate.

h. Adequacy of storage facilities for valuable assets and other warfighting materials.

i. Accessibility of the activity to disruptive, criminal, subversive or terrorist elements.

j. Coordination of security forces.

k. Calculated risk.

l. Potential for increase in threat.

m. Possible damage or harm to the civilian community if the item is stolen or lost.

2004. COST OF SECURITY. Physical security expenditures should be based on the cost of the item to be protected, possible damage which loss of the item could inflict upon the

civilian population, and importance of the item to overall national security and command readiness posture. The cost of security is frequently greater than the dollar value of the property protected. Items that are vital to national security or may pose a threat to the civilian population will be provided additional security commensurate with their sensitivity and the threat.

2005. COORDINATION. Physical security of separate installations/organizations in the immediate geographic area will be coordinated with the installations/organizations and local civilian law enforcement agencies or host government representatives. On Marine Corps installations, the installation commander will coordinate physical security measures employed by tenant activities, regardless of the military command, service or agency represented. Physical security of all AA&E and other hazardous material held by tenant activities will be closely coordinated. Planning that may result in the physical relocation of an organizational element, physical changes to a facility, or a realignment of functions will include the Provost Marshal/Security Officer to ensure that security considerations are identified.

2006. SECURITY CONSIDERATIONS. Security measures to be considered when developing physical security plans include, but are not limited to the following:

1. Personnel screening and indoctrination.
- ▶ 2. Security/protection for vulnerable points/assets/**critical infrastructure** within the activity.
3. Security force organization and training.
4. Personnel identification and control systems.
5. Use of physical security hardware (e.g., electronic security systems (ESS), barriers, access control systems).
6. Key and lock control.

7. Coordination with other security agencies.
8. Designation of restricted areas.

2007. CALCULATED RISK. Calculated risk is the concept that dictates when there are limited resources available for protection, possible loss or damage to some supplies or portions of the activity is risked to ensure a greater degree of security to the remaining supplies or portions of the activity. For example, precious metals should be given protection priority over less valuable property items. However, security controls shall not be relaxed to the degree that controls for less valuable items are disregarded and accountability lost.

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 3

SECURITY MEASURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
SECURITY MEASURES	3000	3-3
▶ PHYSICAL SECURITY SURVEY PROGRAM	3001	3-3
▶ LOSS PREVENTION	3002	3-5
▶ LOSS REPORTING	3003	3-5
PERIMETER AND AREA PROTECTION AND CONTROL	3002	3-7
AREA DESIGNATION	3003	3-8
SIGNS AND POSTING OF BOUNDARIES	3004	3-15
KEY SECURITY AND LOCK CONTROL	3005	3-17
SAFES, CONTAINERS, VAULTS AND STRONGROOMS	3006	3-21
SECURITY CHECKS	3007	3-21
PARKING OF PRIVATELY OWNED VEHICLES (POV)	3008	3-22
TRAFFIC CONTROL	3009	3-23
SECURITY OF SELECTED, SENSITIVE INVENTORY ITEMS, DRUGS, DRUG ABUSE ITEMS AND PRECIOUS METALS	3010	3-21
▶ PROTECTIVE LIGHTING	3010	3-23

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 3

SECURITY MEASURES

3000. SECURITY MEASURES. Security measures are actions taken to establish or maintain an adequate command physical security posture. Collectively, these measures develop attitudes and habits conducive to maintaining good security practices and eliminating existing or potential causes of security breaches and vulnerabilities.

▶ 3001. PHYSICAL SECURITY SURVEY PROGRAM. The physical security survey **program provides** ~~is~~ a systematic evaluation of the overall security of a given facility or activity and should not be regarded as an inspection or investigation. Surveys identify deficiencies and **provide** corrective measures to the commander. This information is provided in order to present and preserve a sound security posture. Programs and systems examined will be physical (e.g., lighting, barriers, locks) and procedural (e.g., access control, lock and key control, property accountability). The concept is to design and implement a system that uniformly protects the facility. Some organizations have specific security requirements outlined in additional orders that complement the requirements of this Manual. In those instances, the security requirements set forth in those directives will be addressed as part of the survey.

▶ 1. Aboard Marine Corps installations, physical security surveys will be conducted ~~on an annual basis~~ by school-trained military police personnel possessing **the additional** MOS 5814 (Physical Security/~~Crime Prevention~~ Specialist), and a Secret clearance. Personnel conducting these surveys serve as a representative of the installation commander for the purpose of evaluating the overall installation security posture. Due to the fact some **surveys** ~~evaluations~~ encompass certain restricted areas, physical security personnel will require access when acting within the scope of their duties.

2. Physical security surveys will be scheduled with the responsible organization. The command requesting/requiring

Coordinating Draft for Review 10 June 2004

3001 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

the survey will assign an individual to assist the physical security specialist during the course of the survey. Additionally, briefings will be conducted with the commander or designated representative prior to and upon completion of the survey.

- ▶ 3. Physical security surveys will be completed using the **CMC(PS) mandated Physical Security Survey Reporting System**, or **at those activities where there is no Physical Security Survey Reporting System the NAVMC Form 11121 or an equivalent electronic copy will be utilized.** ~~An~~ **guide for completing the example physical security survey** is provided in Appendix D.
- ▶ 4. **Physical Security Survey Checklists, tailored to a specific type of facility, can be obtained from the local Provost Marshal's Physical Security Unit.**
- ▶ 5. **The following types of physical security surveys will be conducted:** ~~at the following facilities:~~
 - ▶ a. Arms, Ammunition and Explosive (AA&E) Survey
 - (1) **All Arms, Ammunition and Explosive (AA&E) storage facilities (including Ammunition Supply Points, production buildings, and temporary storage in ready service magazines and lockers) will be surveyed.**
 - (2) **AA&E surveys will be conducted on an annual basis, subsequent surveys will not exceed 365 days.**
 - (3) **A statement will be placed in Block 17 of NAVMC 11121 indicating whether the facility does/does not meet the requirements of this Manual.**
 - ▶ b. Antiterrorism Construction Standard Surveys
 - (1) **All inhabited and primary gathering facilities will receive a survey.**
 - (2) **All inhabited and primary gathering facilities will receive an initial Antiterrorism Construction Standard Survey,**

and a subsequent survey only when the facility has been retrofitted by 50% or more.

(3) This survey will be conducted independently of all other surveys, which may result in facilities requiring two surveys to fulfill all of the requirements.

(4) Identified antiterrorism construction standard deficiencies will be listed on the NAVMC 11121, as they normally would appear for any other type of survey.

(5) A statement will be placed in Block 17 of NAVMC 11121 indicating whether the facility does/does not meet the requirements of reference (i).

~~b. Disbursing offices using Chapter 5 of reference (g). Appendix F is provided as a guide.~~

~~c. Facilities which conduct significant cash transactions, such as banks and credit unions, using Appendix G as a guide.~~

~~d. Exchange facilities using Appendix G as a guide.~~

~~e. Storage facilities, containing sensitive and/or high value materials, using Appendix H as a guide.~~

~~f. All other restricted areas and facilities, not previously identified, and mission critical areas designated in writing by the installation commander.~~

~~5. Physical security surveys of classified facilities will be stored and protected in accordance with references (b) and (c), pursuant to the security classification afforded the highest level of material contained within.~~

► c. Classified Military Information (CMI) Facility Surveys

(1) Physical security surveys of classified **military information (CMI) facilities** ~~material storage/classified material control center (CMS/CMCC)~~ will be structural in nature, **not administrative or procedural.** ~~and~~

(2) CMI surveys will be conducted on an eighteen month basis, subsequent surveys will not exceed 548 days.

(3) The installation commanding officer ~~security manager~~ is ~~will be~~ responsible for the inspection program of subordinate commands as prescribed in references (b) and (c). ~~administrative procedural requirements.~~

(4) A statement will be placed in Block 17 of NAVMC 11121 indicating whether the facility does/does not meet the structural requirements of reference (b). Physical Security Specialist will not indicate the level of CMI a facility can hold.

d. Mission Essential Vulnerable Area (MEVA) Surveys

(1) All other restricted areas and facilities, not previously identified, and mission-critical areas designated in writing by the installation commander will be surveyed.

▶ (2) Mission Essential Vulnerable Area Surveys will be conducted on an annual basis, subsequent assessments will not exceed 365 days.

▶ 6. Physical security surveys will be categorized For Official Use Only (FOUO), and are exempt from mandatory public disclosure under provisions of the Freedom Of Information Act (FOIA).

▶ 7. Destruction of surveys will be accomplished by the shredding or tearing. Records of destruction are not required.

▶ 8. Physical security surveys will be generated, staffed, signed, and delivered to the commanding officer of the unit surveyed within 30 days of the survey control date.

▶ 9. Physical security surveys will be signed by the Provost Marshal or another designated officer in writing.

10. Original surveys will be maintained for a period of three years by the affected facility and the Provost Marshal's ~~office~~ Physical Security Unit.

~~3002. LOSS PREVENTION. A vigorous loss prevention program is essential in every Marine Corps organization. Losses can be minimized by application of a comprehensive loss prevention program consisting of, but not limited to: loss analysis, proper use of available investigative and police resources, employee loss prevention education, application of firm corrective measures, administrative personnel actions, and pursuit of prosecution.~~

~~3003. LOSS REPORTING~~

~~1. Missing, Lost, Stolen or Recovered (M L S R) government property reports will be submitted as required by reference (h). The command security officer is the focal point for M L S R reporting.~~

~~2. Effective reporting of losses and maintenance of loss trend analyses is essential to determining the scope of the loss prevention program that must be developed.~~

~~3. Historically, audit and inspection reports have shown that not all required reports are submitted and actual losses have greatly exceeded reported losses. Nevertheless, actual losses must be reported so that accurate assessments can be made. To this end, steps must be taken to ensure those reportable losses and accountable individuals are identified. This can be accomplished by matching property inventories, requests for investigations, inventory adjustments and submitting loss reports.~~

3002. PERIMETER AND AREA PROTECTION AND CONTROL

▶ 1. Prior to making decisions to employ security measures, a threat assessment must be obtained from NCIS and a vulnerability assessment **conducted**, per reference (j) **and a risk analysis must be performed** to determine the degree of physical security required. Extensive and costly security measures may be necessary to protect certain items of security interest. However, in each case the commander is responsible for complying with established security requirements while working to achieve economy. To achieve this objective, security requirements must

Coordinating Draft for Review 10 June 2004

3003 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

be clearly understood. Additionally, the criticality and vulnerability of the asset must be evaluated in relationship to a ranking of a potential threat. A specific level of security must be calculated to ensure the best possible protection for the threat level in a cost-effective manner. Only after the above preliminary factors are addressed can proper controls be instituted.

2. Installation or perimeter and area protective controls are the first steps in providing actual protection against certain security hazards. These controls include barriers and other security measures. They are intended to define boundaries and may be used to channel personnel and vehicular access. Security barriers may be natural or structural and are addressed in Chapter 5.

3. Enclave ("Island") Security Concept. Enclaving involves the ~~provision of~~ concentration of security measures at specific sites within an installation or activity. It is the preferred method for securing relatively small restricted areas and other critical/essential assets requiring a higher degree of protection than the installation itself. Segregating certain areas and assets and concentrating security measures and resources is more cost effective. A restricted area may be separately fenced, lighted, alarmed or guarded, or the area may be "enclaved" without fencing the entire installation perimeter with standard chain link fencing. Enclaving does not eliminate the requirement to identify and post installation perimeters.

~~— b. Installations that elect to adopt enclaving to protect assets as a temporary or permanent alternative to required perimeter standard fencing must submit a waiver or exception request per paragraph ——. Requests must indicate the type of perimeter fencing planned and/or other compensatory security measures planned or in place.~~

3003. AREA DESIGNATION. Different areas and tasks require varying degrees of security interest and importance. The degree of security is dependent upon their purpose, the nature of the work performed within, and information and/or materials concerned. To address these concerns, facilitate operations and simplify the security system, a careful application of restrictions, controls, and protective measures is essential.

In some cases, the entire area may have a uniform degree of security importance requiring only one level of restriction and control. In others, the degree of security importance will require further segregation of certain security interests.

1. Areas will be designated as either restricted areas or non-restricted areas. Restricted areas are established in writing by a commanding officer within his/her jurisdiction. These areas are established per reference (e). ~~"pursuant to lawful authority and promulgated pursuant to DoD Directive 5200.8, and Section 21, Internal Security Act of 1950; Ch. 1024, 64 stat. 1005; 50 U.S.C. 797)."~~

a. Commanding officers will publish and inform the installation commander, in writing, all areas under their control that are designated as restricted areas. Particular attention will be paid to those areas that are vital to or of substantial importance to national security.

b. Installation commanders will publish a consolidated list of all restricted areas aboard the installation to include tenant command restricted areas. This list will be published annually, and will specify whether or not an area is vital to or substantial to national security. This list will be designated For Official Use Only at a minimum.

2. Restricted Areas. There are three types of restricted areas, which are established in order of importance: Level One, Level Two, and Level Three restricted areas. All restricted areas shall be posted simply as restricted areas per the sign provisions set forth in this paragraph 3004 so as not to single out or draw attention to the importance or criticality of an area. Restricted area designation is often associated with areas storing classified information; however, there are other valid reasons to establish restricted areas to protect security interests (e.g., assets/areas identified as mission critical/sensitive; AA&E; nuclear material; protection of certain unclassified chemicals, precious metals or precious metal-bearing articles; funds; drugs; or articles having high likelihood of theft).

► a. Level One. The least secure type of restricted area, it contains a security interest that if lost, stolen, compromised,

Coordinating Draft for Review 10 June 2004

3003 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

or sabotaged would cause damage to the command mission **and** ~~or~~ national security. It may also serve as a buffer zone for Level Three and Level Two restricted areas, thus providing administrative control, safety, and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement may or may not permit access to a security interest or asset.

▶ b. Level Two. The second most secure type of restricted area, it may be inside a Level One area, but is never inside a Level Three area. It contains a security interest that if lost, stolen, compromised, or sabotaged would cause serious damage to the command mission **and** ~~or~~ national security. Uncontrolled or unescorted movement could permit access to the security interest.

▶ c. Level Three. The most secure type of restricted area, it may be within less secure types of restricted areas. It contains a security interest that if lost, stolen, compromised or sabotaged would cause grave damage to the command mission **and** ~~or~~ national security. Access to the Level Three restricted area constitutes, or is considered to constitute, actual access to the security interest or asset.

d. The general rule is that decisions regarding designations of restricted areas and their levels are at the discretion of the commanding officer, however, the following critical areas will be designated as specified below.

(1) Level One

(a) Motor Pools.

(b) Tank ramps, tank compounds, and tank housing facilities.

▶ (c) Fuel issue points and storage tanks (**500 - 999 gallons**).

(d) Funds and negotiable instrument storage areas.

(e) Provost Marshal Office (PMO) Desk

Sergeant/Dispatcher area, ESS monitoring spaces, and Military Working Dog (MWD) facility.

(2) Level Two

(a) Aircraft hangers, ramps, parking aprons, flight lines and runways.

(b) Aircraft rework areas.

(c) Aircraft and AA&E Research, Development, Test, and Evaluation (RDT&E) Centers.

(d) AA&E storage facilities and processing areas (including ammunition supply points, production building, and temporary storage in ready service magazines and lockers) ~~(including gunparks and ammunition supply points)~~. (Additional requirements are outlined in Chapter 8.

▶ (e) Fuel depots and bulk storage tanks **(1000 gallons or greater)**.

(f) Installation, depot and critical communications, computer facilities, and antenna sites.

(g) Installation, depot, and critical assets power stations, transformers, master valve, and switch spaces.

(3) Level Three

(a) Nuclear, biological, chemical (NBC) special weapons research, testing, storage, and maintenance facilities.

3. Minimum Security Measures Required for Restricted Areas.

▶ a. Level One. The following minimum security measures are required for Level One restricted areas:

(1) A clearly defined perimeter. The perimeter may be a fence, the exterior walls of a building or structure, or the outside walls of a space within a building or structure. If the

perimeter is a fence or an exterior wall it must be posted with restricted area signs per this Manual. Lighting and barrier requirements are set forth in Chapters 3 and 5. Points of ingress will be posted in accordance with paragraph 3004 of this Manual.

(2) Admission of individuals (military, civil service, contractors, official visitors) who require access for reasons of official business, who render a service (vendors, delivery people), and other visitors as authorized by the Commanding Officer.

(3) Secured during non-working hours.

(4) When secured and not adequately equipped with an operational ESS (point and area sensors), security force personnel will randomly check after normal working hours for signs of attempted or successful unauthorized entry, and for other activities that could degrade the security of the restricted area. Security checks are not required for areas adequately equipped with an operational IDS.

► b. Level Two. The following minimum security measures are required for Level Two restricted areas:

(1) A clearly defined and protected perimeter. The perimeter will be a fence or the exterior walls of a building or structure. If the defined and protected perimeter is the outside walls of a space within a building or structure, it must be inside a Level One restricted area. If the perimeter is a fence or wall, it must be posted with restricted area signs per this Manual. Lighting and barrier requirements are set forth in Chapters 3 and 5. Points of ingress will be posted in accordance with paragraph 3004 of this Manual.

(2) Admission only to personnel whose duties require access and who have been authorized in writing by the commanding officer. Controlled admission of individuals (military, civil service, contractors, official visitors) who require access for reasons of official business, who render a service (vendors, delivery people), and other visitors as authorized by the Commanding Officer. Such persons and all other visitors will be

escorted by an authorized/cleared activity escort at all times, and the security interest will be protected from compromise.

(3) A personnel identification and access control system (an electronic control system with the capability of recording ingress and egress may be used to accomplish this) is required. If a computer access control or logging system is used, it must be safeguarded against tampering. During working hours, use of an access list and entry/departure log is suggested for all personnel but is not required. All visitors will be logged in and out in an entry/departure log at all times.

(4) Secured during non-working hours.

(5) When secured, checked once per 12-hour shift if adequately equipped with an operational ESS (point and area sensors), or twice per 12-hour shift for those facilities without an operational IDS. Security force personnel will check for signs of attempted or successful unauthorized entry, and for other activities that could degrade the security of the restricted area.

► c. Level Three. The following minimum security measures are required for Level Three restricted areas:

(1) A clearly defined and protected perimeter. The perimeter will be a fence or the outside walls of a space within a building or structure. If it is the outside walls of a space within a building or structure, it must be inside a Level One or Two restricted area. If the perimeter is a fence or wall, it must be posted with restricted area signs per this Manual. Lighting and barrier requirements are set forth in Chapters 3 and 5. Points of ingress will be posted in accordance with paragraph 3004 of this Manual.

(2) Ingress and egress controlled by guards or appropriately trained and cleared personnel.

(3) Admission only to personnel whose duties require access and who have been authorized in writing by the commanding officer. Controlled admission of individuals (military, civil

service, contractors, official visitors) who require access for reasons of official business, who render a service (vendors, delivery people). Such persons and all visitors will be escorted by an authorized/cleared activity escort at all times, and the security interest will be protected from compromise.

(4) A personnel identification and access control system (an electronic control system with the capability of recording ingress and egress will be used to accomplish this) is required. The computer access control or logging system must be safeguarded against tampering. An access list and entry/departure log will be used for all personnel at all times.

(5) Secured during non-working hours. When secured, an operational ESS (point and area sensors), or security personnel must control access to the area.

(6) When secured, checked twice per 12-hour shift if adequately equipped with an operational ESS (point and area sensors), or twice per 8-hour shift for those facilities without an operational IDS. Security force personnel will check for signs of attempted or successful unauthorized entry, and for other activities that could degrade the security of the restricted area.

d. Assets that are considered as vital to or of substantial importance to the overall mission and national security are identified in reference (k). Figure 2-2 from reference (k) is provided in Figure 7-1 of this Manual. It contains information designed to assist commanders in determining the levels of security that should be provided for various types of assets beyond the standards contained in paragraph 3003(2)d of this Manual.

4. Personnel and Vehicle Administrative Inspections. All instructions designating restricted areas will include procedures for conducting inspections of persons and vehicles entering and leaving such areas. To be effective, administrative vehicle and personnel inspection operations must be conducted on a random basis. The activity security officer will ensure they are conducted. Procedures will be coordinated with the cognizant Staff Judge Advocate and approved, in writing, by the installation commander/commanding officer or

authorized representative.

5. Non-Restricted Areas

a. A non-restricted area is an area under the jurisdiction of an organization where access is either minimally controlled or uncontrolled. Such an area may be fenced, or open to uncontrolled movement of the general public. An example of a non-restricted area is a visitor or employee parking lot that is open and unattended by guards. After working hours it may be closed, patrolled, and converted to a restricted area. Another example is a personnel office where the general public is authorized access during working hours without being required to check in or register with duty personnel. Access is normally minimally controlled. In most cases further security authorization, such as a security clearance would not be required for access. An off base housing area would normally be considered a non-restricted area. Non-restricted areas will not be located inside restricted areas.

b. Installations and organizations contain a number of facilities where military personnel, their dependents, civilian employees and their families are permitted access by displaying vehicle decals or by presenting appropriate identification cards (issued based on employment or status only). These facilities include exchanges, commissaries, administrative offices, dispensaries, clubs, recreational facilities, etc. Areas containing such facilities will normally be considered non-restricted areas. However, the facilities themselves may have internal spaces that necessitate designation as restricted areas.

3004. SIGNS AND POSTING OF BOUNDARIES

1. Restricted areas (including buildings) will be posted at designated primary entry points with signs approximately three feet by three feet in size with proportionate lettering. Signs will read as follows:

Coordinating Draft for Review 10 June 2004

3004 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

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.
INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U.S.C. 797

2. Perimeter barriers of all restricted areas will be posted with signs measuring approximately twelve inches by eighteen inches in size with proportionate lettering. Signs will read as follows:

WARNING
RESTRICTED AREA
KEEP OUT
Authorized
Personnel Only

3. Installation/Marine Corps property boundaries will be posted at all points of ingress with signs approximately three feet by three feet in size with proportionate lettering. Signs will read as follows:

WARNING
U. S. MARINE CORPS PROPERTY
AUTHORIZED PERSONNEL ONLY
AUTHORIZED ENTRY ONTO THIS INSTALLATION CONSTITUTES CONSENT TO
SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL.

INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U.S.C. 797

4. Perimeter boundaries will be posted with signs measuring approximately eleven inches by twelve inches in size with proportionate lettering. Signs will read:

U. S. GOVERNMENT PROPERTY
NO TRESPASSING

5. Where a language other than English is prevalent, restricted and non-restricted area warning notices will be posted in both languages.

6. The interval between signs posted along restricted areas will not exceed 100 feet.

7. The interval between signs posted along perimeter boundaries will not exceed 200 feet.

8. All barrier signs will be placed so as not to obscure the necessary lines of vision for security force personnel.

9. Color Code. All signs shall be color coded to provide legibility from a distance of at least 100 feet during daylight hours under normal conditions. The following color codes are recommended for installation/activity and restricted/non-restricted area perimeter signs:

a. All words except "WARNING" will be black.

b. The word "WARNING" will be red.

c. All wording will be on white backgrounds to obtain maximum color contrast.

10. Signs will be properly maintained. Defective and faded signs will be replaced.

11. These signs may be contracted for or produced locally or acquired through the Naval Surface Warfare Center Division (NAVSURFWARCENDIV), Code 4044, 300 Highway 361, Crane, IN, 47522-5001, commercial (812) 854-5812, DSN 482-5812.

3005. KEY SECURITY AND LOCK CONTROL. Each Marine Corps organization must establish a strict key and lock control program supervised by the command security officer.

Coordinating Draft for Review 10 June 2004

3005 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

Included in this program are all keys, locks, padlocks and locking devices used to protect or secure restricted areas, activity perimeters, security facilities, critical assets, classified material, sensitive material and supplies. Not included in this program are keys, locks and padlocks for convenience, privacy, unclassified administrative or personal use.

► ~~The Navy Lock and Key Control Guide (Ashore), June 1988, prepared by the Naval Facilities Engineering Service Center, 1100 23rd Avenue, Port Hueneme, CA 93043-4370, is an excellent source for additional data regarding establishing and maintaining a key and lock control program.~~

► 1. Key Access Control Officer. The **access key** control officer will be designated in writing by the commanding officer and be directly responsible for all security-related key and lock control functions. Normally, the **key access** control officer will be subordinate to the organization security officer. At those organizations where the security and lock program is too small to warrant a subordinate designation, the security officer may assume this function. The **key access** control officer will conduct an annual inventory of all controlled issued keys and will maintain appropriate logs and records. **Appendix F provides an example key inventory form.** Inventory records will be retained for three years ~~or completion of the next Inspector General inspection cycle, whichever is greater.~~

► 2. Key Access Control Custodian. The head of each major functional area (e.g., department, directorate, etc.) within an organization will designate in writing an **key access control** custodian who will be responsible to the **key access** control officer for all keys controlled by that functional area. Each custodian will inventory keys and log accounts ~~at least~~ semiannually. **Appendix F provides an example key inventory form.** The record of this inventory shall be retained for three years. ~~or completion of the next Inspector General's inspection cycle whichever is greater.~~

3. Central Key Room. Duplicate keys, key blanks, padlocks (key and combination type), and key-making equipment will be stored in a central key room. Access must be controlled and the space must be secured when not in use. Duplicate keys will be provided protection equivalent to the asset/area that original

keys are used to secure. Controlled keys (e.g. AA&E, master, and classified material storage area keys) will not be duplicated at any time for any reason nor removed from the installation/site without prior written consent of the security officer/provost marshal.

a. At those organizations where the security key and lock program is too small to warrant a central key room, a locked security container constructed of 20-gauge steel may be used to provide protection of duplicate keys, blanks and associated equipment.

b. Access to the container will be strictly controlled and the container custodian will be assigned in writing.

► 4. Rotation and Maintenance. Security locks, padlocks, ~~combinations,~~ and lock cores designated as high security shall be rotated from one location to another within the same level areas of protection (e.g., Level Two area locks and cores stay within Level Two areas, etc.) ~~at least~~ annually. Rotation is accomplished to guard against the use of illegally duplicated keys and for regular maintenance to avoid lockouts or security violations due to malfunctions.

5. Criteria for Issuing Keys. Keys for security locks and padlocks will be issued only to those persons with a need approved by the activity security officer. Convenience or status is not sufficient criteria for issue of a security key. Certain categories of security assets have specific rules concerning the issue and control of keys affording access to them. The security officer is responsible for developing and enforcing rules for key issue as part of the access control function.

► 6. Key Control. The central key room **custodian**, and each **access control key** custodian/sub-custodian must develop and maintain a **key control register system** identifying key serial number, name and signature of individual receiving keys, date and hour of issuance, signature of individual issuing keys, key return date and time, and name and signature of individual receiving returned keys. **Appendix F provides an example key inventory form.** ~~or other identifying information on hand, keys issued, to whom, date and~~

~~time the keys were issued and returned, and the name and signatures of persons drawing or returning a security key.~~

▶ Continuous accountability of keys is required. **Key control registers will be maintained at least 3 years after the last entry.**

▶ a. Keys will not be left unattended or unsecured at any time. When not attended, that is in use or in the physical possession of authorized personnel, keys will be secured in containers which provide protection commensurate with that for the materials to which the keys allow access.

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

c. In the event of lost, misplaced, or stolen keys, the affected locks or cores to locks will be replaced immediately.

d. The number of keys shall be held to the absolute minimum. Master keying of locks and the use of a masker key system is prohibited.

e. Inventories of keys and locks shall be conducted semiannually. Inventory records shall be retained in activity files for 3 years.

7. Padlock In-Use Security. When the door, gate, or other equipment which the padlock is intended to secure, is open or operable, the padlock will be locked to the staple, fence fabric, or other nearby securing point to preclude the switching of the padlock to facilitate surreptitious entry.

8. Lock Control Seals. Inactive or infrequently used gates must be locked and have seals affixed. The approved seal is the car ball end seal, Military Specification MIL-S-23769C.

▶ Security personnel should be instructed that lack of free play (approximately one-eighth inch) indicates the possibility of tampering and a follow-up examination of the seal should be conducted. Seals will be serialized, stored, **and safeguarded** in the same manner as prescribed herein for keys, ~~and all seals will be inventoried annually~~. The security officer will control

placement of entrance seals and account for seal numbers on-hand, issued and used.

9. Procurement of Locks and Padlocks. All locks and padlocks used for low, medium and high security applications will meet the minimum military specifications for that level of security use. The security officer must approve all security lock and padlock procurements.

10. Lockouts. All lockouts at restricted areas or buildings will be reported to the **Access key** control officer (or duty officer, as appropriate) for the organization having responsibility for the facility. The commanding officer of the facility will direct an investigation of the incident.

▶ 11. Combinations. Only personnel who have the responsibility and required skills shall change combinations to security containers and safes.

a. Combinations will be changed:

(1) When first placed in use.

(2) When an individual knowing the combination no longer requires access to it.

(3) When a combination has been subject to compromise.

b. Maintain a record for each security container or safe showing the location of each, the names, home addresses, and home telephone numbers of all persons having knowledge of the combinations. Use SF 700, "Security Container Information," for this purpose.

▶ 3006. CLASSIFIED SECURITY CONTAINERS, VAULTS AND ~~STRONG~~ SECURE ROOMS. Security containers, vaults and ~~strong~~ secure rooms will conform to the specifications contained in reference (b).

3007. SECURITY CHECKS

Coordinating Draft for Review 10 June 2004

3008 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- ▶ 1. Each organization must establish a system for daily after-hours security checks of restricted areas, facilities, containers, barriers and buildings to detect any deficiencies or violations of security standards. Deficiencies or violations must be reported to the security officer, commanding officer, and the Provost Marshals Office (PMO). Each deficiency or violation will be reviewed by the organization security officer, and a record maintained of all corrective actions taken. Records of security checks will be maintained for a period of ~~one~~ **three** years.
- 2. This review of subsequent actions is intended to resolve the present deficiency or violation and to prevent recurrence.
- 3. All deficiencies, violations, breaches of rules and regulations, and criminal incidents discovered and handled by the security force will be recorded.

3008. PARKING OF PRIVATELY OWNED VEHICLES (POV)

- ▶ 1. Vehicle parking is prohibited within ~~303~~ feet of any inhabited structure or ~~802~~ feet from **billeting** ~~troop housing~~ and primary gathering places in order to minimize danger in the event of fire or explosion. Privately owned vehicles will not be parked in Level Two and Three restricted areas or within ~~303~~ feet of doorways leading into or from buildings primarily used for the repair, rework, storage, packaging or shipping of government material and supplies. Commands must ensure that parking restrictions are addressed in MILCON and renovations projects as outlined in Antiterrorism/Force Protection orders and directives. Management of the parking assignments is not a function of the security officer.
- ▶ 2. At activities where parking is allowed inside Level One **restricted** areas, parking areas will be located away from Level Two and Three restricted areas and separately fenced in such a manner that occupants of vehicles must pass through an access control point prior to entering the actual restricted area ~~facility~~.

3009. TRAFFIC CONTROL. The installation provost marshal will establish a traffic control program in accordance with reference (1).

▶ 3010. PROTECTIVE LIGHTING

1. General. Protective or security lighting is an integral part of both the command security and safety posture. This lighting provides a continuing degree of security commensurate with that during daylight hours. It increases the effectiveness of security forces performing their duties and has considerable value as a deterrent to criminal activity. Requirements for protective lighting at an activity are determined by the asset(s)/area(s) to be protected, facility layout, terrain, and weather conditions. In the interest of finding the best possible mix between resource allocation, financial commitment, and effective security, each situation must be carefully studied. The overall goal is to provide the proper environment to perform duties such as identification of badges and personnel at gates, inspection of unusual or suspicious circumstances, etc. Where lighting is impractical, additional compensating measures must be instituted.

2. General Principles and Guidelines. Paragraph 4.7 of reference (m) provides general principles and guidelines for exterior protective (security) lighting. These guidelines, including Table 8 (Lighting Specification (Foot Candles)), and Table 9 (Illuminated Area Specification) should be applied by activities when determining protective lighting requirements. When protective lighting is installed and used, the following basic principles, in addition to those provided in reference (m) should also be applied:

a. Provide adequate illumination or compensating measures to discourage or detect 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 avenues of approach and provides relative darkness for patrol roads, paths and posts. To minimize exposure of security force personnel, lighting at entry points will be directed at the gate and the guard shall be in the shadows. This type of lighting technique is often called glare projection (see paragraph 3010 3(a)1).

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

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

f. Avoid drawing unwanted attention to restricted areas.

g. During planning stages, consideration should be given to future requirements of CCTV and recognition factors involved in selection of the type of lighting to be installed. Where color recognition will be a factor, full spectrum (high pressure sodium vapor, etc.) lighting vice single color should be used.

h. Choose lights that illuminate the ground or water but not the air above. These lights must penetrate fog and rain.

3. Types of Protective Lighting Systems

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

(1) Glare Projection Lighting. This system uses lights slightly inside a security perimeter and directed outward. This method is useful where the glare of lights directed across surrounding territory will neither annoy nor interfere with adjacent operations. It is a deterrent to potential intruders because it makes it difficult to see inside the area being

protected. It also protects security personnel by keeping them in comparative darkness and enabling them to observe intruders at a considerable distance beyond the perimeter.

(2) Controlled Lighting. 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 water 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. Care should be taken to minimize or eliminate silhouetting or illuminating security personnel on patrol.

b. Standby Lighting. 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 Lighting. A system (stationary or portable) consisting of movable manually operated searchlights which may be lighted during hours of darkness or as needed. This system is normally used to supplement continuous or standby lighting.

d. Emergency Lighting. 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 alternative power sources, such as installed or portable generators or batteries.

4. Protective Lighting Parameters. It is not the intent of this Manual to prescribe specific protective lighting requirements. Except for minimum standards described in paragraph 5, the commanding officer must decide what other areas or 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 the activity mission and its role in the overall national defense structure.

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

d. Availability of fiscal resources (procurement, installation, and maintenance costs).

e. Energy conservation.

5. Minimum Standards

a. Fence lines, water boundaries and similar areas that cannot be patrolled need not be illuminated. Where these areas are patrolled, sufficient illumination should be provided to assist the security force in preventing intrusion.

b. Vehicular and pedestrian gates used for routine ingress and egress will be sufficiently illuminated to facilitate personnel identification and access control.

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

d. Airfields, aircraft, petroleum storage areas, and other mission critical areas will be provided with sufficient illumination for the security force to detect, observe and apprehend intruders.

e. Protective lighting will be checked weekly by the security force to ensure all lights are operational.

6. Emergency Power. Restricted areas with protective lighting should have an emergency power source located within the restricted area and provisions must be made to ensure immediate availability of emergency power in the event of primary power source failure. The emergency power source shall be adequate to sustain security lighting and communications requirements and

other essential services. Emergency power sources should start automatically. Battery-powered lights and essential communications should be available at all times at key locations within the restricted area in the event of complete failure of primary and emergency sources of power. Emergency power systems will be tested quarterly and the results will be recorded/logged and maintained for a period of three years.

7. Protection - Controls and Switches. Controls and switches for protective lighting systems will be inside the protected area and locked or guarded at all times. An alternative is to have controls in a central location similar to or as a part of the system used in intrusion detection alarm central monitoring stations. High impact plastic shields may be installed over lights to prevent destruction by stones, air rifles, etc.

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 4

SECURITY FORCES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	4000	4-3
FUNCTIONS OF THE SECURITY FORCE	4001	4-3
THE SECURITY FORCE	4002	4-3
SIZE OF THE SECURITY FORCE	4003	4-4
SECURITY POSTS	4004	4-5
POST REQUIREMENTS AND CONSIDERATIONS	4005	4-5
SECURITY FORCE ORDERS	4006	4-6
SECURITY FORCE TRAINING	4007	4-7
SECURITY FORCE EQUIPMENT	4008	4-7

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 4

SECURITY FORCES

4000. GENERAL. The security force constitutes one of the most important elements of an organization's physical security program. Security forces consist of Marines, **civilians, and contract guards** specifically organized, trained, and equipped to provide law enforcement and physical security for the command. Other security forces include Marines assigned as interior guard, who also require organization, training and equipment specific to their assigned duties. Whereas law enforcement personnel duties pertain to an entire installation, interior guard personnel are normally assigned to provide security to an organizational area or asset. Properly used, these Marines are one of the most effective and useful tools in a comprehensive, integrated physical security program.

4001. FUNCTIONS OF THE SECURITY FORCE. Regardless of the type of personnel employed, security force functions fall into four general categories:

1. Prevent/deter theft and other losses caused by fire damage, accident, trespass, sabotage, espionage, etc.
2. Protect life, property and the rights of individuals.
3. Enforce rules, regulations and statutes.
4. Detect, deter and defeat terrorism.

4002. THE SECURITY FORCE. Marines guard Marine Corps assets and installations. Reference (n) requires that Marines performing a security function will be armed. In that capacity, the security force is an integral part of the physical security program and commanders have a responsibility to maintain and support the program. The following security forces may be employed:

Coordinating Draft for Review 10 June 2004

4003 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

1. Military Police. Military police are those Marines, possessing MOS 58XX, who are assigned to installation provost marshal offices and perform installation law enforcement duties.

2. Interior Guard. An interior guard force consists of Marines organic to an organization who are specifically trained and organized for the purpose of providing security for specific areas or assets under the cognizance of the organization commanding officer. Personnel assigned interior guard duties will fall under the direct control of the guard officer. Interior guard personnel will normally not perform law enforcement duties.

3. Other Forces. At those organizations not located aboard a Marine Corps installation, commanders are encouraged to utilize federal, state, and local police in support of law enforcement and security requirements. Private security companies may be utilized in support of security applications. In overseas locations, SOFA agreements may require foreign nationals to serve as a part of the security force. In this application, rules and regulations governing these foreign personnel will be based on those requirements addressed in the SOFA agreement.

4003. SIZE OF THE SECURITY FORCE. The size of the security force is dependent upon many factors, some of which are:

1. Size and location of the installation/site.
2. Geographic characteristics of the installation/site.
3. Mission.
4. Number, type, and size of restricted areas.
5. Use and effectiveness of physical security equipment.
6. Availability of non-organic, supporting security forces.
7. Installation population and composition.
8. Criticality of assets being protected.

In all instances, the size of the security force will allow for a reaction force capability.

4004. SECURITY POSTS. Because no two installations/sites have the same exact security requirements, it is not feasible to establish Corps wide criteria for the required number of posts. In all cases, posts will be based upon the security mission being performed and not upon convenience. Individual installations/sites must analyze security post requirements utilizing a systems approach. Pertinent to this approach is consideration of available manpower, existing security measures and planned upgrades, such as closing of non-essential posts and the employment of mechanical and electronic security technology (barriers, electronic security systems, etc.).

4005. POST REQUIREMENTS AND CONSIDERATIONS

1. Gates. Gates will be limited to the minimum number required to permit expeditious flow of traffic in and out of the installation or activity. 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.

2. Perimeter. The justification for perimeter posts is in direct proportion to the necessity for preventing unauthorized entry. Perimeter protection requires a combination of approved fencing, protective lighting and electronic security systems, all supported by fixed posts and mobile patrols operating in relatively small areas. Some sites may meet security requirements by using nothing more than fixed and mobile posts.

3. Area Posts. Guard force strength must be commensurate with the importance of the area/assets being guarded and the threat. See Chapter 3 for restricted and non-restricted areas.

4. Motorized Patrols. One person vehicular patrols are normally adequate.

5. Visitor Escorts. Full-time posts for visitor escorts will not be established within restricted areas. The person receiving visitors will escort visitors in and out of the area as determined by the commanding officer and applicable orders.

► 6. MCESS Operator. MCESS Operators/dispatchers monitor alarm, Mass Notification Systems, and any CCTV monitors used in conjunction with the MCESS for the purpose of assessing alarm activations. Normally MCESS Operators/dispatchers are assigned the additional duty of Radio Dispatcher, but his/her primary responsibility is to MCESS. Additionally:

- a. Operators will be armed.
- b. Operators will be trained in the proper operation of the MCESS. Training for MCESS Operators is discussed in Chapter 6.

4006. SECURITY FORCE ORDERS. The commanding officer of each installation/organization will publish and maintain security force orders. Security force orders are the written and approved authority of the commanding officer for members of the security force to execute and enforce regulations. The orders will be signed by the installation/organization commanding officer and a copy of post specific orders will be maintained at each post. These orders will be brief, concise, and specific and written in a clear and simple language. The orders will be reviewed annually. The orders, at a minimum, will contain the following:

1. Special orders for each post which specify the limits of the post, specific duties to be performed, hours of operation, and required uniform, arms, and equipment.
2. Specific instructions in the application and use of deadly force as provided in reference (n), and detailed guidance in the safe handling of weapons.
3. Training requirements for security personnel and designated posts.
4. Security force chain of command.

4007. SECURITY FORCE TRAINING. All personnel assigned duties with a security force will meet the following minimal training requirements:

1. The use of force and the safe handling of firearms, to include issue and turn in.
2. Weapons training and qualification as outlined in reference (n).
3. Legal aspects of jurisdiction and apprehension.
4. Mechanics of apprehension, search, and seizure.
5. General and special orders and all aspects of the security force order.
6. Use of security force equipment.
7. Threat specific training (e.g., vehicle bomb searches, terrorism awareness, weapons of mass destruction (WMD) awareness).

4008. SECURITY FORCE EQUIPMENT. Types and quantities of equipment made available to the security force are based on available resources and the mission being performed. Situation requirements such as host nation agreements, assets being protected, and threat conditions also have an affect on equipment issued to security force personnel. The following types of equipment may be employed in support of the security mission:

1. Weapons and Ammunition. Weapons and ammunition will be standard issue items of government property. The use and possession of privately owned weapons by military personnel in the performance of assigned duties is strictly prohibited. Security force personnel will be assigned a service pistol, service rifle, or shotgun while in the performance of their duties, as determined by the installation/organization commanding officer. Requirements for carrying configuration and additional ammunition are provided in reference (n). The

Coordinating Draft for Review 10 June 2004

4008 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

commanding officer may authorize the issue of special equipment (shotguns, machine guns, grenade launchers), provided security force personnel have received required weapons training as directed by reference (o).

2. Vehicles. Security force personnel will be provided sufficient vehicles to conduct required patrols and to dispatch reaction force personnel. Security force vehicles will also be:

- a. Equipped with radios.
- b. Configured for the safe transportation of additional passengers and those persons apprehended or detained by security force personnel.
- c. Operated by personnel possessing valid U.S. Government Motor Vehicle Operator's Identification Card (SF-46) for all vehicles that they may be assigned to operate as required by TM 11-240.
- d. Military police vehicles will conform to requirements identified in reference (l). In addition to the above, military police vehicles will be equipped with law enforcement specific equipment (mobile radios, sirens, code-lights, prisoner security cages, and spotlights/takedown lights). Law enforcement equipment will conform to both federal and state regulations.

3. Communications

a. A communications system is required to allow the security force to complete assigned missions. Communications will be available to all posts. Reliable systems aid in the establishment of a safe and secure working environment. The type of system employed must be tailored to meet the specific needs of the individual installation/organization. Installation/organization communications-electronics offices will be involved in both the procurement of communications equipment and coordination of frequency assignment. Systems employed will be tailored to meet the specific requirements of the security force. Procurement planning for communications systems will include, but is not limited to, the following considerations:

(1) Flexibility of the system for expansion, updates, etc.

(2) Criticality of assets.

(3) Susceptibility to interference or unauthorized monitoring.

(4) Size of the installation and/or area requiring coverage.

(5) Requirement and placement of repeaters.

(6) Terrain and structures.

b. There will be at least two separate and distinct forms of communications available to security force personnel, one must be two-way voice radio (this requirement **is only applicable to military police/response force personnel** and is not applicable to Reserve Centers). A duress button, in those facilities equipped with ESS, is recognized as a form of communication. A phone is also recognized as a form of communication.

~~c. A duress code will be established for use by security force personnel to covertly alert other security force personnel of a need for immediate assistance in the event of emergency. Duress codes should be limited to one or two words, simple, and easily recognizable. Duress codes will be changed monthly or when thought to have been compromised. Training concerning the use of duress codes by security force personnel will be included in security force training.~~

d. Each security force component (military police and interior guard) will have a separate and distinct frequency. These systems must employ two-way communications capable of reaching all posts. The system must incorporate provisions for emergency power and be capable of operating on more than one frequency/channel.

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 5

BARRIERS AND OPENINGS

	<u>PARAGRAPH</u>	<u>PAGE</u>
THE PURPOSE OF PHYSICAL BARRIERS	5000	5-3
TYPES OF BARRIERS	5001	5-3
GENERAL CONSIDERATION	5002	5-4
▶ ENTRY CONTROL FACILITIES	5003	5-5
PERIMETER OPENINGS	5004	5-9
GATES	5005	5-9
FENCES	5006	5-10
TEMPORARY BARRIERS	5007	5-13
VEHICLE BARRIERS	5008	5-13
INSPECTION OF BARRIERS	5009	5-13
WALLS	5010	5-14
CLEAR ZONES	5011	5-14
PATROL ROADS	5012	5-15
DOORS, WINDOWS, SKYLIGHTS AND OTHER OPENINGS	5013	5-15
SEWERS, CULVERTS AND OTHER UTILITY OPENINGS	5014	5-16
UTILITY POLES, SIGNBOARDS AND TREES	5015	5-16

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 5

BARRIERS AND OPENINGS

5000. THE PURPOSE OF PHYSICAL BARRIERS. Physical barriers control, deny, impede, delay, and discourage access to restricted and non-restricted areas by unauthorized persons. They accomplish this by:

1. Defining the perimeter of restricted areas.
2. Establishing a physical and psychological deterrent to entry and providing notice that entry is not permitted.
3. Optimizing use of security forces.
4. Enhancing detection and apprehension opportunities by security personnel in restricted and non-restricted areas.
5. Channeling the flow of personnel and vehicles through designated portals in a manner which permits efficient operation of the personnel identification and control system.

5001. TYPES OF BARRIERS. The two types of barriers are Natural and Manmade. Figure 5.1 provides a list of both natural and manmade barriers and their functionality in security planning.

Barrier Function	Natural Barrier	Manmade Barrier
Established Boundary	River, valley, forest line	Walls, fences, hedges
Isolate Activity or Discourage Visitors	Mountains or hills, jungle dense growth, desert	Walls, fences, berms, canals, moats
Aid Detection of Unauthorized Entry or Intrusion		Electronic detection devices mounted on boundary, sand strips at boundary or areas to be isolated, electronic devices

Impede Vehicle Passage	Rivers, swamps, natural terrain features	Fences, walls, Jersey bounce barriers, specially designed vehicle barriers, aircraft arresting cable
Prevent External Visual Observation	Forests, natural terrain features	Berms, earthworks, walls, solid fences, masonry block screens, translucent glass blocks, polycarbonate sheets, shutters, awnings, draperies
Minimize Ballistic Material Penetration		High berms, earthworks, steel-reinforced concrete or solid-fill masonry walls, blast shields fabricated from steel-ply materials, ballistic-resistant glazing

Figure 5-1. - Security Barrier and Functionality

5002. GENERAL CONSIDERATIONS. Physical barriers delay, but can rarely be depended upon to stop a determined intruder. To be effective, such barriers must be augmented by security force personnel or other means of protection and assessment. In determining the type of barrier required, the following will be considered:

1. Physical barriers will 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. When a section or sections of natural/structural barriers provide a lesser degree of protection, other supplementary means to detect and assess intrusion attempts must be used.

2. 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 should

only be used either in conjunction with an IDS, or other form of alarm system supported by 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 in identifying the location of high risk items. The criticality, sensitivity, and vulnerability of certain areas may require the use of a taut wire fence, which provides the added advantages of an intrusion detection system.

3. The perimeter boundaries of all Marine Corps installations, including Marine Corps Reserve Centers that are either independently located or jointly located with other services, must be posted and will be fenced where feasible. Whenever fencing is impractical, compensatory security measures (e.g., increased patrols) will be implemented.

4. In establishing any perimeter or barrier, consideration must be given to providing emergency entrances in case of fire or other emergency. However, openings will be kept to a minimum consistent with the efficient and safe operation of the facility and without degradation of minimum security standards.

5. Construction of new security barriers and removal of existing barriers at restricted areas must be approved by the security officer. Construction and modification of barriers will be scheduled to maintain security levels or provide commensurate security for the activity.

► 5003. ENTRY CONTROL FACILITIES. Entry Control Facilities (ECFs) are primary points of ingress and egress to Marine Corps installations. The access control ECFs are extremely important to the defense in depth and risk mitigation mission of the installation. The primary objectives of the ECF are to secure the installation from unauthorized access and intercept contraband (weapons, explosives, drugs, etc.) while maximizing vehicular traffic flow. Reference (o) provides further guidance concerning ECFs.

1. Function - ECFs serve as primary ingress/egress points for installations for pedestrian, personal owned vehicles, commercial vehicles, government owned garrison, and tactical

vehicles. The ECFs also serve as the focal point for processing visitors and inspecting vehicles prior to admission.

a. Not all functions are required at each ECF, and installation long-range planning documents need to include plans for establishing ECFs that separate civilian and commercial functions. Figures 5-2 and 5-3 illustrate the general relationships between the different functions of an ECFs.

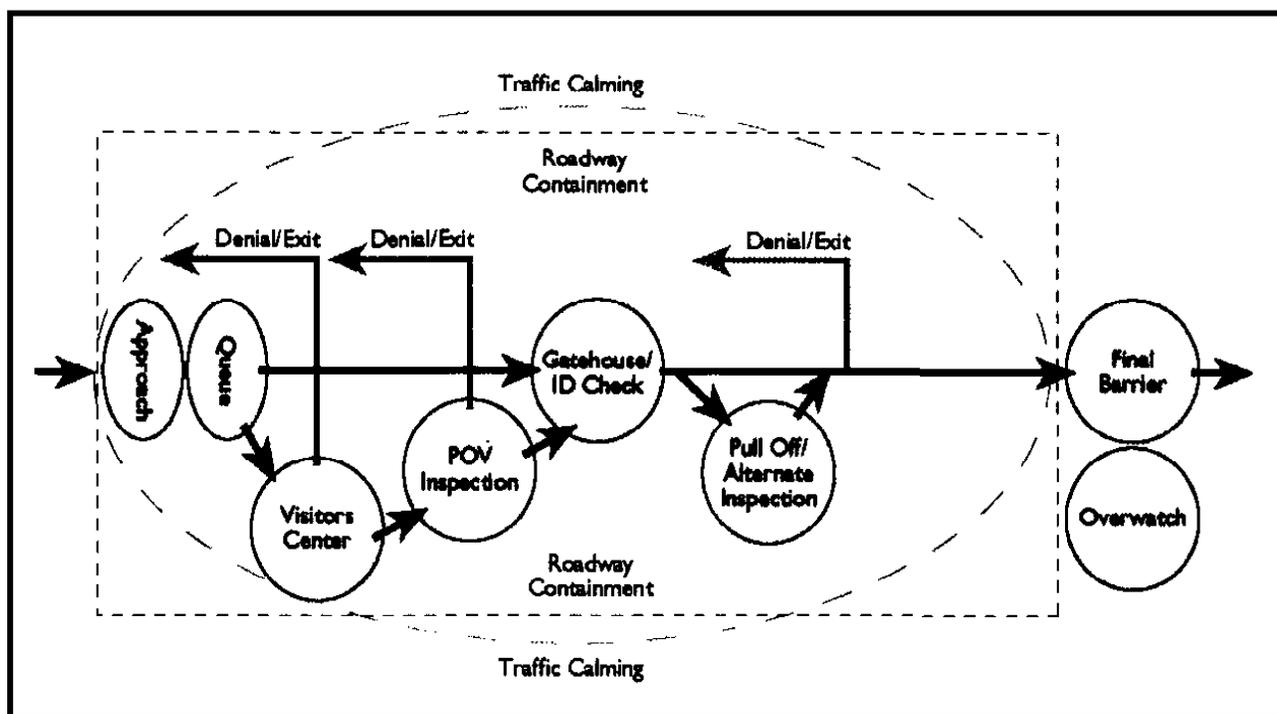


Figure 5-3. - Example Authorized Personnel/Visitors ECF

b. Inspection functions must be included in all planned ECFs.

2. Organization. ECFs are organized in four zones, Approach, Access Control, Response, and Safety. Within each zone, there is a desired function that allows for ease of traffic operation and volume. Based on limited space, some functions will be combined. Figure 5-4 provides a diagram identifying the four ECF zones.

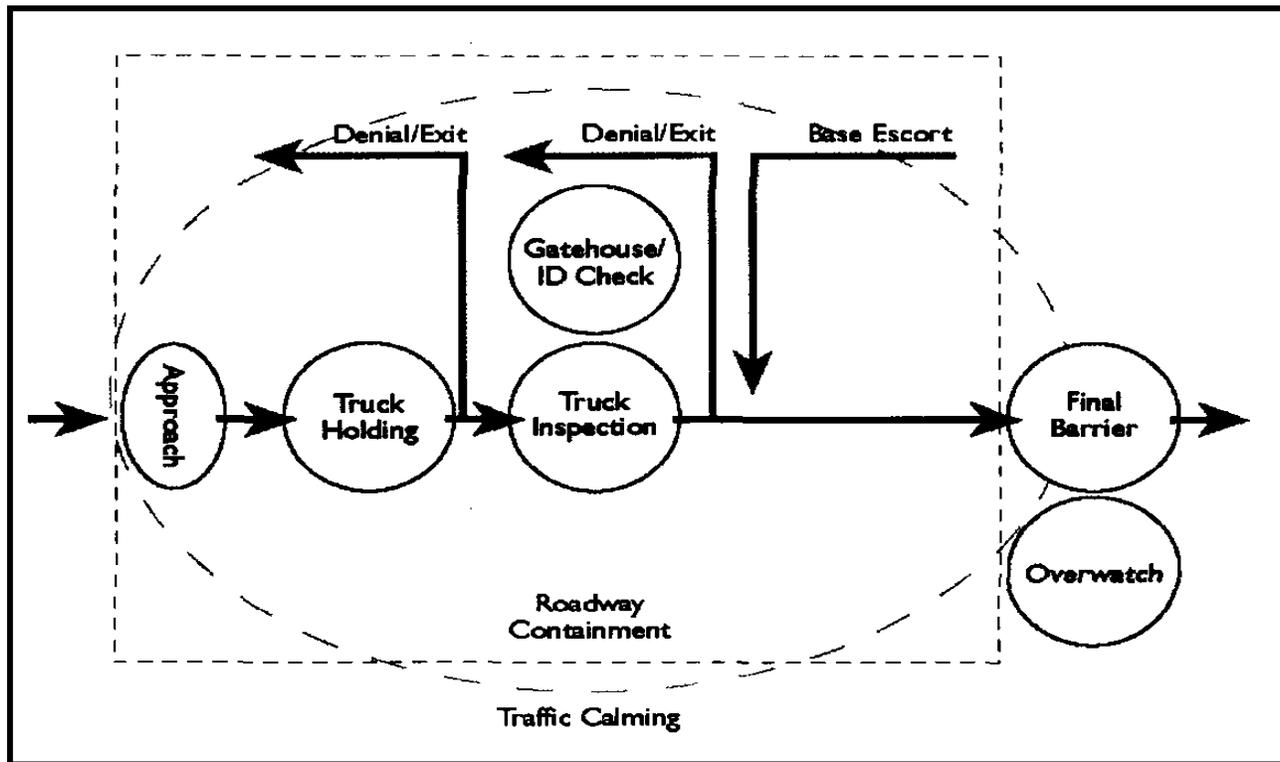


Figure 5-4. - Example Commercial Traffic ECF

a. The Approach Zone is an area all vehicles must pass through before reaching the actual checkpoint and serves as an interface between civilian roads and the installation.

b. The Access Control Zone is the main body of the ECF and includes the gatehouse and all traffic management equipment to support traffic flow and visitor control.

c. The Response Zone is an area that extends beyond the Access Control Zone and defines the end of the ECF. Within the response zone there is a requirement for a final denial barrier. A final denial barrier allows personnel to close off access to the remainder of the installation. The Response Zone needs to be designed in order to allow security personnel to react to a threat, operate the final barriers, and close the ECF if necessary.

d. The Safety Zone is an area that extends through all zones in order to establish acceptable standoff distances to mitigate effects of an explosion on personnel, buildings, or assets.

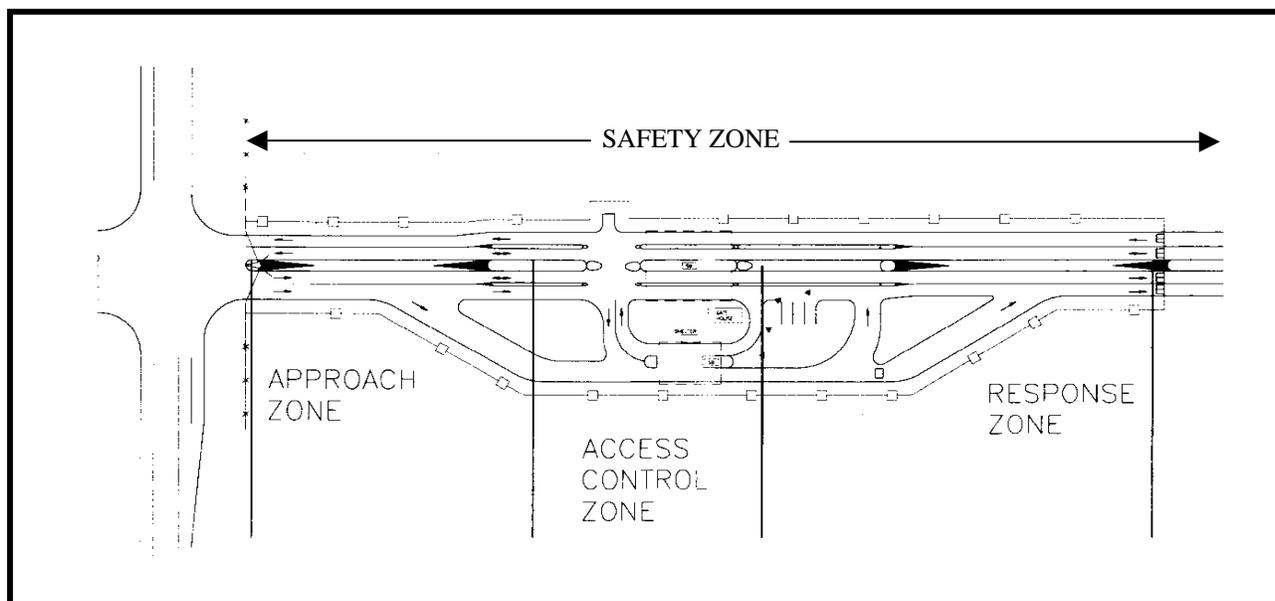


Figure 5-2. - ECF ZONES

3. Design Priorities. ECFs provide a first line of defense for the installation, however, they also present an indication of the installation's professionalism. Design priorities must present a strong, professional, security posture in the design of the total package, including gatehouses, man-stands, inbound and outbound lanes and visitor centers. Design considerations that must be addressed, in order of priority are Security, Safety, Capacity, and Image.

a. Security - The first priority of the ECF is security. The ECF is widely recognized as the first line of defense and the legal line of separation from the adjacent civilian property(s). The ECF must be able to operate at all Force Protection Conditions (FPCONs) and support all measures including 100% vehicle inspections. The ECF will have the capacity for supporting Random Antiterrorism Measures (RAMs) and must possess

and maintain security features that protect against vehicle threats and illegal entry.

b. Safety - Safety of security personnel posted at the ECF is paramount. Security personnel must have a safe work environment that supports force protection against varied attacks. The ECF must also protect security personnel from negligent drivers, and be designed to provide a comfortable working environment giving consideration to climate, location, and orientation. Installations should make every effort to separate pedestrian Entry Control Points (ECPs) and vehicle ECFs. In those instances where this is not possible, ECF designs will facilitate safe passage for vehicles and persons entering and exiting the facility in an orderly manner.

c. Capacity - The ECF must be designed to maximize an orderly traffic flow during peak periods of ingress and egress and without compromising safety and security. Design analysis must include vehicle volume validation, and setback considerations, based on any impact (especially during increased FPCONs) on adjacent public roads.

d. Image - The ECF must be designed to convey the Marine Corps' professionalism and commitment to the protection and safety of Marines, Sailors, their families, and civilian Marines who reside and work aboard the installation and security of facilities and resources.

5004. PERIMETER OPENINGS. Openings in the perimeter barrier will be kept to the minimum necessary for the safe and efficient operation of the activity. Openings shall be constantly locked, guarded by the security force or otherwise secured to prevent unauthorized entry or exit. When locked and not under constant surveillance, the locking device used shall provide the same degree of security as the perimeter barrier.

5005. GATES

▶ 1. Number and Location. Gates will be limited to the number

consistent with efficient operations. Such factors as the centers of activity and personnel and vehicular traffic flow inside and outside the area should 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 will be under ~~security force~~ control **of a guard or appropriately trained and cleared personnel**. They will provide protection equivalent to the fences or barriers of which they are a part when not in use. These gates will be locked to form an integral part of the fence when closed.

2. Inspection. When not in active use and controlled by a guard, gates, turnstiles and doors in the perimeter barrier will be locked and frequently inspected by security patrols. Locks will be rotated at least annually. Security for the keys and combinations to locks on these gates is the responsibility of the key control officer or key custodian, as determined by the commanding officer.

3. Pedestrian Gates. Pedestrian gates and turnstiles will be designed so that only one person may approach the guard at a time. Some gates may be closed between rush hours. Where possible, pedestrian and vehicular gates should be clearly separated.

4. Vehicular Gates. Vehicular gates when physically practical will be set well back from any public highway so temporary delays caused by identification control checks at the gate will not cause traffic hazards. There will also be sufficient space at the gate to allow for spot checks, inspections, searches and temporary parking of vehicles without impeding the flow of traffic.

5006. FENCES

1. Chain Link Fencing. Chain link fencing is the type of manmade barrier most commonly used and recommended for security purposes. Chain link fencing will be used to enclose restricted areas where fencing is required. Mesh openings will not be covered, blocked, or laced with material that would prevent a clear view of personnel, vehicles, or material in

outer perimeter zones/areas. In those instances where a commanding officer determines application of a covering to be more advantageous to protecting the asset within the fenced area, a waiver or exception request must be submitted per paragraph 1014. The following standards apply:

a. Fabric. The standard fence fabric will be 9-gauge zinc or aluminum-coated steel wire chain link with mesh openings not larger than two inches per side and a twisted and barbed selvage at top and bottom.

b. Fabric Ties. Only 9-gauge steel ties will be used. If the ties are coated or plated, the coating or plating will be compatible with the fence fabric plating and coating to inhibit corrosion.

c. Height. The standard height of a security fence is eight feet. This includes a fabric height of seven feet, plus a top guard. Building connections will be higher. An additional four to five feet of fencing height should be added at the building connection point out at least 10 feet away from the building.

d. Fencing Posts, Supports and Hardware. All posts, supports, and hardware for security fencing will meet the requirements of Federal Specification RR-F-191J/GEN of 22 July 1981. All fastening and hinge hardware will be secured in place by peening or welding to allow proper operation of components, but prevent disassembly of fencing or removal of gates. All posts and structural supports will be located on the interior side of the fencing. Posts will be positively secured into the soil to prevent shifting, sagging or collapse in accordance with reference (m).

e. Reinforcement. Taut reinforcing wires will be installed and interwoven or affixed with fabric ties along the top and bottom, on the interior, of the fence to stabilize the fence fabric.

f. Ground Clearance. The bottom of the fence fabric must be within two inches of firm soil or buried sufficiently (concrete footings or gravel may be used) in soft soil to compensate for shifting soil.

g. Culverts and Openings. Culverts under or through a fence shall be of ten inch pipe or a cluster of such pipe. Openings under or through a fence will be secured with material of equal or greater strength than the overall barrier. All openings, which have an area of 96 square inches or greater and which penetrate the restricted area perimeter barrier, will be protected by securely fastened **No. 4 (12.7-mm) reinforcing bars, 9 inches on center, in each direction and staggered on each face to form a grid approximately 4-1/2 inches square.**

h. 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, ladders, etc.) allow passage over, around or under the fence.

i. Top Guards. A top guard must be constructed on all perimeter fences and may be added on interior enclosures. 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 will be permanently affixed to the top of fence posts to increase the overall height of the fence at least 1 foot. Three strands of 12-gauge barbed wire, equally spaced, must be installed on the supporting arms. Top guards constructed in a "Y" or triangular frame (double outriggers), which face both inward and outward, are acceptable. The top guard of fencing adjoining gates may range from a vertical height of 18 inches to the normal 45-degree outward protection, but only for sufficient distance along the fence to open the gates adequately.

2. Taut Wire Fences. A taut wire fence may be installed as a stand-alone 7-foot fence with 31-inch double outriggers equipped with sensor devices. A three-quarter inch steel cable will be attached to support posts 30 inches above the ground to stop lightweight vehicles from crashing through the barrier. The sensor system consists of horizontal wires spaced about 4 inches apart and connected to a central detection device tensioned between two anchor devices. Attempts to cut or climb this type fence will generate an alarm at the central monitoring station.

3. Alternative Fencing. Where a boundary passes through an isolated area that is not patrolled and through which vehicular passage is impossible, the boundary may be defined with a two to four strand 12-gauge barbed wire fence approximately four feet high. It will be posted as required in paragraph 3004.

5007. TEMPORARY BARRIERS. In some instances, the temporary nature of a restricted area does not justify the construction of permanent perimeter barriers. When this occurs, the resulting lack of security will be compensated for with additional temporary security measures.

► 5008. VEHICLE BARRIERS. The use of vehicle barriers such as crash barriers, obstacles, or reinforcement systems for chain link gates at uncontrolled avenues of approach can impede or prevent unauthorized vehicle access. See reference (m) for guidance on barriers, and reference (p) for vehicle barriers at ECFs. ~~Additionally, the manual entitled "Terrorist Vehicle Bomb Survivability Manual (Vehicle Barriers)" is available from the Naval Facilities Engineering Service Center, 1100 23rd Avenue, Port Hueneme, CA 93043-4370.~~

5009. INSPECTION OF BARRIERS. Security force personnel will check security barriers at least weekly for defects that would facilitate unauthorized entry. Personnel must be alert to the following:

1. Damaged areas (cuts in fabric, broken posts).
2. Deterioration (corrosion).
3. Erosion of soil beneath the barrier.
4. Loose fittings (barbed wire, outriggers, fabric fasteners).
5. Growth in clear zones that would afford cover for possible intruders.

5010 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

6. Obstructions which afford concealment or aid entry/exit for an intruder.

7. Evidence of illegal or improper intrusion or attempted intrusion.

5010. WALLS. Walls, floors, and roofs of buildings may also serve as perimeter barriers. Buildings, structures, waterfronts and other barriers used instead of (or as a part of) a fence line must provide equivalent protection to the fencing required for that area. Therefore, all windows, doors and other openings or means of access must be guarded or properly secured.

5011. CLEAR ZONES

1. An unobstructed area or clear zone will be maintained on both sides of, and between, permanent physical barriers of restricted and non-restricted areas. Vegetation in such areas will not exceed 6 inches in height. **Though not desirable, the following exceptions are allowed: light poles, fire hydrants, steam pipes, etc; barricades used for explosive safety; and entry control facilities at ingress and egress points, however, these items must not be located in such a manner that they can be used by an intruder for concealment or as a climbing aid.**

2. ~~An inside~~ Interior/exterior clear zones will be a minimum of ~~least 30~~ 3 feet, with the interior clear zone being no less than 20 feet, and the exterior clear zone being no less than 10 feet. Additional stand-off requirements for inhabited, billeting, and primary gathering areas are discussed in reference (i), and may be greater than those listed above. Where possible, a larger clear zone should be provided to preclude or minimize damage from thrown objects such as incendiaries or bombs.

3. ~~The outside clear zone will be 20 feet or greater between the perimeter barrier and any exterior structures, vegetation or any obstruction to visibility.~~

4. ~~In~~ In those activities 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 obstacle to compensate for the close proximity of aids to concealment or access; **however, this does not negate the requirement for maintaining the appropriate clear zones.** Where property owners do not object, the area just outside the fence should be cleared to preclude concealment of a person. All fencing will be kept clear of visual obstructions such as vines, shrubs, tree limbs, etc., which could provide concealment for an intruder.

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

5. In addition to security, clear zones also provide the safety feature of a **33** ~~50~~-foot wide firebreak between the activity areas, structures or storage facilities and adjoining areas. It is especially important to maintain clear zones during periods of high fire risk.

6. Commands must ensure that clear zone requirements are addressed in MILCON and renovation projects as outlined in AT/FP orders and directives.

5012. PATROL ROADS. When the patrolled perimeter barrier encloses a large area (a large area is considered one square mile or greater), an interior perimeter road in all areas not affected by impassable terrain features must be provided for use by security patrols.

5013. DOORS, WINDOWS, SKYLIGHTS, AND OTHER OPENINGS. Building exterior doors will provide protection commensurate with the requirement for proper protection of the assets accessible through those doors. Unless the width-to-height ratio absolutely eliminates the physical possibility of intruder entry, openings will be protected by securely fastened 9 gauge

wire mesh, framed and permanently bolted to the structure. Such openings are also considered inaccessible to personnel when they are 18 feet or more above ground level and 14 feet or more distant from buildings, structures, etc., outside the perimeter. Protective screens have the additional value of preventing projectiles such as rocks, hand grenades, bombs and incendiaries from being hurled through the windows from outside the perimeter. Hinges to all doors will be located on the interior of the door. In locations where the hinge pin is exposed to the exterior, hinges will be peened, spot welded, or equipped with a hinge secure pin.

5014. SEWERS, CULVERTS, AND OTHER UTILITY OPENINGS. Unless the width-to-height ratio absolutely eliminates the physical possibility of intruder entry (for example, one inch by 6 inches) all utility openings which penetrate the perimeter or restricted area barrier will be protected against surreptitious entry. Protection of these opening may be accomplished by securely fastened bars, grills, locked manhole covers or other equivalent means which provide security commensurate with that of the perimeter or restricted area barrier. Bars and grills across culverts, sewers, storm sewers, etc., create a hazard and are susceptible to clogging. This hazard must be considered during construction planning. All drains/sewers will be designed to permit rapid clearing or removal of grating when required. Removable grates will be locked in place.

5015. UTILITY POLES, SIGNBOARDS, AND TREES. Utility poles, signboards, trees, etc., located outside of and within 15 feet of the perimeter barrier of the activity, present a possible assistance to entry. To reduce this possibility, the perimeter barrier will be staggered to increase the distance to more than 20 feet and may be heightened to the extent necessary to prevent entry. Otherwise, the hazard must be removed. Should these utility poles, signboards, trees, etc., also obstruct the visibility of the guards, they must be at least 20 feet outside the perimeter barriers.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 6

ELECTRONIC SECURITY SYSTEMS

	<u>PARAGRAPH</u>	<u>PAGE</u>
INTRODUCTION	6000	6-3
GENERAL	6001	6-3
ESS DETERMINATION FACTORS	6002	6-4
ESS POLICY	6003	6-4
TYPES OF SYSTEMS	6004	6-10
MAINTENANCE	6005	6-11
TRAINING	6006	6-12
MCESS OPERATOR RESPONSIBILITIES	6007	6-13
CLOSED CIRCUIT TELEVISION (CCTV).	6008	6-14
AUTOMATED ACCESS CONTROL SYSTEMS (AACS) .	6009	6-23
MASS NOTIFICATION SYSTEMS (MNS)	6010	6-25
MARINE FORCES RESERVE	6011	6-28

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 6

ELECTRONIC SECURITY SYSTEMS

6000. INTRODUCTION. Electronic Security Systems (ESS), **synonymous with Intrusion Detection Systems (IDS)**, are an essential element of any in-depth physical security program. ESS is designed to detect, **by way of electronic detection, and provide timely notification to the MCESS Operator; however, it does not prevent actual or attempted penetrations.** ~~ESS consist of sensors capable of detecting one or more types of phenomena, signal media, and energy sources for signaling the entry or attempted entry into the protected area.~~ The design, implementation, and operation of ESS must contribute to the overall physical security posture and the attainment of security objectives. ~~ESS is designed to detect, not prevent actual or attempted penetrations.~~

6001. GENERAL. ESS ~~systems~~ are used to accomplish the following:

1. Permit more economical and efficient use of security personnel ~~through~~ **by allowing MCESS Operators to control and direct the response of** ~~employment of mobile responding~~ security forces instead of fixed guard posts and/or patrols.
2. Provide additional controls at critical areas or points.
3. Enhance the security force capability to detect and defeat intruders.
4. Provide the earliest practical warning to security forces of any attempted penetration of protected areas.
5. **Provide the MCESS Operator, remote visual assessment to make a rapid and accurate assessment of alarming sensors and the approach of possible intruders from outside the activity.**

6002. ESS DETERMINATION FACTORS. For those facilities requiring ESS, specific regulatory guidance has been provided.

6003 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

In addition to regulatory guidance, the following factors must be addressed to determine the necessity for installation of ESS:

1. Mission.
2. Criticality.
3. Threat.
4. Geographic location of the installation or facility and location of facilities to be protected within each activity or installation.
5. Accessibility to intruders.
6. Availability of other forms of protection.
7. Life cycle costs of the system.
8. Construction of the building or facility.
9. Hours of operation.
10. Availability of a security force and expected response time to an alarm activation.

6003. ESS POLICY

- 1. The ~~Marine Corps Electronic Security System (MCESS)~~ program was established to ensure that ~~all MCESS~~ throughout the Marine Corps are ~~is~~ standardized. **Each** Marine Corps installation has a standard ESS terminating at the installation PMO alarm control center (ACC). The purpose is to serve as the foundation for subsequent ESS procured by CMC(POS) or the installation/command. Prior to the advent of MCESS, individual installations ~~bases~~ were required to fund and install ESS at critical facilities and costs often exceeded the resources available. Critical facilities either had substandard ESS or lacked ESS altogether. Additionally, a diversity of systems used created operational and maintenance problems.

2. Under MCESS, CMC(P~~OS~~) is the program manager for ESS and oversees the funding, procurement, installation, and maintenance of ESS. The focal point for the operation of these systems is the installation provost marshal. These systems may not be modified in any way without prior CMC(P~~OS~~) approval. ~~Modification to the systems must be approved by CMC(P~~OS~~) and the MCESS Technical Support Agency (TSA).~~

▶ 3. CMC(P~~OS~~) has the responsibility for managing the MCESS program for the Marine Corps. All **arms, ammunition, and explosives (AA&E) storage facilities, ~~armories, magazines, and~~ flight lines, and Mass Notification Systems (MNS)** in the Marine Corps are serviced by a single alarm **system** type. Any commercial alarm systems procured that will annunciate at, or be monitored by PMO will be compatible with the ~~AA&E/Flight line~~ MCESS. This will eliminate the proliferation of alarm system types currently installed at PMO.

▶ a. CMC(P~~OS~~) is responsible for funding MCESS installation for AA&E, ~~and~~ flight line, **and MNS** security applications. Any other ESS security project will be funded by the installation/command. Installations/**commands** may continue to use current alarm systems. When ~~a these~~ system reaches the end of the life cycle, it will be replaced with a **MCESS AA&E/flight line** compatible system.

▶ b. In procuring ~~these MCESS compatible non AA&E/flight line~~ systems, installations/**commands** may, when using local funding, elect to have the ~~Marine Corps~~ **MCESS Technical Support Agency (TSA)** install ~~the said~~ system, or they ~~may will may elect to~~ use a contractor **approved by the MCESS TSA** ~~of their choice~~. To maintain system integrity, however, final installation to the PMO ~~ACC annunciator~~ will be accomplished/supervised by engineers and technicians from the ~~Marine Corps~~ **MCESS TSA**. **Additionally,** ~~and~~ compatibility must be certified by the MCESS TSA prior to the integration/connection to MCESS. Compatibility review costs will be borne by the installation.

▶ c. **All alarms responded to by interior guard, military police, or contract guard services** ~~In cases where the installation/organization commander determines~~

~~that an ESS system will annunciate at the PMO. these systems will be compatible with MCESS. Compatibility must be certified by the MCESS TSA prior to the integration/connection to MCESS. Installation and compatibility review costs will be borne by the installation, command, or responsible agency.~~

▶ d. MCESS technical **and maintenance** support ~~may~~ will be arranged for ~~installation and maintenance~~ **all MCESS compatible local contractor installed ESS, which is approved for connection to the MCESS.** ~~With prior CMC(PS) approval, local contractors may install and maintain the system provided that the system and components are compatible with MCESS.~~ **Installations/commands, or responsible agencies may elect to use an approved local contractor to perform maintenance of the MCESS compatible ESS, however, the MCESS TSA must approve the maintenance plan submitted by the contractor. Additionally, the MCESS TSA will be responsible for maintenance from the Remote Terminal Unit (RTU) back to the ACC.**

▶ e. Installations, commands, or responsible agencies that elect to utilize the MCESS TSA to install a locally funded ESS, CMC(PS) will provide the sustainment maintenance and life cycle upgrade.

▶ f. Installations, commands, or responsible agencies are responsible for all maintenance costs determined to be negligence on the part of civilian, military, or contractor personnel acting on the behalf of the installation, command, or responsible agency.

g. ESS installed at less critical facilities (i.e., exchange, commissary) and civilian agencies (banks, credit unions) aboard the installation may or may not be part of the MCESS Program. Therefore, installation commanders are responsible for coordinating the procurement, installation, and maintenance of ESS at such facilities.

▶ h. ESS not compatible with the MCESS ~~systems~~ will not annunciate at PMO and do not require approval from CMC(PS). These systems will annunciate at an off base location with personnel who will notify installation PMO of an alarm. **These types of systems may be used until the end of life cycle**

or 10 years. At which time the system will be replaced with a MCESS compatible ESS. These systems do not require coordination with MCESS TSA.

▶ i. Alarm control centers will be monitored 24 hours a day. ~~with a response force capable of responding to all alarms within 15 minutes.~~ The system will provide an audible and visual alarm identifying the affected area. ACCs will be designated as restricted areas and will be properly protected, with controlled access. Where practical, alarm consoles and central dispatching will be consolidated. New construction will include ballistic protection.

▶ j. Installations will have a response force capable of responding to all alarms within 15 minutes, with the exception of the following:

1) Sensitive Compartmental Information Facility (SCIF) alarms will be responded to within 5 minutes for open storage or 15 minutes for closed storage.

2) Flight line alarms will be responded to within 5 minutes.

3) Arms, Ammunition, and Explosives (AA&E) storage facilities will be responded to within 10 minutes.

k. A daily log will be maintained of all alarms, to include the location and time received, nature of the alarm (false, actual, equipment failure), and the response made. Logs will be maintained for a period of three ~~one~~ years and will be reviewed to identify and correct trends, reliability problems, and/or equipment failures.

▶ l. A MCESS log-file backup will be performed on a monthly basis, and maintained for a period of three years.

m. The MCESS Primary and Secondary File Servers will be backed up each month, each on its own tape. The three most recent File Server backups will be maintained on file.

n. Original site specific MCESS tapes will be maintained on file unless directed otherwise by the MCESS TSA.

4. Access codes for manager level access to MCESS will be restricted to the Provost Marshal's Physical Security Specialists ~~site representatives~~, and MCESS TSA maintenance personnel ~~only~~.

5. MCESS trouble calls will be reported to the MCESS TSA Consolidated Call Center by the Provost Marshal's Physical Security Specialists or MCESS TSA contracted maintenance personnel only. Physical security specialists will be assigned as the primary coordinator between all MCESS users and the MCESS TSA.

a. Call priority will be determined by the need to take compensatory security measures (requirement to assign manpower to provide security normally provided by the MCESS) as a result of the reported failure. Levels of priority are based on the following:

1) Priority 1

a) Prevents the accomplishment of an essential capability.

b) Jeopardizes safety, security, or other requirement designated "CRITICAL".

2) Priority 2. Adversely affects the accomplishment of an essential capability and no work around solution is known.

3) Priority 3. Adversely affects the accomplishment of an essential capability but a work around solution is known.

4) Priority 4

a) Results in user/operator inconvenience or annoyance but does not affect a required operational or mission-essential capability.

b) Results in inconvenience or annoyance for

development or maintenance personnel but does not prevent the accomplishment of the responsibilities of the personnel.

5) Priority 5. Any other effects (e.g. something minor, but you want to document it.

b. The following information is required by the consolidated call center upon notification:

- 1) Call priority
- 2) Site name
- 3) Site point of contact and phone number
- 4) Building number and name
- 5) System Name (MDI, Vindicator, etc.)
- 6) Account, Line, RTU Address, and Zone numbers
- 7) Brief description of failure
- 8) Circumstances of failure

c. Response to a critical failure (compensatory measures have been implemented) will be within 4 hours of notification.

d. Response to a non-critical failure will be within 4 hours on the next normal business day.

e. Physical security specialists or any other person(s) will not contact TSA contracted maintenance personnel directly. Doing so violates Federal Acquisition Regulations (FAR) and subjects those person(s) to potential personal liability for contractor incurred costs.

6. Regardless of whether or not ESS is part of the MCESS Program or funded locally, the following requirements apply to ESS used at installations:

- a. If a computerized ESS is used, it will be safeguarded

against tampering by the operator. ~~Supervisory personnel~~ CMC (PS) will regulate operator access levels.

b. Alarm transmission lines between the protected area and monitoring units will be protected by physical measures and/or electronic line supervision systems. These systems protect against signal cutting, shorting, tampering, splicing, or data substitution.

c. ESS will have an emergency power source to ensure the system's continuous operation. This power source will be provided by an uninterrupted emergency generator or battery source. Batteries will have the capacity to maintain proper operation of the system under normal conditions for a minimum of four hours.

d. Keyswitches, controllers, or other mechanisms used to activate and deactivate the ESS will be installed inside the protected area whenever possible. Components mounted on the exterior will be provided additional protection with a locking assembly, or outfitted with an anti-tamper device. Alarm activation delay devices are installed in order to allow sufficient time for personnel to exit the area after the system has been activated.

e. ESS equipment housing will be equipped with anti-tamper devices that will initiate an alarm signal. The anti-tamper device will be in continuous operation regardless of the ESS mode of operation.

f. All sensors, transmitters, transponders, control units and other ESS components associated with an alarmed facility will be physically located within the protected area whenever possible. Components mounted on the building exterior will be provided additional protection with a locking assembly, or outfitted with an anti-tamper device.

6004. TYPES OF SYSTEMS

1. Local Alarm. Local alarms actuate a visible and/or audible signal, usually located on the exterior of the facility. Alarm transmission lines do not leave the facility. Response is

generated from security forces located in the immediate area. Without security forces in the area, response may only be generated upon report from a person(s) passing through the area or during security checks. Maintenance is conducted through a civilian agency.

2. Central Station. Central station system signals are transmitted to and annunciate in an independent monitoring station that records activations and maintains the on site equipment. The monitoring station is usually managed through a civilian firm with operators and guards/response forces available on a 24-hour basis. Connection to the station is primarily over leased telephone lines. Central station monitoring requires a contract, which may include a lease/purchase clause with the civilian agency. The contract should also include maintenance support.

3. Police Connection. Police connection systems are transmitted to and annunciate at a local police agency dispatch center that records activations. Police personnel respond to activations. A formal agreement with the police department is required to ensure monitoring and response requirements. Maintenance of the system is conducted through a civilian agency.

4. Proprietary ESS Station. Proprietary ESS stations currently exist on, and are the prescribed ESS for Marine Corps installations. The MCESS proprietary station incorporates both the central station and police connection concept. Alarmed facilities aboard installations are connected to an ACC that is monitored 24 hours a day by military police and ~~in some cases,~~ civilian employees. Military police are the primary response force however, in some cases personnel assigned duties as interior guard may be assigned as the response force. Maintenance for the proprietary ~~MCESS system~~ is conducted by the TSA and is coordinated with the installation provost marshal.

▶ 6005. MAINTENANCE. Proper maintenance of an ESS is imperative. Systems not properly maintained may fail to detect intrusion and may yield a high number of false/nuisance alarms. Such alarms cause security forces to lose faith in the system and may result

in activations being ignored. Maintenance requirements will be established per the manufacturer. At a minimum, all ESS ~~systems~~ will receive semi-annual preventive maintenance service. All performed maintenance will be recorded and records will be maintained for a period of **three** ~~one~~ years. Additionally:

1. Follow recommendations of equipment manufacturers and installers.
2. Consider actual experience with systems installed.
3. Comply with more stringent criteria in other security directives when they apply.
4. Testing. All ESS will be tested (at least) quarterly to ensure systems are functional. In the conduct of these tests, all individual sensors will be tested to determine the continued adequacy of their application. Tests will include an interruption of the AC power source to ensure proper transfer to alternate power sources in order to determine functionality of the source. Test results will be retained for a period of **three** ~~one~~ years. For perimeter (flight line) ~~and exterior~~ ESS, randomly selected zones should be tested daily. Depending on the type of sensor, such alarm activations could include touching the fence, walking or running over protected ground, or passing through a sensor beam.
5. **Physical security specialists will not perform troubleshooting or first echelon maintenance on ESS sensors, transmission lines, control stations, or monitoring equipment that are not a part of the MCESS. Doing so subjects those person(s) to potential personal liability for costs incurred due to damages or identified problems not attributed to the initial failure.**

► 6006. TRAINING. Personnel, who operate, perform basic troubleshooting, maintenance, or repairs of MCESS will be trained, **tested**, and ~~by certified personnel~~.

1. Physical Security Specialist

- a. ~~Marine Corps site representatives will possess MOS 5814.~~

Physical security specialists ~~Site representatives~~ are the only **installation** personnel authorized to perform basic troubleshooting and first echelon maintenance **of the MCESS besides MCESS TSA personnel.**

b. **All physical security specialist** will be trained, **tested**, and certified by **either** the ~~Marine Corps contracted~~ MCESS TSA, or interactive computer based training in basic troubleshooting and first echelon maintenance **of the MCESS.** First echelon maintenance is defined in Appendix A ~~will be defined by CMC(POS).~~

2. MCESS Operators

a. MCESS Operators, synonymous with PMO Dispatcher, are required to be trained, tested, and certified in the operation of the MCESS.

b. MCESS Operators will be trained, tested, and certified via interactive computer based training.

c. Marines and civilians who do not pass the MCESS Operator test with an 80 percent or higher will not be certified to operate the MCESS, nor issued an operator log-in and password.

3. Training criteria, whether classroom instruction or interactive computer based material, will be reviewed on an annual basis by the releasing authority.

▶ 6007. **MCESS OPERATOR RESPONSIBILITIES.** MCESS Operators are the first line of defense against unlawful entry into areas or against critical assets that are protected by the MCESS. They are also responsible to the Provost Marshal for the effective operation of the MCESS. Additionally, MCESS Operators will:

a. Maintain security of the MCESS Operating System under their control.

b. Monitor MCESS Operating System alarm statuses.

c. Process alarm status, as presented, and dispatching an armed response force.

- d. Direct the response of security force personnel.
- e. Attempt to ascertain the cause of the area in alarm utilizing information provided by response personnel.
- f. Contact appropriate physical security duty personnel for all problematic alarm activations that cannot be resolved by the response force or the MCESS Operator.

6008. CLOSED CIRCUIT TELEVISION SYSTEMS. Closed Circuit Television (CCTV) Systems are used today in ever widening roles in law enforcement and security. These roles can be broadly categorized as (a) detection, (b) area surveillance, and (c) post incident assessment and analysis. Furthermore, the equipment used to fulfill these roles is expected to remain functional over a wide range of environmental and manmade conditions. CCTV Systems are expected to deliver unfettered quality video in lighting conditions ranging between sunlight to starlight, high contrast ratios (light to dark), and other adverse conditions. While technological advances have solved many of these issues, proper design and application are still major factors in achieving quality video assessment systems, and thusly end-user satisfaction. The following paragraphs addresses major areas of concern, and provides guidance for effectively designing, installing, and operating a CCTV System.

1. POLICY

- a. CCTV Systems will not be utilized to meet constant surveillance requirements.
- b. Installations may continue to use current CCTV Systems until they reach the end of life cycle or the next CMC(PS) sponsored MCESS Upgrade, whichever comes first.
- c. For sites with existing CCTV Systems installed as part of the ESS, procurement of any commercial CCTV Systems to be monitored by PMO must be compatible with the existing ESS CCTV system. The system must be installed or certified by the MCESS TSA. This will reduce the proliferation of systems currently installed at PMO and implement configuration management controls.

d. In procuring CCTV Systems using local funding, installations and activities may elect to have the MCESS TSA install said system or they may elect to use a contractor of their choice. To maintain system integrity, however, final installation and connection to the MCESS will be accomplished and supervised by engineers and technicians from the MCESS TSA.

e. Compatibility, performance parameters, and maintenance plans must be certified by the MCESS TSA prior to the installation, integration, or connection to the MCESS. Those systems failing to meet certification and performance parameters established by the MCESS TSA will not be connected to the MCESS. Compatibility review costs will be borne by the installation or activity.

f. CCTV Systems not compatible with the MCESS will not be monitored by PMO and do not require approval from CMC(PS).

g. Sustainment maintenance will be funded by CMC(PS) on all CCTV Systems, even those procured using local funding, as long as installation is performed by the MCESS TSA.

h. Regardless of whether or not CCTV is part of the MCESS Program or funded locally, the following requirements apply to CCTV Systems installed at installations:

1) CCTV transmission will be point-to-point connectivity utilizing a fiber optic or wireless transmission method. Network connectivity will not be used with security CCTV Systems.

a) Transmission lines for CCTV Systems between the protected area and monitoring station will be protected by physical measures and/or electronic line supervision systems. These systems protect against signal interruption, tampering, splicing, or data substitution. Video loss detection is acceptable for line supervision as long as it is displayed as an alarm event to the ESS.

b) Wireless CCTV Systems will be encrypted to the National Institute of Standards and Technology (NIST) 128.0 byte standard.

2) CCTV Systems will have an emergency power source to ensure the system's continuous operation. This power source will be provided by an uninterrupted emergency generator or battery source. Batteries will have the capacity to maintain proper operation of the system under normal conditions for a minimum of four hours.

3) Security cameras used for forensic purposes or event driven events will be connected to a digital capture system. Digital capture systems used for forensic purposes will be approved for chain-of-custody authentication where the video may be introduced and be required to stand up as evidence in a court of law.

4) Event driven CCTV monitoring devices will not number more than four 15-inch color monitors and will be located within the peripheral vision, to the right and left, of the MCESS Operator.

5) Command driven CCTV monitoring devices will not number more than one 15-inch color monitor and will be located directly to the MCESS Operators front. Additional command driven CCTV monitors can be installed in the direct view of the desk sergeant, but will not be monitored by the MCESS Operator.

6) CCTV monitoring and recording devices will not be located in gatehouses.

2. DESIGN CONSIDERATIONS

a. Environmental Issues. Cameras operate much like a human eye, and factors that affect our ability to see clearly also affect a camera's ability to see clearly. Rain, fog, snow, ice, sleet, sunlight, darkness, scene contrast smog, and haze all affect a camera's ability to capture useful images. When designing and using CCTV, one can only recognize that performance will be degraded during periods of inclement weather. There are some common sense issues that should be considered in every CCTV project. Proper equipment selection and design will mitigate many of these effects and ensure cameras function over the widest range of conditions.

1) When faced with adverse weather conditions (hi/low temperatures, humidity, ice, snow and sleet) it is prudent to ensure that cameras are equipped with environmentally sealed housings, include internal heaters, and are positively pressurized with an inert drying agent (Nitrogen is the most commonly used agent). While these features add cost to the camera, they will help to assure uniform performance over the widest range of conditions.

2) There are many issues associated with lighting that must be considered during the planning and design phases. Since a camera's iris automatically adjusts to ambient light conditions (just as our eyes do), planners and designers should avoid placements that are along the path of the sun and moon. Bright objects will cause the iris to narrow and thus reduce the amount of light allowed to reach the camera's sensing element, and dark places will appear darker and scene visibility can be reduced to zero.

a) The same principles hold true for man made illumination and should be given the same consideration. Street lights, flood lighting, and headlights within the camera's FOV will affect overall performance and should be avoided.

b) Areas with high contrast ratios should also be avoided. Ratios of greater than six to one (6:1) can make viewing the darker areas extremely difficult as the lens' iris will adjust to the lighter area. Natural areas of contrast should be avoided. Man made areas can be mitigated with supplemental lighting. The selection of supplemental lighting should take into account the sensitivity of the camera to the light spectrum. Most monochrome cameras have a high response across the visible light spectrum and tend to peak in the orange to near infrared range. Color cameras have similar response curves though some colors may be lost as available lighting approaches the near infrared range. When selecting supplemental lighting, decisions should be based on the requirement or desired result, and the specific response sensitivity characteristics of the camera.

b. Technology Issues. The two types of video systems are; (a) analog systems, and (b) digital systems. Each type has

advantages and limitations. While detection, surveillance and post-action assessment requirements vary, all requirements have common features and a limited number of equipment solutions. When determining the type of technology to include in a system design, designers and managers need to examine not only those camera qualities that meet their requirements, but also have a full understanding of their associated limitations. Video display and storage technologies are addressed below.

1) Analog systems are typically hardware dependent. They display images on a television-like monitor, record the data to videotape, and can produce paper images with specifically designed printers. Analog technology is extremely dependent on the application environment. Scene lighting is critical to producing quality images. For applications involving after-action analysis, these systems offer a relatively low-cost, high performance solution when used in small quantities. When applied to larger installations, the infrastructure costs rise exponentially. This is due to the wiring requirements (one camera requiring a coaxial cable or fiber back to a central monitoring center).

2) Digital systems are software dependent. Not only can digital images be displayed, recorded, or printed on an array of widely used media, digital images take only seconds to search, focus on a specific scene, resize, crop, enhance quality, and e-mail. The major benefit to digitized video is the ability to store large amounts of digitized images and improving the ability to search and retrieve images quickly. Infrastructure costs are also lower since digital video images can be networked.

3) Cameras. Every camera consists of four basic components - the lens, a view finder system, an image sensor and a processing system. The majority of all cameras combine all four components in one casing. The lens plays a central role in cameras. Due to the difference in size between the sensor of a camera, optical components for digital cameras have to be better than for an analog camera. A variety of lenses are available. Lenses are selected based on the resolution requirements and the distance from the camera's position and the object(s) to be

viewed. Color cameras usually offer lower resolution than black & white cameras.

a) Forward Looking Infrared (FLIR) cameras measure the radiated temperature of animate and inanimate objects within their field of view. These measurements are processed to present useful video images to operators. Scene lighting has no effect on these devices as they measure heat in the infrared range. FLIR technology can provide useful images in the total absence of ambient light. This technology has relatively high procurement and maintenance costs, therefore cost-benefit analysis tools should be applied before these devices are procured and deployed. FLIR cameras can be categorized into two areas;

1) Cooled cameras (short-wave) offer longer range, higher resolution and better adverse weather penetration. These features are offset by two considerations; a) procurement costs that are typically five to ten times the cost of uncooled FLIR cameras and b) a typical cooler life span of 8,000 - 10,000 hours. Cryocooler refurbishment typically costs one fifth the purchase cost and as frequently as every 18 months.

2) Uncooled cameras (medium-wave) typically have shorter range capabilities and lower resolution than cooled cameras. Recent advances in infrared detector manufacturing and lens technology has resulted in uncooled thermal images rivaling those of cooled cameras and are proving effective for surveillance applications at distances up to 3,000 meters. Uncooled FLIR's do not have the maintenance costs associated with cooled cameras.

3) Transmission Methods. The following are two types of connectivity used with video systems.

a) Point-to-point connectivity offers the highest quality. Coaxial cable and fiber optics offer high bandwidth and low loss over long distances resulting in high resolution and frame refresh rates. It also is the most expensive connectivity method. Video systems that utilize balanced twisted copper pairs (telephone lines) are available, but bandwidth and frame refresh rates are significantly lower and

these systems are unable to meet most near real time surveillance requirements. As bandwidth and refresh rates decrease the apparent video quality diminishes, significantly for monochrome and dramatically for color.

b) Network connectivity allows numerous cameras to be physically connected to a single transmission medium and uses computer routers to allow the operator or other software to select which camera will be viewed on a monitor using Internet Protocol (IP) addressing schemes. The advantage is infrastructure costs are greatly reduced since a single cable is run from the monitoring point to the first camera then on to the next and so on. Local Area Networks (LANs) are sometimes used to further reduce costs. Since the video from each camera is present on the network at all times, bandwidth availability is a serious consideration. Managers need to be aware that there is a trade-off to be made when selecting the type of transmission media to be used in a project and that the requirement needs to be critically analyzed to ensure satisfaction.

4) Monitors. Size and resolution play a significant role when choosing video monitors.

a) The diagonal length of the viewing surface usually catalogues a monitor's size. Typical sizes range from nine inches to twenty-one inches. Monitor selection should be based on the actual size and clarity.

b) In the context of video display, resolution can be referred to either as the total number of horizontal lines (analog) or the number of pixels per inch (digital). In either case, it determines the amount of detail that can be resolved. A common mistake is failing to match the specified camera resolution with a display device of equal or higher resolution, which results in image distortion. Flat screen monitors such as LCD and plasma convert analog signals to digital, which means slower speeds than the conventional CRT monitor. Attention must be given to the global aspects of the video system in order to produce a well-engineered, optimized display resolution for the operator.

5) Human Engineering Issues. The above paragraphs focused on environmental and technical factors governing system

selection and design. However, the most effectively designed system will be of marginal use if the human operators are not made a part of the design and implementation equation. The specific areas of operator proficiency requiring managerial and design personnel attention include; Task organization, task management, social issues, and technology.

a) Detection Cameras. Video data need only be presented to an operator when undesired activity is present. The majority of activities are related to motion and there are several technologies and matrix applications rapidly draw an operator's attention to the scene. Video motion detectors and event-driven switching matrices are key in this approach. The important factor is the information is not presented to an operator until his/her attention is required. It's just as important to select scenes that are benign. Normal activity in an area that triggers a sensor or prompts an operator's attention will result in information overload, and thus will tend to be ignored. Monitors displaying this type of data should be located within the peripheral vision of the operator and easily accessible once his/her attention has been captured. Since many cameras may be assigned to this category, but only used when an event occurs, operator fatigue is not as critical a factor. Designers should pay strict attention to factors affecting false alarm rates so as not to overload an operator with meaningless data. Since these types of events are occurring in real-time, operators should be fully familiar with detection areas and should have pre-planned procedures of follow-up actions. If the camera is a pan-tilt-zoom (PTZ) is mounted on an articulating platform (PTZ), operators should possess the knowledge and manual dexterity to rapid manipulate the camera's view as the situation may require.

b) Surveillance Cameras. If the purpose of a camera is to provide surveillance of a specified area, the workload on the operator is significantly increased. In this application, the amount of video data being presented to an operator must be considered. If many cameras are assigned, monitoring options include adding additional personnel to monitoring assignments and use technology to "scroll" through the cameras in a pre-determined order and rate. With each subsequent switch to a new

camera, the operator must orient himself to the new scene and then determine if there have been changes from the last time the scene was presented.

1) Using multiple monitors may alleviate some of this problem, but introduces others. If multiple monitors are assigned, then a single operator is required to split his/her attention between these various monitors. Coupled with the factor that each monitor is presenting different scenes every one to three seconds, information can be easily missed. This activity can be mentally fatiguing, and the amount of time an operator remains in this mode becomes critical. Performance begins to degrade after approximately 30 minutes. After that, though not linear nor true for every individual, the likelihood of an undesired event being seen can diminish to as little as 50% of the time.

2) Security officers should be aware of these limitations and carefully ascertain the need for these types of cameras. If the need is present, then the number should be limited to that which is commensurate with the amount and type of manpower available for the task.

c) After-Action Assessment Cameras. This category is actually the easiest of the three, because it requires little or no attention from the operator. Cameras assigned to this category often have their output directed to a video storage unit. The challenge is to select video storage equipment capable of quickly retrieving useful information.

d) Task Management. Security Officers/Provost Marshals must evaluate other tasks assigned to the CCTV system operator, CCTV operation can be a task unto itself. There are few cases in the military police environment where personnel can be so dedicated to a single task. Therefore, other duties assigned to an MCESS Operator must also be considered. Monitoring an MCESS, MNS, answering telephone inquiries, and interaction between the MCESS Operator and other personnel in the area must be considered to effect a high performance CCTV System. Other influences, as identified below, on operator proficiency must also be considered.

1) The number of personnel within a control room

or station and the social interaction can distract or otherwise command the attention of an MCESS Operator. These influences can reduce the effectiveness of a surveillance system. Design and implement policies and procedures to increase proficiency, but human nature dictates these factors will exist and must be considered in the design phase.

2) Control room layout is just as important. Monitors and controls should be placed with respect to an operator such that it is not a burden or strain on the operator. Monitors should be sized to reduce eyestrain, and viewing angles should be within the natural limits of eye and neck movement. Controls should be intuitive to an operator and not require complicated actions to bring an image to his/her attention. Pan, tilt, zoom controls should also require no special dexterity for viewing areas of significance and incorporated into a single control unit. Control room lighting should be selected to reduce glare.

3) To be effective, operators must be familiar with the areas they are being asked to view. Initial and on-going training programs should be developed to ensure that ESS Operators are familiar with the system design, principle landmarks, and/or special circumstances (e.g., construction projects). ESS Operators should be aware of distances between the camera location and significant points within its field of view. ESS Operators lose depth perception when viewing camera scenes and can experience difficulty in relaying accurate information to other personnel dispatched to investigate.

▶ 6009. AUTOMATED ACCESS CONTROL SYSTEMS (AACS). The following policy applies to access control applications within the Marine Corps:

1. The DoD Common Access Card (CAC) will be the principle token for access to buildings, facilities, installations, and controlled spaces.

- a. All newly installed AACS will utilize the CAC.
- b. Existing systems, with the exception of those connected

to the MCESS will migrate to the CAC.

c. AACS connected to the MCESS will be brought into compliance immediately.

d. Those activities with an AACS, that will not be compliant with paragraph (a) through (c) above, should report non-compliance to CMC(PS).

e. Compliance with the requirement to use the CAC will not be waived.

2. The magstripe technology on the CAC will be utilized for all Marine Corps AACS, and all Marine Corps AACS may be upgraded as new technologies are available on the CAC.

3. With the exception of billeting, all other buildings, facilities, installations, and controlled space will adhere to the following:

a. The SEIWG 012 credential will be encoded on track two of the magstripe. Detailed information on the SEIWG 012 credential numbering scheme is available in Appendix G.

b. Encoding of the CAC magstripe will be performed by the local PMO for AACS connected to the MCESS.

c. Encoding of the CAC magstripe, for all other AACS, will be performed by person(s) responsible for access control to that building, facility, or controlled space.

d. The 4-digit system code element of the SEIWG 012 credential, which identifies which system the card is enrolled in, is controlled by the CMC(PS) MCESS TSA. AACS, other than those connected to the MCESS, can obtain a 4-digit system code by contacting HQMC, Security Division, Physical Security Chief at DSN 222-4495/4496.

4. Billeting AACS will adhere to the following:

a. Encode track three of the magstripe.

b. The credential encoded on track three will be a

numbering scheme unique to the type of AACS installed at that activities billeting.

5. Supplemental badging systems considered necessary for an additional level of security not presently afforded by the CAC (e.g., such as entrance into Sensitive Compartmented Information Facilities (SCIF) or other high security spaces) may be used; however, the following will apply for all supplemental badging systems.

a. Supplemental badging systems will not be used for granting access, but for the further identification (e.g., flash badge) of person(s) within the controlled space.

b. Persons not authorized the issuance of a CAC, who work in or requiring access to a controlled space, may be issued an activity specific badge. Such badges will be encoded with SEIWG 012, for allowing access through the AACS.

c. Visitors will be issued a visitors badge when entering a building, facility, installation, or controlled space with an AACS; however, they will not contain a magstripe that can be encoded.

► 6010. MASS NOTIFICATION SYSTEMS (MNS). Mass notification is the capability to provide real-time information to all building occupants or personnel in the immediate vicinity of a building during emergency situations. All Department of Defense (DOD) components are required to provide mass notification capability. This paragraph defines requirements for implementation of MNS aboard Marine Corps installations.

1. Beginning with the fiscal year 2004 construction program, mass notification is required in all new inhabited buildings, including new primary gathering buildings and new billeting. Mass notification is required in existing primary gathering buildings and existing billeting when implementing a project exceeding the replacement cost threshold specified in reference (q).

a. Mass notification is recommended in other existing

inhabited buildings when implementing a project exceeding the replacement cost threshold.

b. Mass notification is required for leased buildings, building additions, and expeditionary and temporary structures as identified in reference (q).

2. MNS falls under the MCESS Program, for which CMC(PS) is the program manager and oversees the funding, procurement, installation, and maintenance of the MCESS.

3. Installations/commands are not authorized to procure non-MCESS compatible MNS.

4. Individual building MNS aboard Marine Corps installations are not authorized. Marine Corps installations will have a base-wide control system for MNS. The focal point for the operation of the MNS will be the installation provost marshal. This requirement does not apply to MARFORRES.

5. In procuring MNS, installations, when using local funding, will have the MCESS TSA install said system, or they will use a contractor approved by MCESS TSA. To maintain system integrity, however, final installation to the PMO ACC will be accomplished/supervised by engineers and technicians from the MCESS TSA. Additionally, compatibility must be certified by the MCESS TSA prior to the procurement of any MNS. Compatibility review costs will be borne by the installation.

6. Installations, commands, or responsible agencies that elect to utilize the MCESS TSA to install a locally funded MNS, CMC(PS) will provide the sustainment maintenance and life cycle upgrade.

7. General.

a. An autonomous control unit will be used to monitor and control the notification appliance network and provide consoles for local operation. Using the console, MCESS Operators can initiate delivery of pre-recorded voice messages, provide live voice messages and instructions, and initiate visual strobes. MNS is capable of activating concurrent pre-recorded voice messages to multiple individual building systems,

including one message for the affected building and a separate message for nearby unaffected buildings. It is capable of delivering live and recorded voice messages originated at the central control unit. It is capable of patching through live voice to individual building systems, including those originated on radio by mobile security forces. A text message notification appliance may be used.

b. The base-wide control system should provide redundant (primary and backup) central control units. The Provost Marshal's ACC will be the primary focal point for the MNS console, with the secondary console located at the Emergency Operations Center (EOC).

c. A notification appliance network consists of a set of audio speakers located to provide intelligible instructions at all locations in and around the building. Strobes are also provided to alert hearing-impaired occupants.

d. The Giant Voice or big voice system will be used in outdoor areas, expeditionary structures, and temporary buildings. It is generally not suitable for mass notification to personnel in permanent structures because of the difficulty in achieving acceptable intelligibility of voice messages.

e. Telephone alerting systems are independent systems and provide delivery of recorded messages over the telephone network. These systems are useful for buildings in which notification to all building occupants may not be appropriate (e.g., child development centers, hospital patient areas, brigs). They also might be appropriate for small facilities and military family housing where mass notification is not required by reference (i). Use of telephone alerting systems, however, should be considered carefully before installing in most buildings and facilities requiring mass notification because there are many limitations in delivering notification messages by telephone. Additionally, use of the base's switched telephone network is the preferred communications method to minimize concerns about the system's reliability and vulnerability. There is no requirement for this application.

f. Performance parameters for the Marine Corps MNS will be determined by the MCESS TSA, and approved by CMC(PS).

6011. MARINE FORCES RESERVE. Because the facilities used by the reserve component are both unique and usually geographically separated from Marine Corps installations, the policies contained in this Manual cannot be strictly applied. Therefore, the Commander Marine Forces Reserve will incorporate the policies of this Manual where applicable. In all other cases, the spirit and intent of this Manual will be adhered to wherever possible. For Marine Corps Reserve Centers, where there is no government response force available, the system may be police connection or central station. Telephone answering services will not be utilized. All requirements for clarification will be addressed to CMC(PS).

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 7

CRITICAL ASSET PROTECTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
INTRODUCTION	7000	7-3
PRIORITIZATION OF ASSETS	7001	7-3
FLIGHT LINE SECURITY	7002	7-5
SECURITY OF PETROLEUM FACILITIES	7003	7-12
SECURITY OF COMMUNICATIONS FACILITIES	7004	7-14
WATERSIDE SECURITY	7005	7-15

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 7

CRITICAL ASSET PROTECTION

7000. INTRODUCTION. Critical assets are defined as facilities, services, resources, or equipment essential to the Marine Corps and DoD mission. Critical assets perform a vital function in operational plans or in support of operational plans. They include physical facilities or equipment, non-physical assets (such as software systems) or assets that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks). Disruption or loss render the asset(s) ineffective and may compromise mission capability.

1. Assets may be owned and operated by either a DoD or non-DoD entity, domestic or foreign. Identified assets must be identified and recognized at all levels; unit, organization, facility, or installation, and warrant protective measures to ensure they continue to function. Commanders must ensure assets are protected against disruption, degradation, or destruction, and plan for timely restoration of services.

2. Identified requirements are intended to mitigate vulnerabilities, however, these measures must be applied in conjunction with existing security (forces, barriers, ESS, etc.) to present and maintain a sound physical security posture.

7001. PRIORITIZATION OF ASSETS. Commanders must balance fiscal, manpower, and operational requirements in order to maintain a sound physical security posture.

1. To determine a course of action, resources and assets must be prioritized. Figure 7-1 is the DoD Resource and Asset Prioritization Chart with example assets, criticality definitions, and supporting security systems. The figure is provided to assist Commanders in asset prioritization. Appropriate security policies and procedures must be established and maintained. Standards must address physical security requirements including, but not limited to, access control, personnel and vehicle inspections, and increased security requirements in accordance with FPCONS and contingencies.

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
<p>A</p> <p>INTEGRATED ELECTRONIC SECURITY SYTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, ACCESS DELAY AND DENIAL SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED IMMEDIATE RESPONSE FORCES</p>	<p>THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE WILL RESULT IN GREAT HARM TO THE STRATEGIC CAPABILITY OF THE UNITED STATES</p>	<p>NUCLEAR AND CHEMICAL WEAPONS AND ALERT/MATED DELIVERY SYSTEMS</p> <p>CRITICAL COMMAND, CONTROL, COMMUNICATIONS FACILITIES AND SYSTEMS</p> <p>CRITICAL INTELLIGENCE GATHERING FACILITIES AND SYSTEMS</p> <p>PRESIDENTIAL TRANSPORT SYSTEMS</p> <p>NUCLEAR REACTORS AND CATEGORY I AND II SPECIAL NUCLEAR MATERIALS</p> <p>RESEARCH, DEVELOPMENT, AND TEST ASSETS</p>
SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
<p>B</p> <p>ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED RESPONSE FORCES</p>	<p>THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD BE EX PECTED TO GRAVELY HARM THE OPERATIONAL CAPABILITY OF THE UNITED STATES</p>	<p>ALERT SYSTEMS, FORCES, AND FACILITIES</p> <p>ESSENTIAL COMMAND, CONTROL, AND COMMUNICATIONS FACILITIES AND SYSTEMS</p> <p>CATEGORY I ARMS, AMMUNITIONS AND EXPLOSIVES</p> <p>RESEARCH, DEVELOPMENT, AND TESTS ASSETS</p>
SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
<p>C</p> <p>ELECTRONIC SECURITY SYTEMS, ENTRY AND CIRCULATION CONTROL, BARRIERS, SECURITY PATROLS, DESIGNATED RESPONSE FORCES</p>	<p>THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD IMPACT UPON THE TACTICIAL CAPABILITY OF THE UNITED STATES</p>	<p>NONALERT RESOURCES AND ASSETS</p> <p>PRECISION GUIDED MUNITIONS</p> <p>COMMAND, CONTROL AND COMMUNICATIONS FACILITIES AND SYSTEMS</p> <p>CATEGORY II ARMS, AMMUNITION, AND EXPLOSIVES</p> <p>(POL)/POWER/WATER/SUPPLY/STORAGE FACILITIES</p> <p>RESEARCH, DEVELOPMENT, AND TEST ASSETS</p>
SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
<p>D</p> <p>ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED RESPONSE FORCES</p>	<p>THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD BE EXPECTED TO GRAVELY HARM THE OPERATIONAL CAPABILITY OF THE UNITED STATES</p>	<p>ARMS, AMMUNITION AND EXPLOSIVES</p> <p>ECXHANGES AND COMMISSARIES, FUND ACTIVITIES</p> <p>CONTROLLED DRUGS AND PRECIOUS METALS</p> <p>TRAINING ASSETS</p> <p>RESEARCH, DEVELOPMENT AND TEST ASSETS</p>

Figure 7-1 DOD ASSET PRIORITIZATION CHART

Threat Type	Threat Description	Threat Example
Maximum	Individuals in organized and trained groups alone or with assistance from an insider; skilled, armed, and equipped with penetration aids	<i>Terrorists</i> and special-purpose forces; highly trained intelligence agents
Advanced	Skilled or semiskilled individual(s) working alone or in collusion with an insider, without penetration aids	Highly organized criminal elements; <i>terrorists</i> or paramilitary forces; foreign intelligence agents with access
Intermediate	Career criminals: individual(s) or insider(s) working alone or in small groups; some knowledge of or familiarity with the security system	Organized crime; white collar criminals; active demonstrators; covert intelligence collectors; <i>some terrorist groups</i>
Low	Individual(s) or insider(s) working alone or in a small group	Casual intruders; pilferers and thieves; overt intelligence collectors; passive demonstrators

Figure 7-2 Physical Security Threat Matrix

2. In order to establish security priorities, commanders need to be aware of threats to installation resources and critical assets. Figure 7-2 provides guidelines to commanders when determining the severity of threats to an installation and resources. Commanders must weigh all available intelligence to maintain installation specific threat awareness. There are a number of resources that the commander has at his/her disposal. Resources include the Provost Marshal, Naval Criminal Investigative Service (NCIS), Base Operations (G3) personnel, and Base Intelligence (G2) personnel. The provost marshal can obtain valuable local, state, and federal criminal activity intelligence via his/her contact with agency representatives.

7002. FLIGHT LINE SECURITY (FLS). The FLS program is designed to enhance security through a systematic employment of personnel and equipment. Security priorities are assigned based on the assets being protected. Commanders are responsible for security of Marine and transient aircraft. Prioritization requires a joint effort by the installation and the Marine Air Wing (MAW)

Commander. To ensure security concerns are addressed, installation commanders will assign the Provost Marshal as the primary coordinator for all FLS matters. MAW Commanders will assign a command security officer as the primary MAW coordinator for flight line security matters.

1. Aircraft security planning requires commanders to consider the degree to which the installation provides a secure environment. Factors included in the decision process include:

Whether the installation is open or closed.

If the installation has a defense in depth posture.

Personnel and vehicular access to the flight line.

Flight line adequately fenced, posted and lighted.

The use of ESS in conjunction with other physical security barriers, devices, and procedures.

Available manpower and equipment response capabilities.

2. FLS Responsibilities.

a. Installation Commanders will:

(1) Approve all plans for aircraft parking and flight line restricted areas.

(2) Designate restricted areas on or adjacent to the flight line in accordance with paragraph 3003.

(3) Notify the provost marshal of changes to aircraft parking areas so physical security requirements may be coordinated prior to modification.

(4) Provide equipment and facilities to support FLS operations.

(5) Approve Access Control Points for flight line restricted area(s).

(6) Procure, install, and maintain physical barriers, (fencing, lighting, etc.) to deter, delay, and deny entry of unauthorized persons to flight lines and related areas.

(7) Address FLS issues at meetings of the Physical Security Council.

(8) Incorporate FLS issues into the Installation Physical Security Plan.

(9) Notify CMC(PS) when planned flight line construction or upgrades require modifications to existing ESS.

b. MAW Commanders will:

(1) Provide the installation commander proposed plans for aircraft parking areas, restricted areas, and personnel and vehicle Access Control Points. Notify the installation commander when modification is required.

(2) Ensure FLS programs and command security programs support, and are integrated in, the installation Physical Security and AT/FP plan in.

(3) Provide initial and annual FLS training emphasizing aircraft and flight line area surveillance.

(4) Coordinate taxiway and runway policy use by security/safety personnel.

(5) Establish transient aircraft policy and procedure to include parking and security.

(6) Coordinate security support procedures with the installation commander and provost marshal concerning off-installation emergency or downed aircraft incidents.

c. Provost Marshals will:

(1) Ensure that FLS personnel are properly trained and equipped.

7002 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- (2) Supervise the FLS Program.
- (3) Maintain the FLS access database.
- (4) Issue FLS access badges.
- (5) Publish a FLS security operation SOP.
- (6) Assign patrol zones in and around flight lines.
- (7) Screen and train non-MP personnel assigned to augment the FLS program prior to assignment.
- (8) Coordinate security support procedures with installation and MAW Commanders concerning off-installation emergency or downed aircraft incidents.
- (9) Conduct annual physical security surveys of the flight line restricted areas.

3. Aircraft Parking Areas. Plans for establishing aircraft parking areas will include proximity to public areas, avenues of approach, and response routes for use by security force personnel.

a. Aircraft parking areas will be consolidated with, or located adjacent to, other support assets within the flight line restricted area.

b. Aircraft parking areas will be clearly marked.

4. Flight Line and Aircraft Surveillance. All unit personnel assigned to the flight line and adjacent areas will actively participate in flight line and aviation assets security.

a. Surveillance requirements include aircraft, hangars, parking aprons, and the flight line perimeter.

b. During normal working hours unit operations and maintenance personnel fulfill surveillance requirements.

c. After normal working hours, parking areas will be provided constant surveillance. Electronic surveillance equipment (CCTV used in conjunction with IDS) is encouraged, however, in the absence of electronic surveillance equipment, security personnel will be assigned.

d. CCTV surveillance equipment must be used in conjunction with an IDS which annunciates at a security force ACC, and include an event driven recording and assessment capability.

e. The use of electronic surveillance equipment is not designed to reduce manpower, but more so to enhance the security forces capability to perform its security mission.

f. Electronic surveillance equipment may be used to satisfy constant surveillance requirements for alert aircraft; however, personnel are required to conduct a security check of the aircraft every 4 hours.

5. Flight Line Restricted Access. Access control for the flight line is designed to prevent the unauthorized entry of personnel and vehicular traffic. Measures and procedures must be developed to provide appropriate access control during periods of increased threat.

a. Entry will be conducted only at designated Access Control Points (ACPs) (pedestrian or vehicle) manned by security force personnel, or those controlled by an Automated Access Control System (AACS).

b. Immediate access will be granted to all emergency vehicles responding to locations within the flight line (i.e. ambulances, fire trucks, military police vehicles, crash trucks, and explosive ordnance disposal vehicles). Such vehicles should not be impeded, and security personnel will render assistance as directed.

c. Government vehicles authorized on the flight line will be clearly marked. The manner of marking will be coordinated with security personnel.

d. After normal working hours, security personnel will be notified for vehicle access to the flight line, and movement within the flight line.

e. Commands will appoint an access control officer, in writing, who will provide the provost marshal with a flight line access roster. The roster will identify individuals authorized access to the flight line.

f. Lost or recovered access control badges will be reported immediately to PMO, and immediate steps will be taken to prevent access via the lost badge.

g. Privately owned vehicles are prohibited from entering all flight lines.

5. Flight Line Security Force. Flight lines present a unique security challenge, and the use of both mobile and foot patrols is highly encouraged. Security force personnel, including augmentees, will be trained and equipped as directed in Chapter 4.

6. Off-Installation Security Requirements. MAW Commanders will coordinate and provide security when and where Marine Corps Air assets are staged and/or stored at an off-installation location. Security will be coordinated with host-installation or host-nation security forces as applicable and will be addressed prior to any air asset deployed. Security will be provided commensurate with guidance contained in this Manual.

7. Emergency Situations. A National Defense Area (NDA) will be established in any emergency involving an asset that has crashed or is forced to land outside of the legal jurisdiction of the Marine Corps/DoD. A NDA is defined as an area established on non-federal lands located within the United States and its possessions or territories, and is established for the purpose of safeguarding classified defense information or protecting government equipment and/or material. The establishment of a NDA temporarily places such non-federal lands under the effective control of the Department of Defense and results only from an emergency event. The nearest military installation will

assume immediate responsibility for establishing the NDA upon notification of a forced landing or crash. The owning service or government agency will be notified without delay and will assume on-site security and responsibility upon arrival. Security personnel will coordinate overall site security with local law enforcement. Security personnel must ensure that the following measures are applied:

- a. Ensure the safety of civilian bystanders.
- b. Protect classified cargo and aircraft components.
- c. Prevent tampering with, or pilfering from, the aircraft.
- d. Preserve the accident scene for later investigation.

8. Transient Aircraft. Marine Corps Air Station (MCAS) and Marine Corps Air Facility (MCAF) Commanders will ensure that a secure area is provided for transient aircraft parking and or staging.

- a. Administrative aircraft security may be met by parking the aircraft in an area where normal personnel movement provides a high degree of surveillance and deterrence.

- b. Alert and critical transient aircraft require additional security measures. MCAS and MCAF Commanders will make every effort to provide the same degree of security that the owning Service would provide.

- (1) Aircraft will be parked in an established restricted area on the flight line with an ESS when possible.

- (2) If ESS is not available, the aircraft will be placed in a hangar.

- (3) In the absence of a permanent restricted area or hangar, the aircraft will be enclosed with barriers. All tactical and critical transient aircraft parking/staging areas will be clearly identified and posted as a restricted area. Lighting will be provided to support security personnel. Access to the area and aircraft will be limited to those personnel authorized by the aircraft commander. Transient aircraft commanders are required to identify any significant security requirements or priorities to the host installation.

7003 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

7003. SECURITY OF PETROLEUM ASSETS.

1. Bulk Fuel Storage Areas. Bulk Fuel Storage Areas are those areas that store 1000 or greater gallons of fuel. Access control will be established, in writing, for those personnel whose primary duties require access to bulk fuel storage areas.

a. Bulk fuel storage areas will be fenced in accordance with paragraph 5006. Vehicle and personnel gates will be kept to a minimum as required by operational requirements. Gates will remain closed and locked when not in use. Use of automated access control systems is encouraged. Main entry points and fence lines will be posted in accordance with paragraph 3004. Privately owned vehicles are prohibited from entering bulk fuel storage areas.

b. Facilities will be provided security lighting during the hours of darkness.

c. Key control will be established for the facility as indicated in paragraph 3005 of this Manual.

d. Pump houses, pumps, and power/relay switches, boxes, etc., will be locked and electrical power secured after normal business hours. Off-installation, remote, and stand-alone pump houses will be hardened against criminal or terrorist activity. Hardening includes rod and bar grills constructed over the windows, solid metal doors, and reinforced concrete walls.

e. Pipelines outside of the protected perimeter should be buried to lessen vulnerabilities when possible. For those sites where burial of pipelines is not practical, Commands will institute a vigorous inspection program. Commanders are encouraged to establish liaison with local, State, and Federal, and host nation officials for support.

2. Petroleum, Oil, Lubricant (POL) Facilities. POL facilities are defined as issue points and storage areas maintaining unit level issue stocks. These facilities may include tactical and garrison Motor Pools where large amounts of POL stocks are maintained.

a. Depot level POL issue points and storage areas will be fenced in accordance with paragraph 5006. Access control will be established. Vehicle and personnel gates will be kept to a minimum as dictated by operational requirements. Gates will remain closed and locked when not in use. Use of automated access control systems is encouraged. Main entry points and fence lines will be posted in accordance with paragraph 3004. Privately-owned vehicles are prohibited from entering Motor Pools.

b. Facilities will be provided security lighting during the hours of darkness. Individual pump islands will be provided lighting. Storage areas and power administration areas will be provided security lighting over entry points.

c. Key control will be established as indicated in paragraph 5006 of this Manual.

d. When not under the surveillance of personnel authorized to dispense the products, POL pumps and power/relay switches, boxes, etc., will be locked and electrical power secured. These measures are not required if pumps are activated by a credit card type device.

e. Packaged POL will be stored in structures under secure storage. Large POL packages, such as 55-gallon drums will be stored to preclude their use as hiding places for pilfered items.

f. POL tank trucks that contain fuel will be parked inside of a controlled area (flight line, motor pool) after normal working hours.

7004. Security of Communication Facilities. Communication systems play a major role in the Marine Corps' mission by providing essential communications in garrison and the operational environment. Marine Corps policy requires protection for communications facilities and systems to ensure continuity of operations of critical users, facilities, and systems that they support, to include mobile facilities.

7004 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

Communications facilities will be designated, and posted, as restricted areas in accordance with paragraph 3004. Based on location, layout, and equipment, security requirements must be thoroughly assessed for each particular communications system. Physical security will be tailored to that particular facility or system.

a. Remote, stand-alone, and off-installation facilities should be hardened against criminal or terrorist activity. Hardening includes rod and bar grills constructed over the windows, solid metal doors, and reinforced concrete walls.

b. Fencing of facilities is recommended, however, all off-installation communications sites will be fenced in accordance with paragraph 5006. Vehicle and personnel gates will be kept to a minimum as required by operational requirements. Gates will remain closed and locked when not in use. Use of automated access control systems is encouraged. Main entry points and fence lines will be posted in accordance with paragraph 3004. Privately owned vehicles are prohibited from entering communications facilities/sites.

c. Facilities will be provided security lighting during the hours of darkness.

d. Key control will be established as indicated in paragraph 3005 of this Manual.

7005. WATERSIDE SECURITY. Waterside security presents a unique and challenging task to installation commanders. Waterside security requirements must be addressed in the installation physical security plan. There are mechanisms available to assist commanders in establishing control of installation waterside/waterfront perimeters, thereby limiting personnel, vehicle, and vessel access to areas under their control.

1. Establishing Limited Waterways. The U.S. Coast Guard (USCG) and the U.S. Army Corps of Engineers (USACE) are the implementing authority(s) for establishing control, access to, and movement within certain areas of their jurisdiction, as it

pertains to waterways and waterfront property. This authority is granted under the Ports and Waterway Safety Act (PWSA) of 1972 (33 USC 1221 et seq.); Magnuson Act of 1950 (50 USC 191); the Outer Continental Shelf Lands Act (OCSLA) (43 SUC 1331 et esq.); and the Deepwater Port Act (33 USC 1501 et seq.), waterfront property. Access control and movement within certain areas may be restricted in the interest of safety, security, or when other national interests dictate. Figure 7-3 provides information for each type of Limited Waterway Area.

a. The USACE local field office is the responsible agency for establishing restricted areas. The Coast Guard Captain of the Port is responsible for establishing all other types of Limited Waterway Areas. Requests for controls and/or designation of a limited waterway require that Commanders provide a written application with supporting documents to the responsible agency. Supporting documents include complete justification regarding the type of designation requested and a detail map of the affected area(s). The establishment of any Limited Waterway requires public notification and hearings in order to identify any affects or concerns with regards to the local populace.

b. Commanders must coordinate designation and protection of the waterways with the respective agency. Operations and/or security plans will fully identify areas of responsibility and jurisdiction. Liaison between security personnel and the respective agency must be continuous in order to ensure that the conditions for the designation, and all procedural requirements remain valid and current.

c. Figure 7-3 provides waterside/waterway security zones and areas and cognizant agencies that assist in their establishment.

2. Waterside Assets and Potential Threats, Targets, and Consequences. The following assets are common at installations with waterside/waterfront property(s):

a. Passenger and cargo vessels

AREA	AGENCY	AUTHORITY	LIMITATIONS	PENALTIES	ENFORCEMENT	COMMENTS
RESTRICTED AREA (1)	USACE (2)	33 CFR 207	Only on inland waterways	Misdemeanor	Enforcement may be delegated to the command	No threat needed. Easy to obtain. Provides limited area jurisdiction for command.
SAFETY ZONE (1)	USCG/ COTP (3)	33 CFR 165	Temporary, but may be long term	Misdemeanor Can result in civil or criminal penalties under 33 USC 1232.	USCG only. Marine Corps may patrol. COTP authority.	No Threat needed. Can be placed around moving vessel.
SECURITY ZONE (1)	USCG/ COTP	MAGNUSON ACT (50 USC 191) 33 CFR 6.10-5 33 CFR 165	Only within territorial limits of U.S. No person or vessel may enter zone without permission from COTP. Can be placed over land.	Felony -10 years/ 10,000	USCG Only. Marine Corps may patrol under COTP authority.	Threat required. COTP controls access and movement of all vessels, persons & vehicles (including their removal), and may take possession and control of any vessel. (see 33 CFR 165.33)
RESTRICTED WATERFRONT AREAS (1)	USCG/ COMDT (4)	MAGNUSON ACT (50 USC 191) 33 CFR 165.40	Must be issued and directed by Commandant of the Coast Guard. COTP may be directed to enforce. Must be in regulation. Limits access of persons.	Felony -10 years/ 10,000	USCG only. COTP directed by COMDT	Threat required. Long term limited access area Any change must be directed by the COMDT.

- (1) Does not include airspace. (2) USACE - U.S. Army Corps of Engineers
 (3) USCG - U.S. Coast Guard (4) COTP - Captain of the Port
 (5) COMDT - Commandant of the Coast Guard

Figure 7-3 LIMITED WATERWAY AREAS

- b. Pleasure Craft and Pleasure Craft Piers
- c. Pier/port complex
- d. Military Support Vessels
- e. Waterfront Facilities
- f. Warships
- g. Passenger Ships and terminals
- h. Navigational Aids
- i. VIPs (aboard ship or at waterfront facilities)
- j. Military Piers
- k. Shore facilities connectors; causeways, tunnels, cables utility towers, and bridges and facilities where unauthorized access may be gained or an approach made from the waterside

3. Waterborne Threats. Commanders must consider a number of waterborne threats such as mines, swimmers, small boats with armed personnel, and small boats laden with explosives. Targets include ships, shore facilities, wharfs, and piers.

4. Physical Security Measures. Commanders need to address facility and asset security by erecting perimeters and properly outfitting them to identify attempted or successful penetrations. This includes the full complement of physical security measures, including instructions, barriers, security systems, and response capabilities to combat waterborne threat(s) and present a sound waterside physical security posture.

a. Enforcement Zones. Zones must be established to enforce waterside security and serve as an action position for security forces. Figure 7-4 provides an example of waterside enforcement zones.

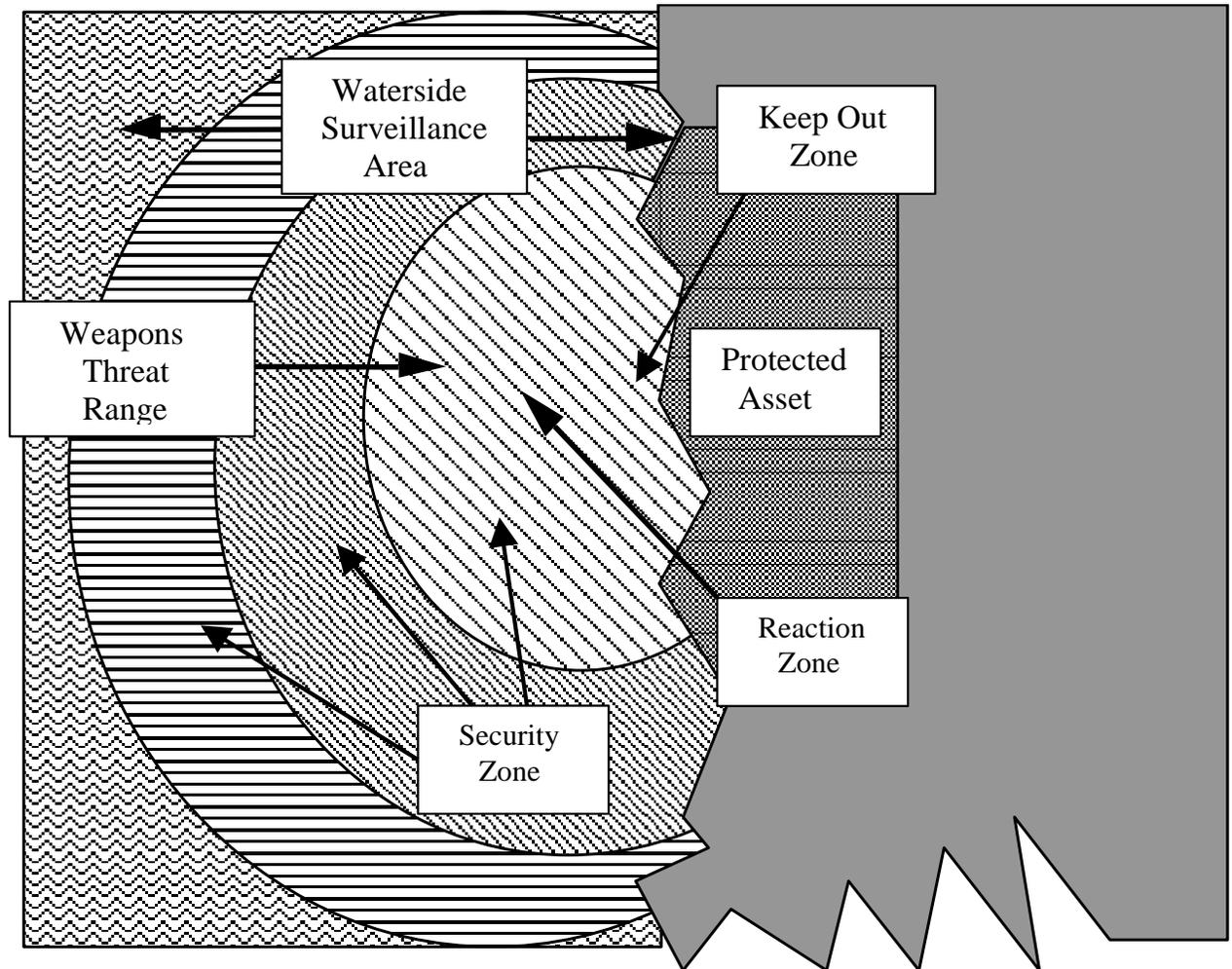


Figure 7-4 Waterside Security Zones

(1) A security zone is the area from the average high water mark to a point at the range of anticipated waterborne threats. Security forces notify vessels, crafts, and swimmers that they are entering restricted waters and must alter their course. Security forces may stop and search vessels if necessary, although as a general rule, engagements are not a high priority. Security zones usually extend to the furthest point allowed by USACE and USCG requirements.

(2) A reaction zone is the area from the high water mark to a distance beyond the maximum range of anticipated waterborne threats. Security forces stop and challenge intruders, taking action to stop potential threats.

(3) A keep out zone is the area closest to protected assets and is located from the asset to the maximum range of anticipated threat weapons (hundreds of yards for small arms and rocket propelled grenades to several thousand yards for man-portable anti-tank weapons). Security forces must prevent entry of hostile craft or vessels into this zone; local defenses may be engaged if hostile craft or vessels enter this zone.

b. Boundary Markers. Several devices can be used to establish boundaries separating the installation or asset from surrounding or bordering waters. Boundaries can provide areas of operation for waterborne security patrols, Special Reaction Team patrols, and Contact and Escort services. Among the devices that can be used to establish and mark boundaries are:

- (1) Buoys or floats
- (2) Nets
- (3) Anchored or pile mounted channel markers
- (4) Signaling devices
- (5) Log Booms
- (6) Barges
- (7) Workboats, whalers, and other small boats at anchor

c. Barriers. Waterside barriers at an installation, facility, or asset afloat perform functions that barriers on land perform; establishing boundaries, isolating activity, discouraging visitors, and impeding passage by boat or swimmer. They can be installed at land/water interfaces or at average high-water marks. Rules of navigation allow for inadvertent and

innocent penetration of certain types of barriers, as may occur with small craft engine failure, sail boats, and pleasure craft operators who lack navigational and operational skill.

(1) Barriers can be used to restrict waterside access to the installation. Use of floating nets, especially those made of wire mesh and anchored to the floor of the body of water, can deny access to swimmer delivery vehicles, small commercial-type submarines, or divers. Barges create a physical barrier of considerable penetration resistance to small craft. Barges should be secured bow to stern with the lead and aft barges being secured to the pier or shore side mooring point. The primary purpose for deploying a barrier of this type is to absorb a large portion of the blast from an explosive laden vessel that managed to elude initial defenses.

(2) Several barriers can be used to slow or impede access to facilities by boats or swimmers. Nets are among the best for this purpose. Well-marked partially submerged objects can also be used; there are legal implications regarding the emplacement of barriers that constitute a hazard to navigation; such devices should be emplaced only after exhaustive consultations with appropriate legal authorities.

d. Patrol Boats. Patrol boats are the most effective means of isolating an activity and discouraging vessels from approaching identified boundaries. Patrol boats require establishment of a perimeter, surveillance beyond the perimeter to identify potential intrusions, and dispatch of Contact and Escort (C&E) boats to intercept intruders within the security zone. Vessels should not be allowed within the reaction zone of the protected asset.

5. Security and Response Forces. Waterborne security and response forces are employed to maintain perimeter security and enforce security zone restrictions. Depending on the installation, the nature of facilities and activities, and jurisdiction under which waterside security is conducted, security forces may be provided by the Marine security forces, U.S. Coast Guard, state or local police, or host-government forces.

a. While patrolling the land-water interface, security forces must be equipped with vehicles, communications equipment, and personal protection equipment. It is essential that waterside and landside security force command, control, and communications systems be integrated.

b. Patrol forces are deployed to patrol the security zone, provide detection and identification information to a central command post, and to aid other security forces as necessary.

c. Contact and Escort (C&E) forces are deployed in the outer security zone. C&E forces are responsible for positioning the C&E boats between intruders and protected assets, making initial contact with intruders, and providing navigational assistance and escort services to ensure intruders exit restricted waters.

d. Tactical Response Boat (TRB) forces are deployed close to or within the reaction zone and are responsible for engaging intruders and terminating incidents outside of the "keep out" zone.

e. If boarding becomes necessary it should be conducted by contact/escort vessel personnel, local or state law enforcement officers, or designated boarding teams transported to the scene by a standby vessel. In all cases boarding should take place outside the security zone at a secure location.

6. Patrol Techniques. Random patrolling is an effective tool in installation waterside security. Water approaches to the asset need to be divided into sectors with sector boundaries that converge at the asset.

a. **One-Boat Security Zone.** In one-boat security zone enforcement, the security boat maintains a position near the zone centerline at the outer boundary. The position allows maximum visibility for observing the security zone and for warning vessel traffic. All turns should be made to the outside so the crew can maintain surveillance of zone boundaries.

b. Two-Boat Security Zone. In two-boat security zone enforcement, the zone is divided with each security boat maintaining a position near the centerline of their assigned half. If either boat leaves their position, the second boat moves to the centerline of the entire zone.

c. Moving Security Zone. In a moving security zone (primarily used when the asset is underway), a two-boat minimum is recommended. Additional security vessels may be used if the threat indicates a need.

7. Defensive Boat Tactics. Defensive measures provide a response option for intercepting and neutralizing an identified, incoming hostile threat. The protected asset can be a ship, pier, waterfront facility, or any area or object vital to national security that requires protection from a waterborne threat.

a. In a CONUS environment, operations must continually maintain a law enforcement posture that recognizes the constitutional rights and privileges of citizens to use the waterways.

b. In a hostile environment without a declared war, extraordinary measures are required, to separate friend (or neutral) from foe.

c. The first level of response with this tactical doctrine is to notify transiting vessels of the security zone and to determine their intentions. Non-aggressors will simply be escorted out of the area. The utilization of these tactics will provide a system for effectively responding to a wide range of threats.

9. Surveillance/Intrusion Detection Systems. There are a variety of surveillance systems for use in connection with waterside security. There is a substantial difference in daylight and night surveillance of waterside activities. During hours of darkness, a reduction in surface activity occurs. As a result, nighttime surveillance of waterside activity can rely on active measures such as radar with comparatively good

success in locating, and partially identifying potential problems.

a. Once a potential intruder has been detected, it must be classified and identified in order to ensure that proper security measures are employed. In some instances, detected intruders can be identified as either swimmers or vessels; such identification is not sufficient enough information upon which to base a response.

b. Electronic security detection devices cannot be easily installed on most boundary barriers when the boundaries extend several hundred meters or more into the water. Some electronic security detection devices can be mounted on fixed structures that extend into the water such as wharfs, piers, or navigation aid platforms.

10. Pier, Hull, and In-Water Structure Inspections. Prior to a ship's arrival, if current threat information dictates, divers should inspect pier areas for any pre-positioned explosive devices. Explosive Ordnance Disposal (EOD) Units, if available, may be used for this mission. While a ship is in port, landside personnel and Coast Guard waterside patrols should inspect the pier area and ship's hull randomly. Other at risk structures such as navigation aids, bridges, utility cable towers, tunnels, etc. should also be inspected on a periodic basis. Frequency of inspections should be increased on the basis of increased FPCONS.

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 8

SECURITY OF ARMS, AMMUNITION, & EXPLOSIVES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	8000	8-3
PRIORITY.	8001	8-6
PERSONNEL	8002	8-6
ACCOUTABILITY AND INVENTORY	8003	8-11
AA&E STORAGE FACILITIES	8004	8-12
SECURITY OF ARMS	8005	8-15
SECURITY OF AMMUNITION & EXPLOSIVES	8006	8-24
FENCES	8007	8-29
AREA DESIGNATION AND ACCESS CONTROL	8008	8-29
ELECTRONIC SECURITY SYSTEM.	8009	8-30
KEY SECURITY AND LOCK CONTROL	8010	8-31
SURVEILLANCE AND SECURITY CHECKS.	8011	8-33
SECURITY LIGHTING	8012	8-36
COMMUNICATIONS.	8013	8-37
PHYSICAL SECURITY SURVEYS	8014	8-37
PHYSICAL SECURITY PLAN.	8015	8-38
READY FOR ISSUE (RFI) AA&E STORAGE AREAS.	8016	8-38
DISPOSAL AND DEMILITARIZATION	8017	8-38

Coordinating Draft for Review 10 June 2004

ROTC/GUN CLUB/RESERVE UNIT PROHIBITIONS	8018	8-39
CLASSIFIED AA&E	8019	8-39
NAVY AND MARINE CORPS RESALE FACILITIES AND EXCHANGES.	8020	8-39
NAVY AND MARINE CORPS MUSEUMS AND UNIT DISPLAYS	8021	8-40
ORGANIC/UNIT AND STATION MOVEMENTS.	8022	8-41
SECURITY STANDARDS FOR SECURE HOLDING AREAS FOR AA&E ON AN INSTALLATION OR CONTRACTOR FACILITY	8023	8-46
SPECIAL CONSIDERATIONS FOR SMALL QUANTITY SHIPMENTS.	8024	8-49
REPORTING OF MISSING, LOST, STOLEN, AND RECOVERED (MLSR) AA&E	8025	8-49
SIMULATED WEAPONS SYSTEMS	8026	8-50

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 8

SECURITY OF ARMS, AMMUNITION, AND EXPLOSIVES

8000. GENERAL. This chapter prescribes standards, which will provide adequate protection against loss or theft of arms, ammunition, and explosives (AA&E) as defined in Appendix H, at Marine Corps activities and contractor facilities. It does not authorize methods, actions, or operations inconsistent with the explosive safety standards of references (r) through (t).

1. The criteria in this chapter is intended for sites where AA&E are maintained on a permanent basis during daily peacetime conditions, contingency sites, exercises, and not operational readiness inspections. For sites not specifically covered in this instruction and operational environments, commands will establish procedures to protect AA&E consistent with the intent of this chapter.

2. The security standards provided within this chapter apply to all Marine Corps AA&E in the custody of Marine Corps and Navy activities, or contractors. Furthermore, other DoD Component AA&E in the operational or administrative custody of Marine Corps activities will adhere to the security requirements as prescribed herein. When Marine Corps AA&E is maintained on naval vessels, units are directed to adhere to standards outlined in references (u) and (v).

a. This chapter covers:

(1) Arms: In addition to Appendix H, comparable foreign arms, U.S. prototyped arms, and illegally manufactured weapons in the DON inventory are also included.

(2) Ammunition: In addition to Appendix H, see stock list of Navy ammunition ~~TW010 AA ORD 010~~ NAVSUP Pub-802 (formerly OD 12067) NAVAIR 11-1-116A.

(3) Explosives: In addition to the categorized explosives in Appendix H, also uncategorized class 1.1, 1.2 (1.2.1, 1.2.2, 1.2.3), 1.3, 1.4, 1.5, 1.6, and explosives when being transported.

b. This instruction does not cover:

(1) nuclear weapons;

(2) devices charged with chemical agents (unless specified in appendix A);

(3) blank, .22 caliber, and inert ammunition;

(4) artillery, tank, mortar shells 90mm and larger and naval gun ammunition 3 inches, 76mm and larger; and

(5) non-lethal ammunition.

(6) Security criteria in this instruction do not apply to commercially available Risk Category III and IV AA&E while at a commercial production facility. However, once such items are placed in transit to a DoD activity, all pertinent requirements of chapter apply.

4. A list of AA&E Security Risk Categories is provided in Appendix H.

► 5. **Commanders and** individuals issued or in possession of AA&E are responsible for its security.

6. Installation physical security plans will address the protection of AA&E. The host installation/activity will assume responsibility for coordinating tenant AA&E protective measures.

a. Plan for effective use of security, tailored to local needs. Consider: NCIS local threat assessment, categories and types of AA&E maintained; location, size, and vulnerability of storage facilities, including theft by employees; and responsiveness of the security force. Also consider security aids such as perimeter barriers, security lighting, communications, key and lock controls, access control, structurally secure storage buildings, personnel and vehicular entry control, administrative inspections at entry/exit points, security training programs, Electronic Security Systems (ESS), and Closed Circuit Television (CCTV).

b. Prepare contingency plans for increased security measures for AA&E storage areas during periods of special vulnerability such as natural disasters, emergencies, or increased terrorist or criminal threat.

c. Barriers and locks are merely delay devices; they must be supported by means to detect and quickly react to an attempted intrusion. The security force must be alerted to attempted intrusions as early as possible and be capable of responding before access to AA&E can be gained.

▶ **d. Establish and publish the physical security plan.**

7. Deficiencies of, or non-compliance with, standards of this manual, and this chapter, require immediate command attention. Once it has been identified a standard cannot be met and adequate compensatory measures cannot be emplaced, or the command cannot fiscally support corrective action, the affected organization is required to request a waiver or exception as outlined in paragraph 1014 of this Manual.

▶ 8. PS maintains cognizance over AA&E security policy, while D/CMC Installations and Logistics (I&L(Code LPC-3)) is responsible for Ammunition and Explosives (A&E) transportation policy. Marine Corps Systems Command (MARCORSYSCOM) Program Manager Ammunition (PM AMMO) maintains cognizance of inventory, **Explosives Safety**, tracking, storage, issue, distribution rework, and disposal requirements for all ground ammunitions and explosives. Cognizance of aviation ordnance policy falls under the purview of D/CMC Aviation (AVN ASL-30).

9. Commanding Officers will ensure there is a strong, viable, and visible command emphasis with regards to the security of AA&E. The command AA&E security posture will be continuously assessed and all possible resources will be provided to execute the security program and maintain a sound, aggressive physical security posture.

10. Security of AA&E is paramount, and in those instances and situations not specifically addressed in this manual, units will protect all AA&E consistent with the intent of this chapter.

8001 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- ▶ 11. AA&E will be consolidated in as compact an area as possible consistent **with explosives safety and compatibility to** minimize the cost of physical security and inventory control and to reduce theft vulnerability. Further, A&E will be segregated and stored by risk category and provided the required level of security defined in this manual. Arms will be stored and provided the level of security defined by this manual required for the highest risk category stored in the facility.

- ▶ 12. Under the requirements of applicable laws and regulations, appropriate action will be taken against persons responsible for violating procedures and requirements imposed under this instruction. Action may include court-martial **or civil action for civilian personnel.**

- 13. Security requirements for AA&E produced and/or stored at contractor owned facilities are provided in reference (f).

8001. PRIORITY. Marine Corps priority for meeting security requirements will begin with the highest Risk Category I items and progress consecutively down through Risk Category IV. Within each category, facilities having the largest quantity will receive initial attention.

1. Based on threat and vulnerability, Marine Corps sites outside the continental U.S. (OCONUS) will receive priority over CONUS sites.

2. Deviations from these priorities will be permitted only when CMC(PS) has determined that an identified local threat dictates the deviations.

8002. PERSONNEL. Activities must be selective in assigning personnel to duties involving control of AA&E. Only personnel who are mature, stable, and have shown a capability to perform assigned tasks in a dependable manner will be assigned to duties involving AA&E.

1. Screening.

a. Personnel assigned custody, maintenance, disposal, or security responsibilities for AA&E on military installations will be subject to one of the following investigations as set forth in reference (w).

(1) Military Personnel: National Agency Check, Local Agency Check, Credit Check (NACLIC).

(2) DoD Civilian Personnel: National Agency Check with Written Inquiries and Credit (NACIC).

(3) Contractor Personnel: NACLIC.

b. All personnel who account for, maintain, dispose of, distribute, and provide security for AA&E in the performance of their duties will be screened using the AA&E Screening Package, see Appendix I. The Qualification and Certification (QUAL-CERT) Program is a further requirement of the A&E Program, but does not replace the annual AA&E screening requirement.

► (1) The Commanding Officer is responsible **for ensuring that the** initial and annual screenings **are completed.** The Commanding Officer may assign the Security Officer, AA&E Officer, or other designated Officer. The assignees will examine the service records of those being screened and discuss the duties to be assigned with the person. Those persons assigned as a screening officer will be assigned in writing, **and may be either a commissioned officer, warrant officer, staff non-commissioned officer, or civilian equivalent.**

(2) At each screening read the following statement to the person being screened and have him/her sign a copy of this statement:

"I understand that my behavior on duty as well as off duty is expected to reflect mature, stable judgment and that I may be removed from my duties involving control of arms, ammunition and explosives, or other administrative action taken, if my behavior does not reflect high standards. I further understand

that serious harm can come from my failure to properly carry out my duties. I am aware that my improper actions or failure to carry out my duties may result in criminal prosecution, fines, and imprisonment. I understand and accept the responsibility to safeguard arms, ammunition and/or explosives."

▶ (3) Screening will be conducted on an annual basis, and will be documented in **either** the Service Record Book (SRB) or Officer Qualification Record (OQR), **or an Unit Diary Entry (TTC 489) will be made. Additionally, the Basic Individual Record (BIR) will reflect that the individual has been screened for AA&E duties.** The statement and date(s) of screenings for civilian personnel **and local nationals** will be entered into the **appropriate** ~~civilian~~ personnel record. Annual screening for personnel who are part of the Qualification/Certification Program, screening will be documented in the individuals Qualification/Certification record.

(a) Maintain for at least 6 months after termination of the person's assignment (or 6 months after the final interview if the person is disqualified).

(b) Rescreen personnel annually or when circumstances indicate a review would be prudent.

▶ (4) Determination of which traits and actions are disqualifying is at the discretion of the commanding officer. **Additional criteria for making these determinations can be obtained from CMC(PS).**

▶ (5) Personnel that do not meet screening requirements will not be assigned responsibilities that require accounting for, maintaining, or distributing AA&E. For those Marines **possessing the requisite MOS**, who do not meet requirements, or have been disqualified, Commanding Officers must notify CMC (MMOA/MMEA) to request reassignment. Civilian personnel that do not meet the screening requirements notify Commanding Officers or supervisors for appropriate action.

c. Personnel operating a vehicle or providing security to a vehicle transporting Category I and II AA&E (including

contractor personnel transporting such items on Marine Corps installations in direct support of installation requirements) will be subject to an investigation as provided in paragraph 8002(1)a, above.

d. Designated commercial carrier employees providing Protective Security Service for the transportation of AA&E classified SECRET must possess a Government-issued SECRET clearance, as provided for in reference (x), and carrier-issued identification.

▶ 2. AA&E Responsible Officer. Commanding Officers will designate in writing, an individual, military or civilian, as the AA&E Officer, **synonymous with AA&E Responsible Officer throughout this manual**. The AA&E Responsible Officer designation letter will be maintained for 3 years. The AA&E Responsible Officer is responsible for all AA&E accountability and security matters and will ensure command-wide compliance with this chapter. He or she may serve as the weapons officer and/or audit and verification officer, and will maintain close liaison with the security and inventory accuracy officers. Additionally:

a. Assist the investigating agency in any AA&E losses.

b. Provide monthly AA&E status reports to the commanding officer to include but not limited to:

(1) Command compliance with accountability controls

▶ (2) Command **T/E allowance or inventory versus AA&E allowance**

(3) A&E requisition status

▶ (4) Maintain all AA&E reports for 3 years (**e.g. monthly inventories, MLSR Reports, etc.**)

c. Monitor performance and reporting of all AA&E inventories, as well as related Missing, Lost, Stolen, or Recovered (MLSR) reports.

▶ d. All A&E expenditure reports, to include signatures on all documents.

3. Training. Activities possessing AA&E will establish an annual training program for personnel with AA&E-related duties (including personnel responsible for issuing, receiving, security, handling, and accountability of AA&E items). The AA&E Training Program will include training in; inventory and accountability procedures including instructions for completing required documentation, explosives safety, reporting requirements, physical security requirements, off-station/on-station movement procedures, AA&E shipment accountability procedures, emphasis on individual responsibility for the control and safeguarding of AA&E, **unit-wide annual AA&E awareness**, and instruction on use of deadly force, per reference (n), as applicable. Activities will conduct annual training to ensure that all personnel remain vigilant of their responsibilities for controlling and safeguarding AA&E.

a. Training will be documented and maintained in command training records.

b. Personnel whose AA&E duties require the carrying of a weapon will participate in qualification and deadly force training of references (n) and (o), with the exception of periodic deadly force refresher training. Deadly force refresher training will be conducted on a semi-annual basis, and will be documented and maintained in command training records.

4. Arming of Security Personnel. Armory and Ammunition Supply Points (ASP) personnel will be armed upon the deactivation of the MCESS/IDS as required by reference (n).

5. Security Forces. In the addition to those security force requirements listed in chapter 4, the following apply.

▶ a. An armed response force must be capable of responding within **10** ~~15~~ minutes of all alarms or reports of attempted or actual intrusion in AA&E storage areas. Response forces are responsible for prioritizing response to facilities based on the criticality of AA&E stored within.

b. Entry and exit points into magazines and holding areas will be controlled by armed guard. When guards or working party personnel are not present or ESS is not provided, surveillance and physical checks requirements identified in paragraph 8010, will be adhered to. CCTV is not a substitute for guards or constant surveillance.

► c. An armed security patrol (**PMO**) will periodically check facilities and areas storing AA&E, as prescribed in paragraph 8011. Checks will be increased based on Force Protection Conditions (FPCONS) or vulnerability. Increased patrols and checks at night, on weekends and holidays are recommended to provide deterrence and early detection of loss. Random checks with irregular timing avoid establishing a predictable pattern.

(1) Checks will include physical checks of all doors and locks, and windows.

(2) Checks will be recorded and all records will be maintained for 3 years.

d. Supervisory personnel will inspect all security posts, spaces, and patrols periodically.

► 8003. ACCOUNTABILITY AND INVENTORY. Commanding Officers will assign, in writing, a commissioned officer, warrant officer, staff-noncommissioned officer, or civilian equivalent as an AA&E ~~Accountability~~ **Audit and Verification** Officer. The AA&E **Audit and Verification** ~~Accountability~~ Officer is responsible to the Commanding Officer for all AA&E accountability and inventory matters as prescribed in this chapter. AA&E **Audit and Verification** ~~Accountability~~ Officers will verify the validity of all actions concerning AA&E to include rejecting excess and unauthorized requisitions. All activities will maintain complete records identifying shipment, receipt, storage, use, and demilitarization/destruction in accordance with references (y) through (aa) and (t). Further guidance on the demilitarization of AA&E can be found in paragraph 8017.

1. Marine activities will ensure that all Marine Corps AA&E stored at non-Marine facilities, whether by another branch of

Service, foreign nation, NATO, or other, are inventoried to a level equivalent to that required herein.

2. The nature and sensitivity of arms control dictates strict adherence to the provisions of other specialized orders with respect to research of potential inventory adjustments, reversal of inventory adjustments, retention of accountable documentation, quality control, and inventory effectiveness reporting. Inventory requirements for AA&E are further delineated in paragraphs 8005 and 8006.

~~3. Commands will prescribe and implement inventory procedures that ensure sight physical counts of arms and ammunition by both in-coming and out-going key custodians each time the custody of the keys is transferred.~~

3. Inventory Adjustments and Losses. No AA&E loss shall be attributed to an accountability or inventory discrepancy unless determined through investigation that the loss was not the result of theft. Documentation for all inventory adjustments, including MLSR Reports and investigation findings, will be retained for 3 years.

8004. AA&E STORAGE FACILITIES. AA&E will be stored as prescribed in paragraphs 8005 and 8006, with the following exceptions.

1. Existing Facilities Located On Military Installations. Existing substandard facilities may continue to be used as long as they provide 10 minutes of forced entry delay and meet the requirements contained within this Manual for arms racks, storage containers, security lighting, key and lock control, and ESS. Structural upgrades to existing facilities must provide 10 minutes of forced entry delay; reference (m) provides both design and retrofit guidelines and requirements. **Substandard facilities must have an approved waiver/exception. All AA&E facilities will meet explosive safety requirements of reference (s) and (t).**

2. Facilities Located Off Military Installations. Substandard facilities may continue to be used but they must provide 10

minutes of forced entry delay; reference (m) provides both design and retrofit guidelines and requirements.

a. Bolts of Risk Category II arms must be removed and secured in a separate building or separate Class 5 container. Bolts so removed will be tagged with the weapon's serial number to ensure return to the same weapon. Etching of weapon's serial number on the removed parts is prohibited.

b. Where AA&E is stored off military installations in civilian communities, and where security checks cannot be conducted by DoD personnel due to legal or operational considerations, liaison shall be established with local law enforcement to ensure that non-duty hour checks are conducted by local police authorities.

3. Arms Storage Facilities in a Field Environment. Arms will be stored in a prepared shelter (e.g. Quadcons, ISO Containers, AAV's, M109 Vans, Tents, pre-existing buildings, etc.), as such, it should provide security personnel with the reasonable means to secure and protect that arms at all times. All shelters are to be hardened with sandbags or reinforced as much as practically possible to provide maximum security. The facility will be guarded 24 hours a day by armed personnel from the interior guard force.

a. The shelter perimeter will be secured with triple strands of concertina wire. Maintain clear zones of 20 feet on the interior and 20 feet on the exterior of the wire. Access through the wire should be limited to one ingress/egress point. Access should be limited to the minimum number of personnel required to maintain the facility.

b. When possible secure weapons in storage racks. When racks are unavailable, use crates or other storage containers to secure weapons. When not possible, connect the weapons together by running a steel cable through the receivers. Low security padlocks or bolts will be used to secure the ends of the cables together.

c. Major weapons parts (i.e. bolts, barrels, receivers, etc) must be secured to the same level as complete weapons.

d. When possible maintain security lighting in accordance with paragraph 8012. When tactical situations deem lighting inappropriate, night vision equipment will be utilized by all guard personnel.

e. The using unit physical security plan will address the protection of AA&E to include maintaining two separate and distinct forms of communication. The communications will be tested on a daily basis. There will be a distinct alarm established to alert the interior guard of a forced entry to the facility. Commanders will utilize all assets available to ensure the security of AA&E.

f. Upon establishment of a field armory, a serialized inventory must be conducted. Each time the facility is opened and closed a sight count will be conducted. Upon disbanding the facility a serialized inventory must be conducted. Commanders will establish a tracking system (e.g. logbook, spreadsheet, temporary 10520) to ensure accountability of weapons coming in and out of the facility.

4. Storage in Naval Vehicles, Aircraft, and Small Craft. When operational readiness impedes storage of arms in armories, or when arms are an integral part of or permanently mounted and are not man-portable or easily removed, arms may be stored in the small craft, vehicle, or aircraft to which assigned. Entry and exit points into holding areas where vehicles, rail cars, or aircraft with missiles, rockets, ammunition, or explosives are parked must be controlled by armed guards. Surveillance and physical check requirements are outlined in paragraph 8010.

5. Personal Protection and Duty Weapons and Ammunition. Weapons and ammunition issued to General/Flag Officers for personal protection, as directed, are exempt from requirements of this manual, except for inventory and loss reporting. Weapons issued to accredited Criminal Investigators are exempt from requirements of this manual (*if compliance impedes mission performance*), except for inventory and loss reporting. In the case of General/Flag Officers and Criminal Investigators, weapons and ammunition will be stored at a minimum, during non-duty hours, in commercial weapons containers within the affected residence. Use of commercial trigger guards/locks is also required during non-duty hours.

6. Security of Small Amounts of AA&E. On military installations, small numbers of arms (not totaling more than 15 Arms) may be stored in a Class 5 security container or weapons locker with a GR 1 combination lock providing forced entry protection as approved by GSA (Federal Specification AA-F-363 (latest series)). The container must be under constant surveillance or protected by an IDS including volumetric sensor, and the facility checked by a security patrol at least once every 24 hours. Containers weighing less than 500 pounds will be secured to the structure.

8005. SECURITY OF ARMS. This paragraph prescribes security standards and requirements for the storage and protection of conventional Category II through IV arms. All category I, II, and III Missiles and Rockets, all category A&E will be stored in fixed structures as prescribed in paragraph 8006.

1. Arms Storage Facilities. Arms will be stored in fixed structures built as prescribed in reference (m), outlined herein, and in accordance with specifications of reference (r).

a. Walls. Walls will be constructed as indicated below:

(1) 8-inch concrete reinforced with No. 4 (12.7-mm) reinforcing bars, 9 inches on center, in each direction and staggered on each face to form a grid approximately 4-1/2 inches square.

(2) 8-inch concrete block (or concrete masonry unit) with No. 4 (12.7-mm) bars threaded through block cavities filled with mortar or concrete and horizontal joint reinforcement at every course.

(3) 8 inches of brick interlocked between inner and outer courses.

b. Floors. Floors will be constructed of 6-inch concrete reinforced with 6- by 6-inch W4 by W4 mesh or equivalent bars.

c. Roof/Ceilings. The ceiling or roof will 6-inch concrete reinforced with No. 4 (12.7-mm) reinforcing bars, forming a grid

so that the area of any opening does not exceed 96 square inches. If the ceiling or roof is of concrete pan-joint construction, the thinnest may not be less than 6 inches and the clear spaces between joists may not exceed 20 inches.

d. Personnel Doors. Doors will be constructed of 1 3/4-inch thick solid or laminated wood, with a 12-gauge steel plate on the outside face, or standard 1 3/4-inch thick, hollow metal, industrial-type construction with minimum 14-gauge skin plate thickness, internally reinforced vertically with continuous steel stiffeners spaced 6 inches maximum on center. General Service Administration (GSA) approved Class 5 or 8 vault doors meeting Federal Specification (Fed Spec) AA-D-00600C may also be used.

(1) Door bucks, frames, and keepers will be rigidly anchored and provided with anti-spread space filler reinforcement to prevent disengagement of the lock bolt by prying or jacking of door frame. Frames and locks for doors will be designed and installed to prevent sufficient removal of the frame facing or built-in locking mechanism to allow disengagement of the lock bolt from outside.

(2) Door frames and thresholds will be constructed of metal.

(3) Door hinges will be strong enough to withstand constant use and the weight of the doors. They will be located on the inside where possible and will be of the fixed pin, as defined in Appendix A, security hinge type or equivalent.

(4) Exterior doors with exposed hinges will be provided with at least two supplemental brackets, pins, or other devices to prevent opening the door by destroying the hinge or removing the hinge pin. Such devices must be of sufficient positive engagement and resistance to shearing force to prevent opening the door from the hinge side.

e. Vehicle or Large Bay Doors. Vehicle or large bay doors will be at a minimum, 4-inch thick sliding doors, constructed of 14-gauge hollow metal, or solid or laminated wood with a 3/8-inch gauge steel plate on the outside as prescribed by reference (m).

f. Windows and Other Openings. Windows, ducts, vents, or similar openings of 96 square inches or more with the least dimension greater than 6 inches will be sealed with material comparable to that forming the adjacent walls. Weapon issue points will not exceed 190 square inches when opened and when not in use will be secured with material comparable to that forming the adjacent walls.

g. Locks and Hasps. All exterior doors will be secured with a high security hasp meeting Military Specification (Mil Spec) MIL-P-29181 and high security lock meeting Mil Spec MIL-P-43607, or an Internal Locking Device (ILD).

h. The following items are also approved for the storage of Security Risk Category III & IV arms:

(1) Modular vaults meeting Fed Spec AA-V-2737.

(2) Portable Explosive Magazine as specified in Naval Facilities Engineering Service Center Technical Data Sheet 82-12, outlined herein, if operationally necessary.

(a) Constructed of 1/4 inch steel plate with a 3-inch interior hardwood buffer.

(b) Ventilation is provided through a top exhaust vent and rectangular side vents constructed with angle iron covers.

(c) The door is constructed with 1/4-inch steel and is mounted on two heavy-duty strap hinges. All hinges vents and shrouds are welded in place. Hinge side protection and high security hasp installation are required in order to store arms.

(d) Further information concerning procurement of the portable explosive magazine is available by contacting Commander, Code 4044, Building 361, Naval Surface Warfare Center (NSWC) Crane, IN, 47522.

i. Arms Racks, Storage Containers, and Safes. Arms in an armory will be stored in banded crates, standard or locally made metal arms racks, or Class 5 GSA approved weapon containers or

safes. Locally made arms racks must be constructed to prevent removal of a weapon by disassembly.

(1) Arms racks will be locked with low security padlocks meeting Fed Spec FF-P-2827 or Commercial Item Description (CID) A-A-1927.

(2) Hinged locking bars for racks will have the hinge pins welded or otherwise secured to prevent easy removal.

(3) In facilities that are not continuously manned, arms racks and containers/safes weighing less than 500 pounds, including weapons, will be fastened to the structure (or fastened together in groups totaling more than 500 pounds) with chains equipped with low security padlocks or with bolts. Bolts must be spot welded, peened, or otherwise secured. Chains will be heavy duty hardened steel or welded, straight link, galvanized steel, of at least 5/16-inch thickness, or equivalent.

► (4) When weapons, in crates or containers, are in transit, stored in depots or warehouses, **within armories**, or held for contingencies, they will be fastened together in groups totaling at least 500 pounds and banded or locked and sealed.

2. Arms Parts. Major arms parts such as barrels and major subassemblies will be protected at least the same as Category IV arms. The frame or receiver of an arm constitutes a weapon and such parts must be stored according to the appropriate category (for example, the receiver of a .30 caliber machine gun must be stored as a Category II arm).

3. Multiple Unit AA&E Storage Facilities. Two or more units may share the same storage facility; however, stocks will be identified and separated by unit.

a. Each unit AA&E storage area will be separated from the other unit storage areas within the same storage facility.

b. Unit AA&E storage area walls will be constructed of galvanized chain-link fencing material or ¼-inch wire mesh covered by material (e.g. plywood, drywall, etc.) that prevents;

- (1) observation of another unit storage area,
- (2) passing or removal of arms from one unit storage area to another,
- (3) ESS sensor devices from penetrating adjacent unit storage areas,
- (4) and the surreptitious entry from one unit storage area to another.

c. Walls may also be constructed of wood framing covered with drywall material.

d. Doors will be installed on each unit storage area. Day-gates will not be used as the main security door to unit storage areas.

e. One unit will be designated as responsible for the security of the entire storage facility in writing, addressed to the affected units.

4. Accountability and Inventories

a. Arms Unique Item Identifier (UII)(formerly serial number) Registration and Reporting

(1) Delineation of Responsibilities

(a) The Army operates the DoD Central Registry that maintains control over UIIs for all arms defined herein, and a file of arms that have been lost, stolen, demilitarized, or shipped outside the control of DoD. DoD Central Registry maintains tapes (forwarded monthly from component registries) containing the most recent UII list of arms. The DON registry is Crane Division, Naval Surface Warfare Center (Code 4086) .

(b) NAVSURFWARCENDIV Crane (Code 4086) is responsible for maintaining a automated registry for UII of arms in their inventory. The registry is updated based on transaction reporting; for example, receipts, issues, and turn-ins.

(c) When the DoD Central Registry receives an inquiry concerning a lost, stolen, or recovered weapon listed as Marine Corps property, or as missing from Marine Corps, the Central Registry informs NAVSURFWARCENDIV Crane, which ensures that:

1) Such losses, thefts, or recoveries are, or have been, investigated and reported as outlined in para 8013.

2) Marine Corps AA&E recovered by police or investigative agencies is returned to Marine Corps control upon completion of the investigative and prosecutorial action.

(2) Non-appropriated fund arms are not reported to the DoD Central Registry, however installations with non-appropriated fund arms will establish procedures to identify such weapons by type and serial number. Foreign captured weapons and war trophies will be registered with the DoD Central Registry.

(3) Registration and Reporting Procedures

(a) Arms UII registration and reporting procedures will ensure control over UII from the manufacturers to depot, in storage, in transit to requisitioners, in activity custody, in the hands of users during turn-ins, in renovation, and during disposal or demilitarization. The DoD Central Registry maintains records of UII adjustments and shipment to flag rank officers, Foreign Military Sales (FMS) and grant aid, activities outside of DoD control, and transfers between DoD components. Activities will inventory incoming shipments promptly after receipt to ensure all items have been received and entered into the DoD or Navy registry, as appropriate and per reference (bb).

(b) National or DON-assigned UIIs will be used by NAVSURFWARCENDIV Crane for transactions to the DoD Central Registry.

(c) All arms, regardless of origin, that are accounted for in unclassified property records must be reported. Automatic weapons will be reported on a priority basis.

(d) Arms with NSN or UII missing, illegible or obliterated, will be reported by message or letter in the

following format to the DoD Central Registry by NAVSURFWARCENDIV Crane for assignment of an NSN and management control UII:

- 1) NSN (NSN or "None")
- 2) Unique Item Identifier (UII or "None")
- 3) Description (Make, model, caliber, nomenclature or other)

(e) When the DoD Central Registry identifies a duplicate UII by arms type in DoD component, the U.S. Army Munitions and Chemical Command will provide instructions for modifying the UII. Movement and shipment of arms must be held in abeyance pending correction of UII.

(f) To ensure the DoD Central Registry is properly maintained, the following is required for small arms shipments:

- 1) Attach two Weapon Serial Number (WSN) control cards for each weapon in shipment to the supply documentation;
- 2) When operational procedures prevent compliance with subparagraph 1, attach a separate listing of WSNs to the supply documentation.

3) Incoming shipments will be opened by a designated receiver and the receipt of each item verified by check of the UII. However, incoming shipments from new procurement received at logistic bases/depot activities that are preservation packaged, need not be individually checked if the contract provides for a 100 percent serial certification by the contractor which is checked by government contract representative based upon acceptable sampling techniques. The receiving activity will conduct random sampling to verify the accuracy of UIIs in each new procurement shipment.

(g) NAVSURFWARCENDIV and other DoD component registries will reconcile inter-service transfers of weapons on a transaction-by-transaction basis. Establish follow-up procedures to ensure the loop is closed on inter-service transfers.

8005 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

(h) Refer questions concerning daily operations to the Navy Registry, Navy Small Arms Management:

Commander
Code 4086
NAVSURFWARCENDIV
300 Highway 361
Crane, IN 47522-5001

b. Physical Inventories of Arms. In addition to physical inventories required by paragraph 8005(c), the following additional minimum requirements will be met:

(1) Arms will only be placed in long-term storage after they have been inventoried by UII.

(2) For level A packs at the unit level and boxed/banded arms at the installation and logistic base level, the inventory shall consist of 100 percent count as reflected by the number of items listed on the boxes.

▶ (3) A complete UII inventory of the contents of any box will be conducted if there is any evidence of tampering **by the Commanding Officer**.

▶ (4) Unit level monthly inventory of all arms by UII will be conducted by a disinterested third party, not in the inventory chain of command and not having access to the items being inventoried, using an extract of the most currently signed Consolidated Memorandum Receipt (CMR). The third party must be a commissioned officer, warrant officer, staff-noncommissioned officer, or civilian equivalent. Persons conducting the inventory will be assigned in writing by the Commanding Officer. Written results of inventories (including seal numbers that were verified on level A packed arms, supporting documentation for arms not on hand (e.g., receipt copy of ERO's, NAVMC 10520), inventory officer appointment letter, CMR extract utilized for inventory, commanding officer's instructions concerning any discrepancies, **and an addendum from the supply officer outlining the corrective action being taken to correct any discrepancies found**, will be provided to the commanding officer.

▶ (5) All arms not level A packed, boxed, banded, and secured with a tamper proof seal will be physically **"sight"** counted upon **initial** opening and **final** closing of any armory.

▶ (6) Records of the inventories (including the signed CMR, inventory assignment letter, letter of discrepancy from inventorying officer, supply officer endorsement, and commanding officers endorsement), and will be retained for a period of three years.

c. Category II, III, and IV Arms

(1) Activities having custody of these items will establish and maintain UII registration, records that provide continuous accountability, and reporting in accordance with reference (y). Additionally, activities will establish procedures for AA&E Responsible Officers to ensure the adequacy of requisition verification of Category II-IV arms. Such procedures shall include positive steps for rejecting excess and unauthorized requisitions.

(2) Inventories. Physical inventories shall be conducted as indicated below:

(a) Unit Level: 100 percent monthly count. 100 percent quarterly inventory by UII.

(b) Installation: 100 percent semiannually inventory by UII.

(c) Logistic Base: 100 percent inventory by UII each fiscal year.

d. Custody Receipt for Arms. Individuals receiving sub-custody of arms (including man-portable hand-launched missile systems in ready-to-fire configuration or easily made ready-to-fire) must obtain authorization from the commanding officer or his/her designated representative and, sign a custody receipt listing serial number and type of item(s) received.

(1) Individuals issued, or in possession of, arms are responsible for its security. If the individual receiving is

unable to provide adequate security as outlined in this chapter, he/she may check out small arms and related ammunition only as an immediate need exists and must return them to the original responsible activity.

(2) Individuals being issued small arms will be qualified as prescribed in reference (o).

(3) Arms should be removed from secure storage areas for as brief a time as possible and in as small a quantity as practical.

8006. SECURITY OF AMMUNITION AND EXPLOSIVES (A&E). This paragraph prescribes security standards and requirements for the storage and protection of conventional Category I through IV A&E, including Category I through III Missiles and Rockets.

1. Ammunition and Explosives Storage Facilities.

a. Bulk Storage Areas (Logistic Bases/Depot Activities/Ammunitions Supply Points (ASP)). All category I, II, and III Missiles and Rockets, and all category A&E will be stored in fixed structures as prescribed in reference (r). Magazines will be constructed to the requirements, outlined herein, in accordance with specifications of reference (m).

(1) Walls. Walls will be constructed with 8 inch (200 mm) concrete reinforced with No. 4 (12.7 mm) reinforcing bars, 9 inches (150mm) on center in each direction and staggered on each face to form a grid approximately 4-1/2 inches (114 mm) square; 8 inch (200 mm) concrete block (or concrete masonry unit) with No. 4 (12.7mm) bars threaded through block cavities filled with mortar or concrete and with horizontal joint reinforcement at every course; 8 inches (200 mm) of brick interlocked between inner and outer courses.

(2) Floors. Floors will be constructed of 6-inch (150 mm) concrete reinforced with 6 inch by 6 inch (150 mm by 150 mm) W4 by W4 mesh or equivalent bars.

(3) Roof/Ceilings. Roof and/or ceilings will be constructed of 6-inch (150 mm) concrete reinforced with 6 inch

by 6 inch (150 mm by 150 mm). Reinforcing bars spacing will form a grid using No. 4 (12.7 mm) or larger so that the area of any opening does not exceed 96 square inches (0.6 sq m.). Ceilings or roofs designed for concrete pan joist construction may not be less than 6 inches (150 mm) at the thinnest point and clear spaces between joists may not exceed 20 inches (500 mm.).

(4) Doors/Frame. Doors will be GSA approved Class 5 Vaults doors, constructed of 1-3/4 inch (44mm) solid or laminated wood with a 12 gauge (2.7mm) steel plate on the outside face. or 1-3/4 inch (44mm) hollow metal, industrial type construction with a minimum 14 gauge (1.9 mm) skin plate thickness, internally reinforced vertically with continuous steel stiffeners spaced 6 inches (150 mm) maximum on center.

(5) Locks. All exterior doors will be equipped with an Internal Locking Device (ILD). High security locks/hasps, Universal Security System (USS), and Anti-Intrusion Barriers (AIB) may continue to be used until replaced.

► (6) Windows and Other Openings. Windows, ducts, vents, or similar openings of 96 square inches or more with the least dimension greater than 6 inches will be sealed with material comparable to that forming the adjacent walls. Weapon issue points will not exceed 190 square inches when opened and when not in use will be secured with material comparable to that forming the adjacent walls. **A&E storage facilities will not be designed or constructed with windows. Existing facilities with windows must meet requirements of reference (r).**

b. The following storage facilities will also meet requirements for bulk storage:

(1) The High Performance Magazine and Security System, designed by the Naval Facilities Engineering Service Center,

(2) The Portable Explosive Magazine, which is constructed of 1/4 inch steel plate with a 3-inch interior hardwood buffer. Ventilation is provided through a top exhaust vent and rectangular side vents constructed with angle iron covers. The door is constructed with 1/4-inch steel and is mounted on two heavy-duty strap hinges. All hinges vents and

8006 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

shrouds are welded in place. Hinge side protection and high security hasp installation are required in order to store A&E. Further information concerning procurement of the portable explosive magazine is available by contacting Commander, Code 4044, Building 361, Naval Surface Warfare Center (NSWC) Crane, IN, 47522.

(3) Storage in prefabricated magazines should be conducted only as operationally necessary.

c. Unit Level (Basic Load, Training, or Operational Quantities). Unit level Category I, II, and III missiles and rockets, and all A&E will be stored in any of the following manners:

(1) Arms rooms constructed in accordance with reference (MIL-HDBk-1013/1A) further defined in paragraph 8005, modular vaults meeting Fed Spec AA-V-2737, portable explosive magazines as defined in paragraph 8006(b)2, or GSA approved class 5 weapons storage container located in arms rooms or modular vaults.

(2) All A&E will be maintained in the original container, banded and sealed to reflect the integrity of the container and contents. A&E maintained in Ready for Issue (RFI) rooms and armories (security ammunition) will be stored in a container weighing 500 pounds or greater. In any instance where this requirement cannot be met, containers will be fastened together to establish a combined weight greater than 500 pounds with bolts and chains, or fastened to the structure. Chains will be heavy duty hardened steel or welded, straight link, galvanized steel, of at least 5/16-inch thickness, or equivalent.

(3) Two or more units may share the same storage facility. One unit will assume all security responsibilities with the responsibility identified in writing, addressed to the affected units. When units fall under different commands, the units/commands will physically separate and fully identify A&E stocks.

2. Accountability and Inventories.

► a. Inventories. Ground A&E accountability and inventories will be conducted in accordance with **reference (cc) for unit inventories and reference (dd) for depot level inventories**.

► b. In no case will a single individual be permitted unescorted entrance into A&E storage facilities or areas. The two man rule will apply at all times.

~~(MCO P8020.10A Marine Corps Ammunition and Explosives Safety Manual). Aviation ordnance accountability and inventories will be conducted in accordance with reference (MCO P8020.11 DoN Explosives Safety Policy). Inventories shall be conducted by a disinterested third party person, not in the inventory chain of responsibility and, not provided access to the items being inventoried. The third party must be a commissioned officer, warrant officer, staff noncommissioned officer, or civilian equivalent. Persons conducting the inventory will be assigned in writing by the Commanding Officer and will provide inventory results to the Commanding Officer. All discrepancies will be noted, investigated, and reported. No A&E loss shall be attributed to accountability or inventory discrepancies before an investigation has determined that the loss was not the result of a theft. Records of inventories will be retained for a period of three years.~~

~~b. Category I, II, and III Missiles and Rockets (Non-Nuclear)~~

~~(1) Activities having custody of these items will establish and maintain UII registration, records that provide continuous accountability, and reporting in accordance with reference (MCO P4400.150E). Such reporting shall include and reflect:~~

~~(a) Missiles and rockets issued for training~~

~~(b) Missiles and rockets returned unexpended from training~~

~~(c) Expended residue, as applicable~~

~~(2) Activities will establish procedures for AA&E Responsible Officers to ensure the adequacy of requisition verification of Category I missiles and rockets. The procedures shall include positive steps for rejecting excess and unauthorized requisitions. Procurement contracts shall provide for individual item serialization.~~

8006

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

~~(3) Inventories. Inventories shall be conducted as indicated below:~~

~~(a) Unit Level: 100 percent monthly sight count; 100 percent quarterly serial number or UII inventory.~~

~~(b) Installation Level: 100 percent monthly sight count; 100 percent semiannual serial number or UII inventory.~~

~~(c) Logistics Base/Depot Level: 100 percent annual inventory by serial number or UII.~~

~~(d) Upon assignment of a new responsible officer, 100 percent serial number or UII inventory is required.~~

~~(4) All Category Ammunition and Explosives. The Conventional Ammunition Integrated Management System (CAIMS) is the central records repository for worldwide Navy non nuclear expendable aviation ordnance. The Retail Ordnance Logistics Management System (ROLMS) is the principal system utilized to perform all ground ammunition inventory activities. All units will maintain stock records that provide continuous accounting in accordance with references (DoD 4140.1 R DoD Material Management Regulation), (MCO P8020.10A Marine Corps Management and Explosive Safety Manual) and (MCO P4400.150 Consumer Level Supply Policy Manual). Inventories shall be conducted as indicated below:~~

~~(a) Unit Level: 100 percent monthly count.~~

~~(b) Installation Level: 100 percent semiannual count.~~

~~(c) Upon assignment of a new AA&E accountability officer and/or key control officer, 100 percent count.~~

~~(5) For all Category Ammunitions and Explosives that are boxed and banded, to include missiles and rockets, the inventory shall consist of, and reflect, a 100 percent count as noted on the container, shipping, or packing list. Any noted signs of tampering or breaching of the container will require a 100 percent count.~~

~~c. Custody Receipt for Ammunition and Explosives. Individual authorized to receipt for ground and/or aviation ordnance must obtain authorization from the cognizant Commanding Officer or his/her designated representative in writing. All ground ordnance transactions will be recorded as directed in reference (MCO P4400.150 Consumer Level Supply Policy Manual).~~

~~Aviation ordnance transactions will be recorded as directed in reference (MCO P9020.10A Marine Corps Ammunition and Explosives Safety Manual).~~

8007. FENCES. Category I and II A&E storage areas must be fenced in accordance with requirements outlined in chapter 5.

8008. AREA DESIGNATION AND ACCESS CONTROL

1. Restricted Area Designation and Posting.

a. All areas containing Risk Category AA&E will be posted as restricted areas per paragraphs 3003 and 3004.

b. Clear zones will be established around all AA&E restricted area perimeter fencing. Clear zones will extend a minimum of 20 feet on the outside and 30 feet on the inside.

▶ c. **Parking within a designated clear zone is strictly prohibited for all government and privately owned vehicles.**

2. Access Control. Unaccompanied access to ammunition and explosives storage facilities will be limited to the minimum number of personnel required to maintain safe, efficient operation. Strict access control will be maintained at all gates leading into AA&E storage areas. Personnel must be designated in writing by the commanding officer. A pass, badge, access roster, or sign in/out system will be used to properly identify authorized personnel.

a. The commanding officer or his/her designated representative must approve visitors. All visitors will be escorted, and their ingress and egress logged. Visitor control logs will be maintained for 3 years.

b. Vehicles and personnel will be subject to random inspections upon entry and exit from AA&E areas.

c. Privately-owned vehicles are prohibited from entering AA&E storage areas.

8009. ELECTRONIC SECURITY SYSTEMS. All AA&E storage facilities located aboard Marine Corps installations will be protected by the MCESS. AA&E storage facilities located outside Marine Corps installations will be equipped with a commercial ESS, that is equivalent to the MCESS. Arrangements will be made to connect the ESS to the local police or a commercial monitoring company from which immediate response to alarm activations can be directed. Approval of all ESS protecting Marine Corps AA&E will be approved by HQMC (PS). In addition to the MCESS/ESS requirements of chapter 7, the following also apply:

1. AA&E storage facilities not equipped with an MCESS/ESS will be continuously manned by an armed guard providing constant surveillance.
2. MCESS/ESS will include point sensors on all doors, other human-passable openings, and interior motion or vibration sensors.
3. Intrinsically safe equipment.
- ▶ 4. The Provost Marshal's Physical Security Personnel will perform periodic unannounced openings of AA&E facilities by setting off an alarm, so that alarm monitoring and security force reactions and procedures can be exercised and evaluated. At a minimum, one drill will be performed semiannually, Record the date, time, and results of security force drills, including deficiencies and corrective action taken, and maintained for at least 3 years. Drills are intended to maintain proficiency, and allow supervisory personnel an opportunity to evaluate and educate security force personnel. **Additionally, the unit AA&E Officer may conduct unannounced openings of AA&E facilities only after coordination has been arranged with the Provost Marshal's Physical Security Section.**
5. AA&E storage facilities with multiple units require each unit storage area to be equipped with its own ESS. The ESS will be configured in such a manner that another unit within the same storage facility cannot activate/deactivate another unit's storage area ESS.

8010. KEY SECURITY AND LOCK CONTROL. In addition to the Key Security and Lock Control requirements of chapter 3, the following also apply:

1. Key custodians will not be unit armorer or other persons responsible for the AA&E storage facilities.
2. Keys to AA&E storage areas, buildings, rooms, racks, containers, and ESS will be maintained separately from other keys. They will be accessible only to those individuals whose official duties require access to them. A current roster of personnel authorized key access will be maintained and kept from public view.
3. Keys to AA&E storage facilities will be provided protection commensurate with the material that the keys allow access.

a. Keys will be provided security during their transport to and from non-working hour storage containers by armed personnel ~~or by using the two-man rule~~.

b. Keys to storage facilities, that allow direct access to the AA&E being protected will be transported by armed personnel, or by using the two-man rule. Direct access is defined as unimpeded access to weapons racks from which weapons can be obtained by simply cutting a low security padlock, upon entrance into the AA&E storage facility.

c. The transport of AA&E keys by armed personnel or the use of the two-man rule is not required if one of the following apply:

(1) The AA&E storage facility is equipped with a GSA approved Class 5 or 8 vault doors meeting Fed Spec AA-D-00600C, equipped with a combination lock meeting Fed Spec FS-L-2740.

(2) The AA&E key non-working hour security container is located within the same restricted area as the AA&E storage facility.

(3) Personnel transporting AA&E keys are equipped with a portable duress, which annunciates at an alarm control center from which a response force can be dispatched. The AA&E keys

and the portable duress will be kept on the same welded or brazed ring. Procedures, approved by the commanding officer in writing, will be provided to the response force indicating the route to be taken by personnel transporting the AA&E keys to their security container.

(4) Personnel transporting AA&E keys are equipped with a two-way voice radio from which a duress code can alert response force personnel of the need for assistance in the event of an emergency. A duress code will be limited to one word, simple, easily recognizable, and will be followed immediately by the location of personnel transporting AA&E keys.

d. Utilization of subparagraphs 3 and 4 requires response force personnel to secure all traffic outbound the installation until an assessment of the emergency can determine if a compromise to the security of AA&E has occurred.

▶ e. When not attended or in use, operational keys to Category I and IV AA&E will be secured in a Class 5 GSA approved security container or equivalent. Equivalent is defined as a security container constructed of 20 gauge steel secured with a GSA approved changeable combination padlock (Fed Spec FF-P-110), and located within a restricted area. ~~Keys to Category III and IV AA&E will be secured in at least a security container constructed of 20 gauge steel secured with a GSA approved changeable combination padlock (Fed Spec FF-P-110).~~

4. AA&E Keys will not be removed from a Marine Corps-controlled space (off installation).

5. The official duties of duty officers or designated representatives may require individuals not on an authorized unaccompanied access roster to safeguard keys to AA&E storage facilities. Such individuals will sign for a container sealed with a GSA approved changeable combination padlock (Fed Spec FF-P-110).

▶ a. When container custody is transferred **which contains a seal and not a padlock**, the **serialized** seal will be checked for

- ▶ original container integrity. Unbroken and intact **serialized** seals will preclude the necessity for physically counting the keys with each change of custody.
- ▶ **b. A logbook will be maintained of all seal serial numbers when removed or replaced. Logbooks will be maintained for 3 years.**
 - c. During non-working hours, staff duty officers or designated personnel will provide surveillance for the following:
 - (1) Security containers, storing AA&E keys, not secured within the same restricted area as the storage facility.
 - (2) Security containers, storing AA&E keys, that allow direct access to the AA&E being protected.
- ▶ **d. Duplicate keys for AA&E facilities will not be maintained in the AA&E facility.**

8011. SURVEILLANCE AND SECURITY CHECKS. For the purpose of this chapter constant surveillance is the continuous visibility of an item(s) or area, or of all means of access to the item(s) or area.

1. Category I through IV Arms

- a. All storage locations ashore without ESS require constant surveillance.
- b. All storage locations afloat without ESS require constant surveillance.
- c. All storage locations ashore and afloat with ESS require a check every 24 hours.
- d. Temporary storage in open areas, vehicles, inadequately secured structures, aircraft ready service magazines and Lockers, rooms, RDT&E test ranges/areas, and production buildings.

8011 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- (1) Without ESS requires constant surveillance.
- (2) With ESS requires one check every 8 hours.

2. Category I through IV Ammunition and Explosives

a. Category I Missiles and Rockets

- (1) All storage locations ashore without ESS require constant surveillance.
- (2) All storage locations, in port, without ESS require checks every 2 hours.
- (3) All storage locations, at sea, without ESS requires one check every four hours.
- (4) All storage locations ashore and afloat with ESS require checks every 24 hours.

b. Category II Ammunition and Explosives

- (1) All storage locations afloat without ESS, but with high security hasps require one check every 24 hours.
- (2) All storage locations afloat with ESS require one check every 24 hours.
- (3) All approved magazines ashore without ESS require constant surveillance.
- (4) All approved magazines ashore with ESS require one check every 24 hours.
- (5) Temporary storage in open areas, vehicles, inadequately secured structures, aircraft ready rooms and service magazines and lockers, RTD&E test ranges and areas, and production buildings without ESS require constant surveillance.
 - (a) Without ESS requires constant surveillance.
 - (b) With ESS requires checks every 8 hours.

c. Category III Ammunition and Explosives

(1) On station reinforced concrete construction without ESS requires one check every 24 hours.

(2) On station reinforced concrete with ESS requires no check.

(3) On station frame construction without ESS require one check every 12 hours.

(4) On station frame construction with ESS requires one check every 24 hours.

(5) Temporary storage in open areas, railcars, vehicles, aircrafts, etc;

(a) Without ESS during operational hours requires constant surveillance.

(b) Without ESS during non-operating hours requires hourly checks.

(c) With ESS requires one check every 24 hours.

(6) Temporary storage in ready service rooms, magazines and lockers, RTD&E tests ranges and areas, and production buildings;

(a) Without ESS requires checks every 4 hours during non-operating hours.

(b) With ESS requires one check every 24 hours.

d. Category IV Ammunition and Explosives

(1) On-station reinforced concrete or frame construction with or without ESS requires one check every 24 hours.

(2) Temporary storage in open areas, railcars, vehicles, aircraft, etc., without ESS requires constant surveillance

8012 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

during operating hours and one check every hour during non-operational hours.

(a) Without ESS requires constant surveillance during operating hours.

(b) Without ESS requires checks every hour during non-operating hours.

(b) With ESS requires one check every 24 hours.

(5) Temporary storage in ready service magazines and lockers, rooms, production buildings with or without ESS requires a check every 24 hours.

e. Temporary Barge Storage at Anchorage or Ammunition Piers

(1) Category I and II

(a) Without ESS requires a 24-hour armed guard.

(b) With ESS requires a check every 8 hours.

(2) Category III and IV

(a) Without ESS requires a check every 4 hours by boat at anchorage.

(b) With ESS requires a check every 12 hours.

(3) Temporary storage in ready service magazines and lockers, rooms, production buildings without ESS requires a check every 24 hours.

8012. SECURITY LIGHTING. Exterior lighting will be provided above ingress/egress points for the facility, and shall be of sufficient intensity to allow security personnel to observe unauthorized activity in and around the area.

a. Security lighting, designed to provide complete perimeter coverage, may be accomplished by using pole or

building mounted fixtures; however, it's recommended that such lighting be connected to motion sensing devices.

b. Switches for exterior lighting will be installed in such a manner that they are accessible only to authorized individuals.

▶ 8013. COMMUNICATIONS. All AA&E storage areas must maintain two separate and distinct forms of communication. The ESS duress button is recognized as a form of communication. The additional form of communication will be either a two-way radio or phone. The communication system will be tested on a daily basis; **however, coordination will be made with the MCESS Operator prior to testing duress buttons, which will prevent the dispatching of the response force. All forms of communication in the ammunition supply point (ASP) area will meet HERO standards.**

8014. PHYSICAL SECURITY SURVEYS. Physical security surveys of AA&E facilities (including AA&E Research, Development, Test, and Evaluation (RDT&E) Centers, Ammunition Supply Points, Production Buildings, and Ready Service Magazines and Lockers) will be conducted as prescribed in paragraph 3001. Additionally:

1. Reviewing status of any corrective action taken on security deficiencies noted during previous surveys, assistance visits, or command inspections.

2. Ensuring waivers and exceptions for AA&E security have been requested where appropriate, copies of approved current waivers and exceptions are on file, and compensatory measures are being enforced.

3. Comparing a random selection of AA&E items with listed inventory quantities.

▶ 4. **Physical security survey comments concerning Program 8 of the Explosives Safety Inspections (ESI) will be forwarded to MARCORSSYSCOM PM AMMO, 2200 Lester Street, Quantico, VA 22134-5060.**

8015 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

8015. PHYSICAL SECURITY PLAN. The installation physical security plan will address the protection of AA&E.

8016. READY FOR ISSUE (RFI) AA&E STORAGE AREAS. Arms and ammunition may be stored together in the same area only for security force personnel. Those arms and ammunition must be secured in separate containers when not being issued or received, and only the minimum necessary to complete the mission. Security force RFI AA&E storage areas are not required to have a high security locking device, an AIB, ESS, or meet construction standards provided all other requirements contained within this Manual and the following conditions are met:

1. Security force personnel with communication equipment to summon assistance must maintain constant surveillance of the area(s) or door to the area(s) at all times;
2. Security force personnel whose other duties, such as the monitoring of alarms and desk sergeant must not interfere with constant surveillance;
3. Storage areas are inventoried at each change of watch; and
4. Access to the area is restricted.

► 8017. DISPOSAL AND DEMILITARIZATION. Disposal of AA&E to (Foreign Military Sales, transfer to law enforcement agencies, etc.,) is governed by reference (z). Demilitarization of all AA&E will be conducted as directed by reference (z). A technically qualified Marine Corps, or U.S. government representative, will perform the demilitarization, and will complete, sign, and maintain, a certificate of demilitarization. One copy of the certificate will be maintained with the affected AA&E, until the item is disposed of. All museums, offices spaces, and other areas desiring to display demilitarized AA&E, must request permission from the installation security manager. A copy of the demilitarization certificate will be maintained in the affected building in close proximity of the affected AA&E.

The certificate must be produced for examination upon request. **For ammunition items a request for disposition must be sent to the Designated Disposition Authority (DDA) MARCORSSYSCOM PM AMMO.**

8018. ROTC/GUN CLUB/RESERVE UNIT PROHIBITIONS. Reserve Officers Training Corps (ROTC/JROTC) units and gun clubs are not authorized possession of Category I or Category II AA&E. ROTC units may possess Category II during authorized training with active DOD Components. Reserve units will not store Category I AA&E at their facilities, but may be given temporary custody of Category I AA&E for training on military installations, as specified by the installation commander.

8019. CLASSIFIED AA&E. Classified AA&E must be protected as directed by this chapter and reference (b).

1. A GSA approved Class 5 vault door, or a door as described in paragraph 8005.1.d secured with a high security hasp and padlock will be used on structures housing classified AA&E.
2. AA&E classified SECRET or CONFIDENTIAL will receive protection equivalent to that provided for Security Risk Category II and III respectively (or higher if required by the assigned risk category).

8020. MARINE CORPS RESALE FACILITIES AND EXCHANGES. Minimum standards for Exchange Resale Facilities are:

1. Store AA&E per this instruction.
2. Use only empty ammunition boxes for display.
3. Keep arms in display racks that are locked with low security locking devices (see appendix D) and kept under constant visual surveillance during open hours. Display only one model of each type of arm. Move all arms from sales areas to an armory after open hours.
4. Take a 100 percent count daily and a 100 percent inventory

8021 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

by serial number weekly. Retain records for 3 years.

5. Comply with Federal legislation, State laws, and local ordinances. Prominently display State laws and local ordinances next to where sales take place.

8021. MARINE CORPS MUSEUMS AND UNIT DISPLAYS. AA&E will be safeguarded per this instruction unless it is certified as demilitarized under OPNAVINST 8020.14 and NAVSEAINST 4570.1A (reference (k). However, historically significant items must be protected without damaging their operational or aesthetic value. No museum AA&E item will be permanently altered by cutting, welding, or any other means without the written approval of the Marine Corps University, EDCOM, MCCDC (HDM).

1. Storage. Secure arms in an armory or appropriate container as prescribed in paragraph 8005, and ammunition per paragraph 8006.

▶ 2. Display. Only antique or unique items may be displayed. Current AA&E items (live ammunition and weapons which use self-primed metal cartridges) will not be displayed if functional. **Arms will** ~~They may~~ only be displayed if they are modified to render them ~~temporarily~~ inoperable by removal of firing pins and/or other key internal components (store these components separately in a secure container). **Ammunition will only be displayed when completely inert.**

a. On exhibit cases containing weapons, use locking hardware and break-resistant glass or plastic with secure mounting hardware. Other methods include attachment with wire to secure stanchions.

b. Use an IDS with point sensors (preferably Balanced Magnetic Switches (BMS)) on all doors and other man-passable openings, and area (volumetric) sensors covering weapons display areas;

c. For items exhibited in static outdoor displays, remove minor caliber weapons (up to 25mm) from vehicles and mounts

(they may be replaced with reproductions). Medium and major caliber weapons (3 inch and larger) will be rendered inoperable.

d. Museum personnel will check arms displays every 2 hours during public visitation hours, and the structure every 8 hours during closed hours.

3. Inventory arms by **sight** count every month, and by serial number every quarter. Keep records for 3 years.

8022. ORGANIC/UNIT AND STATION MOVEMENTS OF AA&E

1. Organic/Unit Movements. Commanding Officers will provide security commensurate with the Category and significant military value of each AA&E shipment, and they, or a designated representative may modify guidelines on a case-by-case basis if operations necessitate. Any changes will be reported to HQMC (I&L(LPC)) for evaluation of standards and modifications as necessary. Commanding Officers are directed to acquire and assess current FPCONS in order to further evaluate security of, and the need for, shipments during increased FPCONS.

2. On Station Movements. Movements via organic and commercial vehicles will adhere to all security requirements with the exception that Satellite Motor Surveillance (SM) is not required. AA&E contained in organic and commercial vehicles outside of restricted areas will be under constant surveillance. ~~Within restricted areas,~~ Organic movements of **AA&E** requires ~~two explosive drivers,~~ ~~or~~ one explosive driver and one assistant driver, while commercial vehicle drivers will meet Defense Transportation Tracking System (DTTS) guidelines. Category I and II movements within restricted areas will be conducted with seals in place, while Category III and IV do not require seals.

a. Category I and II AA&E movements will be conducted only after all accountability entries are documented and receipt/issue forms are completed. Designated unit of issue for each item will be noted and receipt/issue documentation will accompany the shipment at all times. Transfer of custody between points on station will be maintained using receipt/issue

documentation containing type, quantity, date and time of transfer, type, and the signature of the person receiving custody.

b. An armed guard is required aboard Marine Corps installations for the movement of any amount of Risk Category I and II.

c. Accountability for ammunition and explosives manufactured and renovated on station and involving bulk explosives, propellants, and illuminants, will begin when and where the items in process become finished products.

d. AA&E contained in vehicles, vans, and railcars must be parked in designated restricted areas. Each door to the conveyance will be secured by a numbered seal that meets specification FF-S-2738, "Seals Anti-Pilferage" (latest revision), Type 11 or 12. Protection will be provided for stocks of numbered seals and seal inventory records to prevent theft or alterations to documents that accompany movements and shipments to points inside and outside the activity. All AA&E will be under constant surveillance or each vehicle, van, and railcar will be physically inspected by a security patrol every hour.

3. Off Station Movements. Movements will adhere to commercial standards set forth in reference (DOD 4500.9-R), chapter 205, except that SM is not required. The level of physical security protection varies with the FPCON status at origin and/or at destination. Note that CAT I and CAT II movements off-station require the accompaniment of a security escort vehicle (SEV) under all FPCON conditions. ~~Two explosive drivers, or~~ One explosive driver and one assistant driver ~~are~~ **is** required for all A&E movements off-station. For AA&E off-station movements, the drivers must maintain 2-way radio communication capability with the originating installation, the destination installation, and municipal law enforcement and emergency response officials along the planned route. Military movements of AA&E on and off-station will adhere to the requirements cited above, except that armed guard surveillance will be subject to local command policy and direction based on the assessed threat and the need to safeguard mission integrity.

a. Off-station transport of small quantities of explosives by Explosive Ordnance Disposal (EOD) personnel and in the transportation of Military Working Dog (MWD) explosives training aids is authorized. These evolutions will normally not require armed guard surveillance unless otherwise directed by the commanding officer in response to heightened threat conditions. The explosives must be in the custody of designated EOD or MWD personnel or secured in designated vehicles. Use of privately-owned vehicles may be authorized by the commanding officer in writing.

b. Commanding officers may authorize transportation of small arms and associated ammunition to facilities on or near a military installation for marksmanship training, competition, or other requirements on a case-by-case basis. The commanding officer's authorization may also include CONUS transport of .30-06 and .30 caliber ammunition of up to 12,000 rounds for Director of Civilian Marksmanship Program. Weapons and ammunition must be in the custody of a designated individual. Use of privately owned vehicles (POV) for this purpose may be authorized by the commanding officer in writing. When POVs are used, consistent with the vehicle design, the arms and ammunition must be securely stowed and protected from view. A locking mechanism must be provided for stowage spaces aboard the POV. The arms and ammunition must be under constant surveillance during stops enroute to destination.

4. Shipping and transportation. Shipments of AA&E, categorized in Appendix (h), and Class 1.1, 1.2, and 1.3 ammunition and explosives, will be protected against loss, theft, or damage. Protective Service requirements are provided in reference (ee), while safety, security and traffic management guidelines during transportation of AA&E is addressed in reference (ff). All classified AA&E will be stored and transported in accordance with this manual and reference (b). With the exception of inventory and daily checks, Military Preposition Ships (MPS) are exempt from AA&E requirements of this manual. Commanding Officers will ensure that all requirements of transportation security are adhered to at all times. Additional protection for AA&E shipments, based on threat information, may be provided. Under no circumstances, will AA&E be provided protection not adequate with the requirements of this manual.

a. HQMC (I&L)(Code (LPC-3), will support Marine Corps Component Commanders, supporting Unified Theater Commanders, in all transportation matters. Additional support is provided from Naval, Military Traffic Management Command (MTMC), and Military Sealift Command (MSC) Components, HQMC (I&L) will:

(1) Ensure transportation protective measures utilized for all A&E shipments are established in applicable tariffs, government tenders, agreements, or contracts.

(2) Negotiate with commercial carriers for establishing transportation protective measures that meet both shipper and Marine Corps requirements.

(3) Determine the adequacy of services provided by commercial carriers for A&E movements.

(4) Provide routing instructions as required, and requested by shipper.

(5) Ensure that all transportation security guidelines incorporate and maintain established Force Protection Condition (FPCON) measures as provided in reference (gg).

b. AA&E security at military and commercial terminals will conform to standards outlined in this manual. These standards will be provided to commercial carriers by MTMC. AA&E shipments shall normally be processed through air-operated and managed air and ocean terminals, or through DoD approved commercial air and ocean terminals. A listing of approved terminals is available from MTMC. In transit protection of AA&E at commercial and military terminals shall be in accordance with Defense Transportation Regulations (DTR) and applicable MTMC Freight Traffic Rules. Instances of non-compliance shall be reported to MTMC Command Operations Center.

c. OCONUS commercial transportation services will adhere to requirements of this order. When and where available, export and import shipments will be processed through military managed and operated air and ocean terminals, or through DoD approved commercial air and ocean terminals. When requirements cannot be met, compensatory measures will be addressed and emplaced in

order to lessen the threat and Commanders will notify HQMC (I&L (PSC)).

(1) AA&E shall be transported on locked and sealed containers (MILVAN, SEAVAN, or CONEX). When utilizing commercial carriers to transport sensitive weapons and ammunition of the same caliber, they will not be combined in the same package or on the same pallet. Shipments of one pallet are exempt. Missile main body sections will be shipped separately from launch, guidance, and control sections. Uncategorized hazard class 1.1, 1.2, and 1.3 A&E will be afforded the same protection as Category III A&E. Every effort will be made to consolidate shipments into Truckload (TL) and Carload (CL) quantities. Less than TL quantities are extremely vulnerable to theft. AA&E shipments shall be locked/sealed and inspected on transit as specified in Chapter 205, of the DTR. Shipments of AA&E scheduled for demilitarization and retrograde will receive protection commensurate with the prescribed Category in Appendix H. Receiving commercial and military activities must be capable of securing and protecting AA&E during normal working hours and also after normal working hours.

(2) All Category I shipments will provide a continuous audit trail from shipper to receiving activity, with advance serial number certification. Two-man certification is required at all shipping and receiving points. Category I ordnance main bodies, launchers, guidance, and control sections will be packaged and shipped separately.

(3) Small quantities of A&E, generally less than 200 pounds gross weight, of Category IV small arms ammunition, Class 1.4, may be shipped via DoD CIS regardless of FPCON. These shipments may be transported via the DoD blanket purchase agreement awarded carriers under the GSA schedule provided the shipments are within the contract's size and weight limitations. Inert, non-hazardous ordnance components may be sent via registered mail (return receipt requested) when the shipment size and weight meet U.S. Postal Service (USPS) requirements.

(4) Carriers shipping Category I through IV items, via rail, are required to immediately notify the receiving activity of the shipment's arrival at the prescribed rail-yard. Instructions shall be provided to rail carriers transporting

Category I and II items requiring them to immediately notify the receiving activity of a shipment arrival at rail yards.

5. Shipment Inventory. Shipments shall be checked upon receipt by the receiving activity to ensure that seals are intact and for any signs of theft, tampering, or damage. If seals are intact, and there are no signs of damage or tampering, Category I and II AA&E will be checked within 24 hours, while Category III and IV AA&E will be checked within 48 hours.

6. Installation Commercial Carrier Support. Contingencies, emergency and non-emergency, may arise requiring installation support to commercial carriers in transit. Increased FPCON declarations may cause commercial carriers to request installation access and temporary accommodations. Additionally, requests may be in response to conditions that include, but are not limited to, vehicle difficulty, natural disasters, driver illness, etc. Marine Corps installations are required to provide temporary parking, safe haven and secure holding support to commercial carriers transporting DoD owned AA&E, if requested. Support requirements exist whether or not the load is destined for the affected installation. Installation response may be limited and influenced by current FPCON, the shipment Security Risk Category, the level of security offered by the installation, and explosive safety quantity distance (ESQD) limits of the secure holding area. In the event that the ESQD limits of the secure holding area do not meet load requirements, Commanders will identify another installation site that meets ESQD limits.

7. OCONUS installations are required to coordinate with commands to arrange in-country security for delivery only to the nearest U.S. controlled port facility.

8023. SECURITY STANDARDS FOR SECURE HOLDING AREAS FOR AA&E. For the purpose of the Marine Corps, safe havens and secure holding areas are one and the same. Secure holding areas are locations within the installation restricted area that is used for the temporary parking of commercially owned motor vehicles carrying government owned AA&E, or the staging of AA&E. Secure holding area security requirements are identified in reference (ee), outlined herein, will comply with references (s) and (t).

1. Security standards for the secure holding of Category III and IV, and uncategorized HD 1.1, 1.2, and 1.3 are as follows:

a. General. AA&E will be afforded double barrier protection. Secure holding areas will have access controlled and be within an area surrounded by a perimeter fence to limit access (perimeter fence may be the installation/facility boundary fence). For situations in which the guard does not have direct unobstructed view of the entire secure holding area, it will have an IDS or CCTV system to provide added security.

b. Restricted Area Signs. Restricted area sign posting will be per paragraphs 3003 and 3004.

c. Access Control. The installation commander or facility director will establish strict personnel and vehicle access measures for the secure holding area. Procedures will be in accordance with Service security regulations.

d. Fencing. Where used to delineate a secure holding area, all fencing will be in accordance with chapter 5, paragraph 5003.

e. Lighting. Protective lighting will be provided to discourage or deter attempts by intruders, make detection likely if entry is attempted and prevent glare that may temporarily blind guards. Security lighting will be automatically timed and controlled to provide illumination from dusk until dawn. Design lighting to not unnecessarily expose/silhouette guards or other personnel to targeting by criminal/terrorist elements. Lighting will illuminate the area beyond the perimeter to the outer edge of the clear zone that extends 25 feet beyond the secure holding area. The installation commander or facility director will insure a professional lighting survey is conducted for each facility, and a lighting plan will be approved by the commander or director as a part of the overall plan.

f. Power. Primary and alternate power sources will be identified. The primary source may be installation power or a local public utility. An alternate source will be provided to start automatically upon failure of the primary power, adequate to power the entire lighting system. It will be equipped with adequate fuel storage and supply, be periodically tested under

load to ensure effectiveness, and located within a controlled area for additional security. All electrical cabling and telephone lines within 10 feet of the ground will be encased in metal conduit to preclude lines from being manipulated/cut.

g. Key and Lock Control. A formal key and lock control program will be established per chapter 3, paragraph 3005.

h. Communications. Communications will provide a means of alerting local law enforcement and/or response forces to the presence of intruders immediately. The area will have a duress system that is linked to the response force to report emergencies.

j. Security Checks. Security patrols will check secure holding areas at a minimum interval of once each hour. They will be aware of the location and nature of classified, hazardous and sensitive equipment or material in the holding area. Additional security force requirements are addressed in Chapter 4.

2. Additional Security Standards for the secure holding of Category I and II AA&E.

a. Secure holding areas for Category I and II AA&E and all AA&E materials designated as secret must be under constant surveillance as outlined in this manual.

b. Dedicated, 24-hour surveillance by guard or IDS/CCTV coverage will be expanded to include the secure holding area.

c. Vehicle undercarriage inspections will be performed on all inbound traffic entering the secure holding area, if not already checked as a part of installation entry procedures.

d. Coordination will be made with local, county or State law enforcement to provide additional security, including back-up forces, during higher FPCONS, as required.

3. The installation physical security plan, per paragraph 2002, will address the protection of secure holding areas

4. Protection for Classified Shipments. Classified SECRET

shipments will be afforded the same physical security protection as for CAT I and II AA&E. Classified CONFIDENTIAL or CCI shipments will be provided the same security as CAT III/IV/UNCAT Hazard Class/Division 1.1, 1.2, and 1.3 AA&E.

8024. SPECIAL CONSIDERATIONS FOR SMALL QUANTITY SHIPMENTS.

Small quantity shipments are individual shipments of 15 or fewer small arms, or 200 pounds or less of ammunition or explosives.

1. Small arms and missile components (excluding ammunition and explosives) may be sent by registered mail (return receipt requested) when the size and weight meet U.S. Postal Service requirements.
2. Small quantities of AA&E may be shipped by commercial carrier providing DoD Constant Surveillance Service (CSS) (as the only required transportation protective service) when loaded in a locked container, and the size, weight, and safety factors meet the carrier requirement.

8025. REPORTING OF MISSING, LOST, STOLEN, AND RECOVERED (MLSR) AA&E. Marine Corps activities will report missing, lost, stolen, or recovered AA&E, and gains or losses due to inventory adjustments per Chapter 10.

8026. SIMULATED WEAPONS SYSTEMS. The Marine Corps currently maintains two types of simulated weapons systems that support enhanced marksmanship training. Based on system differences, security requirements are outlined below:

1. Indoor Simulated Marksmanship Trainer (ISMT). The ISMT is an interactive audio/video weapons simulator instructed with lasers to simulate target engagement. ISMT employs imitation weapons with forged imitation parts. The imitation parts render the simulator incapable of firing an actual projectile. Commanders are encouraged to provide the same level of storage as other high dollar items.
2. Special Effects Small Arms Marking Systems (SESAMS). SESAMS is a user-installed weapons modification kit that allows Marines

to fire low velocity marking ammunition at short ranges, precluding the weapon(s) from firing live ammunition. The SESAMS Kits should be provided the same level of security as high dollar items, but weapons associated with SESAMS will be secured per paragraph 8005.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 9

CRIME PREVENTION PROGRAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	9000	9-3
PROGRAM ELEMENTS	9001	9-3
PROGRAM OBJECTIVE	9002	9-4
CRIME FACTORS	9003	9-4
RESPONSIBILITIES	9004	9-5
SCOPE	9005	9-7
COMMUNITY RELATIONS/CRIME PREVENTION PROGRAMS	9006	9-9
STORAGE AND SECURITY OF PERSONAL AND NON-GOVERNMENT ARMS, AMMUNITION AND EXPLOSIVES	9007	9-10
LOST, FOUND, AND ABANDONED PROPERTY	9008	9-12
MARINE CORPS EXCHANGE CRIME AND LOSS PREVENTION	9009	9-19

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 9

CRIME PREVENTION

9000. GENERAL. Crime prevention is any measure taken to reduce the opportunity for crime by improving community safety through measures such as increased awareness and confidence, improved planning and design, and committing to strategies and programs that address risk factors. Crime prevention is key in the quality of life issues within our communities in the effort to minimize hazards and threats that result from criminal and anti-social behavior. Installation commanders will protect Marines, Sailors, family members and civilian Marines from criminal acts by minimizing the opportunity and inclination to commit a crime. Crime prevention is a responsibility of all Marines, Sailors, family members and civilian Marines. A successful Crime Prevention program serves as an excellent public relations tool for the installation and for the Marine Corps.

9001. PROGRAM ELEMENTS. A successful Crime Prevention Program must be tailored to the specific needs of an installation or command.

1. Programs will incorporate three major elements; education, prevention, and enforcement.

a. Education emphasizes providing and presenting timely, pertinent information to the community. This is accomplished through continuous and comprehensive community interaction, crime prevention awareness training (briefs, etc.), news media (installation paper and television), the internet (local area network, dedicated websites), and crime prevention material (pamphlets, handouts, etc).

b. Prevention focuses on reducing conditions conducive to criminals committing crimes against the Marine Corps, persons, and property. Prevention reduces the opportunity and desire to commit a crime.

c. Enforcement ensures timely detection and investigation of criminal activity, and the apprehension and prosecution of the criminal(s).

9002 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

9002. PROGRAM OBJECTIVE. The primary objective of a Crime Prevention Program is to provide effort and support that enhances Marine Corps combat readiness mission by producing and fostering a sense of community. Objectives are accomplished by:

1. Increasing the morale and personal safety of Marines, Sailors, family members and civilian Marines aboard Marine Corps installations and activities.
2. Protecting government assets and personal property from theft, misuse, and unlawful destruction.
3. Reducing manpower, time, and administrative costs in the investigation, pursuit, and prosecution of criminal activity.
4. Achieving maximum support and involvement of the entire Marine Corps community, in association with Military Police, for crime prevention activities.
5. Under no circumstances will crime prevention initiatives compromise the safety and security of Marines, Sailors, family members and civilian Marines. Conversely, properly designed fire and safety regulations need not compromise crime prevention efforts.

9003. CRIME FACTORS. There are three factors common to every criminal act; the desire of the criminal, the ability to commit the offense; and the opportunity to commit the offense.

1. Early detection of crime leads to an increased chance of apprehending the offender, and reduces the possibility of destruction of physical evidence that may be critical to the prosecution of the offender(s).
2. Crime Prevention programs need to address hardening of likely targets of crime, recognition and appraisal of crime risks aboard the installation, and an increased level of public awareness.

3. One of the most significant factors in decreasing violent crimes is reducing alcohol and drug abuse. Commanders must continue to educate Marines on the Corps' no-tolerance alcohol and drug abuse policy.

9004. Responsibilities. Installation commanders are responsible for developing and maintaining a Crime Prevention Program. The staff officer for the program aboard the installation is the provost marshal.

a. Installation commanders will:

(1) Establish and maintain an installation wide Crime Prevention Program.

(2) Establish crime prevention goals for areas of concern and outline procedures necessary to attain the goals.

(3) Establish standard operating procedures for the control of personal weapons and ammunition stored or transported aboard the installation, in accordance with paragraph 9008 of this Manual.

(4) Ensure crime prevention and physical security measures are coordinated with the installation Antiterrorism Officer, fire department, and safety personnel to ensure compatibility with initiatives and regulations.

(5) Ensure crime prevention matters are presented to the installation physical security council as a means for planning and evaluating the effectiveness of crime prevention and physical security initiatives.

(6) Provide funding for purchasing crime prevention materials and equipment.

(7) Conduct a monthly welcome aboard brief for new-join personnel and family members detailing information about the installation, installation services, and the local community.

b. The Provost Marshal will:

(1) Supervise the conduct of physical security and crime prevention surveys for installation organizations and activities in accordance with this Manual.

(2) Liaison with local civilian police agencies to foster and maintain a working relationship in support of a coordinated security and crime prevention effort.

(3) Identify funding requirements to maintain a robust Crime Prevention Program.

(4) Direct and support manpower and equipment requirements, as necessary, for those recommended community relations and Crime Prevention Programs outlined in paragraph 9006 of this Manual.

(5) Provide annual crime statistics to the installation commander and CMC(PS) in accordance with paragraph 10004 of this Manual.

(6) Support unit crime prevention briefs as requested.

(7) Support the Commander's Welcome Aboard Brief.

(8) Establish and maintain a Lost and Found Property Program in accordance with paragraph 9008 of this manual.

c. The Provost Marshal's Office Physical Security Section will:

(1) Provide the installation Public Affairs Office (PAO) crime prevention media for release in installation newspapers, television, and other media sources. One article or presentation will be published monthly, at a minimum.

(2) Conduct crime prevention surveys as directed by the provost marshal, and in accordance with paragraph 9005 of this Manual.

(3) Maintain installation crime statistics to identify trends and areas of increased criminal activity.

(4) Conduct annual installation Crime Prevention briefs.

(5) Conduct unit level Crime Prevention briefs as directed.

(6) Conduct community relations and crime prevention programs identified in paragraph 9006, as directed.

(7) Brief new joins and family members on installation and state law enforcement and crime prevention matters.

d. The installation PAO will support the Crime Prevention Program through the use of radio, television, newsprint, LAN, and other media.

e. The command inspector will support the Crime Prevention Program by actively inspecting unit crime prevention efforts and the availability of the installation Fraud, Waste, and Abuse Hotline.

f. Unit commanders, including tenant commands, will support the installation crime prevention plan as directed by the installation commander.

9005. SCOPE. Crime Prevention is a command responsibility that requires planning, support, awareness, and participation at every echelon of command including tenant organizations.

1. Staff Assets. Staff asset integration, involvement, resources, and ideas are key to the success of the program. Assets include the Provost Marshal; Staff Judge Advocate (SJA); Personnel Officer; Base Inspector; Chaplain; Comptroller; Substance Abuse Counseling Officer (SACO); Public Affairs Officer (PAO); Facilities Officer; Marine Corps Community Services (MCCS); Navy/Marine Corps Relief Society.

2. Media Use. Installation commanders need to take advantage of available news media to promote the program. Media reaches a wide audience and increases awareness of Crime Prevention and the command's emphasis. Newspapers articles, television

"infomercials", and local area network (LAN) announcements are excellent media platforms. Banners, handouts, and bumper stickers are excellent vehicles for promoting the program as well. Company and higher commanders will ensure that command bulletin boards contain Crime Prevention Materials that reinforce issues such as securing valuables and wall lockers. Additionally, Commanders will ensure command briefs encompass crime prevention information.

3. Crime Prevention Surveys. Crime prevention surveys are conducted to identify the nature, extent and underlying causes of criminal activity, or conditions conducive to criminal activity within an area or a specific facility. A survey is an analysis to identify conditions that may indicate the presence of, or potential for criminal conduct. Crime prevention surveys recommend corrective action to a commander for the purpose of reducing the opportunity for crime.

a. Crime Prevention surveys will be conducted by Physical Security Specialists assigned to the PMO.

b. Crime Prevention surveys will be scheduled with the responsible organization. Organizations will assign an individual to assist the Physical Security Specialist during the course of the survey.

c. Crime Prevention surveys will be completed using the CMC(PS) mandated Physical Security Survey Reporting System or, at those activities where there is no system, the NAVMC Form 11121 or an equivalent electronic copy. A guide for completing the survey is provided in Appendix E.

d. Crime Prevention checklists may be obtained from the PMO Physical Security Unit.

e. A Crime Prevention survey will be conducted at the following facilities:

- (1) Bachelor Enlisted Quarters (BEQs).

(2) Bachelor Officer Quarters (BOQs).

(3) Government facilities that maintain negotiable instruments.

(4) Facilities designated by the installation commander.

(5) Facilities requested by unit commanders, at the discretion of the Provost Marshal.

4. Armed Forces Disciplinary Control Board. Installation commanders will establish and maintain an installation Armed Forces Disciplinary Control Board (AFDCB) in accordance with reference (hh). The board will meet on a quarterly basis to identify establishments and areas that are detrimental to the well being of Marines aboard the installation. The board will publish and release all findings. Unit commanders are required to brief their Marines, and post the AFDCB findings in conspicuous location.

5. Crime Analysis. An effective Crime Prevention Program requires a systematic approach and crime analysis identifies target areas for increased crime prevention efforts. Common Marine Corps target areas are ideal for command emphasis and education. Common target areas include:

- a. Personal security aboard the installation.
- b. Personal security while on leave and liberty.
- c. Security of personal property in the barracks.
- d. Quarters/home security and crime prevention.
- e. Child and Spouse Abuse. (NOTE: Physical abuse of a child or spouse is a crime punishable under the Uniformed Code of Military Justice (UCMJ). Actual or suspected abuse discovered by medical, school, daycare, or other persons will be immediately reported to the installation provost marshal for investigation and further reporting requirements).

9007 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- f. Security of government property.
- g. Security of Automated Data Processing equipment.
- h. Fraud, waste, and abuse of government property.
- i. Reporting of Missing, Lost, Stolen, Recovered (MLSR) government property.
- j. Security of Marine Corps Community Services (MCCS) retail and service activities.

9006. COMMUNITY RELATIONS/CRIME PREVENTION PROGRAMS. There are a number of Crime Prevention Program options available to commanders. National, state, and local programs offer further program guidance and information. Commanders are encouraged to use all available assets to supplement the program including installation specific designs. Installations commanders need to design their program around the specific needs of their military community. Proven programs include:

- a. Child Identification (CHILD ID). This program provides parents an up to date record of a child's fingerprints, photograph, and other identification data. Fingerprint cards, and photographs will be presented to the child's parent or guardian. Under no circumstances will a child's identification data be maintained in government files.

- b. Child Beware. Presented to children to increase their awareness that strangers may represent a danger to them. Children are encouraged to report strangers and unusual incidents to parents, teachers, and Military Police officers.

- c. Officer Friendly. Designed to familiarize children and adults with the roles and responsibilities of Military Police Officers, and enhance community relations.

- d. Citizen Awareness Program. Designed to educate the base community through all available media about typical crimes occurring on the installation and throughout the surrounding communities. The program provides prevention tips concerning

the crime trends and can target specific event prevention tips (Halloween, Christmas, etc.).

e. Crime Prevention Month. Using all available media, this effort is directed at increasing community awareness of the crime(s) that affect the community and what is available to address the issues and combat crime.

f. Lady Beware. An informational program developed with the goal of preventing rape and sexual assault. Rape scenarios are presented and discussed. Emphasis is placed on high-risk situation avoidance. Local police departments, Rape Crisis Centers, and the installation Family Service Centers should be invited to attend as part of a community effort.

9007. STORAGE AND SECURITY OF PERSONAL WEAPONS AND AMMUNITION. Storage of personal weapons in Marine Corps armories must be authorized, in writing, by the Commanding Officer or authorized individual. One copy of the authorization letter will be maintained in the affected armory/magazine, while the affected owner(s) will maintain a second copy. Personal weapons or ammunition will not be stored in a magazine.

a. Federal, state, and local statutes will be adhered to concerning possession of explosives in a non-official capacity.

b. Storage of explosives in government quarters is prohibited.

c. Each transaction regarding the receipt and issue of personal weapons and ammunition will be recorded in a logbook in a single event format. Logbooks will be opened and closed on an annual basis and will be retained for three years.

d. Personal weapons maintained in government quarters will be stored in accordance with installation directives. Installation commanders will publish directives on the storage of personal weapons within government quarters pursuant to federal, state and local statutes.

e. Storage of any weapon in Bachelor Enlisted Quarters (BEQ) is strictly prohibited. Personal weapons storage within

Bachelor Officer Quarters (BOQ) and SNCO BEQ is at the discretion of the installation commander.

f. Personal weapons will be stored in a separate container, or weapons rack (size permitting), but never in the same container with government arms or ammunition.

g. Storage of personal ammunition in an armory is at the discretion of the commanding officer. The ammunition will be stored in a box/container, but never in the same box/container as government ammunition. The individual ammunition box/container is required to identify the owner, shell or casing count, and other identifying characteristics in order to maintain accountability.

h. Withdrawal of ammunition or weapon(s) requires the owner(s) provide a copy of the storage authorization letter to the custodian with at least one form of identification. Each transaction regarding the receipt and issue of personal weapons and ammunition will be recorded in a logbook in a single event format.

i. Inventory of personal weapons and ammunition (if applicable) maintained in an armory will be conducted concurrently with the unit level monthly inventory. Personal weapons will be listed, by serial number on a separate document from government weapons. Caliber, lot number, and other distinguishing characteristics will be listed on the personal weapons and ammunition inventory checklist.

j. Loss or theft of personal weapons or ammunition will be reported to the installation PMO.

k. In the event a personal weapon(s) or non-government ammunition is abandoned in an armory or magazine, an attempt will be made to locate the owner(s) in accordance with reference (z) and Title 10 U.S. Code, 2575. Once the requirements of reference (z) and Title 10 U.S. Code, 2575 have been satisfied, and the owner(s) not located, commanders will ensure that the weapon(s) and/or ammunition is destroyed in accordance with reference (ii).

1. Waiver and exception provisions are not extended to requirements for storage of personal weapons and ammunition.

9008. LOST, FOUND, AND ABANDONED PROPERTY. Lost, found, or abandoned property is defined as deserted, unclaimed property discovered aboard the installation. Found property will be turned over to Military Police for proper handling and further disposition.

1. Policy

a. Any found or abandoned property turned over to the custody or control of Military Police will be handled in accordance with references (jj) and (z). The installation provost marshal will publish instructions for receipt, handling, and disposal in accordance with this Manual.

b. All government property designated as found or abandoned will be initially treated as lost and found property, and processed in accordance with this Manual. The property will be turned over to the cognizant supply office in a timely manner for further disposition.

c. Property determined to have evidentiary value will immediately be turned over to the Criminal Investigative Division (CID) Evidence Custodian.

d. The Provost Marshal will assign, in writing, a Lost and Found Custodian who will be responsible for processing all lost and found property. An alternate custodian will be assigned in writing to assume duties in the absence of the primary custodian.

e. The provost marshal will designate a secure storage area for lost and found property. Access will be limited to the primary and alternate custodian on an unaccompanied access roster. The access roster will be maintained inside the main entry point.

f. A container will be provided for temporary storage after normal working hours. Access to the temporary container will be

restricted to the primary and alternate lost and found custodian.

2. Property Receipt and Storage.

a. Military Police that come into receipt of found and/or abandoned property will immediately complete a Department of the Navy Evidence/Property Custody Receipt (OPNAV 5527/22) and further mark the property with a Department of the Navy Evidence Tag (OPNAV 5527/17B).

b. The PMO Desk Sergeant will receive the property in order to ensure that the activity is entered in the Military Police Blotter. During normal working hours, the property will be turned over to the Lost and Found Custodian in a timely manner; after normal working hours the property will be deposited in the temporary lost and found locker.

c. Upon receiving property from the Desk Sergeant or the temporary lost and found locker, the lost and found custodian will move the property to the Lost and Found Secure Storage Area.

d. All property will be immediately entered in a lost and found property logbook. Lost and found property logbooks will be maintained on an annual basis (Jan 1 -Dec 31). Property entries will be identified with a lost and found case number. Case numbers will be numbered sequentially beginning with the number 001 and the last two digits of the corresponding year (i.e. 001-05, 002-05, etc.). Each entry will identify, at a minimum, the date of receipt, a brief item description, current location, item disposition, and date of disposition.

e. A case folder will be opened for each item received. The purpose of the case folder is to maintain comments concerning when the items have been published for public information as required by federal law. The case folder will also contain the original Property Custody Receipt once the property disposition has been completed. Case folders may be stored with the property however it is not required.

3. Handling, Storage, and Destruction. Certain items require special handling, storage and destruction. The following paragraphs identify some special instructions. In events not covered, lost and found custodians will obtain further guidance from the Provost Marshal/Commanding Officer.

a. Firearms

(1) Definition. For the purposes of this instruction, firearms are defined as a weapon and all components therefore, not over .50 caliber which will, or is designed to, or may be readily converted to expel a projectile by the action of an explosive. Firearms include, but are not limited to; handguns, rifles, shotguns, black powder muskets (including matchlock, flintlock, or percussion caps), BB and pellet guns, and any instrument capable of firing a projectile.

(2) Storage. Upon turn-in of a firearm, Criminal Investigative Division (CID) will be notified. The on-duty CID Agent will be responsible for assuming custody, or determining further disposition.

(3) Destruction. Firearms not claimed by certified owners will be destroyed. A certified armorer will accomplish destruction in accordance with the reference (ii). The Lost and Found Custodian and one other designated individual will witness destruction, and all parties will sign the Property Custody Receipt as a witness to the destruction.

b. Ordnance. Found ordnance will be reported immediately to the Criminal Investigation Division and the installation Explosive Ordnance Disposal (EOD) Unit. The ordnance will be turned over immediately to the EOD Unit for disposition. All Marines will be instructed to treat ordnance as unstable and ensure that only authorized, trained personnel conduct handling.

c. Alcoholic Beverages. Disposal of unopened containers will be completed by opening each container and emptying all contents in an approved location/container. The Lost and Found Custodian and one other designated individual will conduct/witness destruction, and sign the Property Custody Receipt as witnesses to the destruction.

d. Money/Negotiable Instruments. All money, government checks, and other government negotiable instruments not claimed will be turned over to the installation Finance Office.

e. Department of Defense (DOD) Identification Cards and Badges. Department of Defense U.S. Government Identification cards will be turned in to the installation Centralized Identification Center/DEERS office. Badges will be turned over to the issuing agency.

f. Contraband. Contraband can be defined as items identified as illegal and prohibited aboard an installation. Contraband includes, but is not limited to, knives, martial arts weapons not in the possession of trained, authorized personnel, and miscellaneous weapons prohibited by state and installation orders. Contraband will be destroyed. The Lost and Found Custodian and one other witness will conduct/witness destruction and sign the Property Custody Receipt as witnesses to the destruction.

g. Miscellaneous. Items such as toilet articles, cosmetics, used/soiled personal items and undergarments having no value except to the owner are excluded from processing. The items will be listed on the Property Custody Receipt and may be disposed of within 24 hours. Disposition will be noted on the Property Custody Receipt.

h. Lost and found property stock will be inventoried on a quarterly basis by an officer or SNCO not directly involved in the supervision of the storage and disposition of lost and found property.

i. In any cases not covered by this instruction the Provost Marshal will provide guidance.

4. Public Notice. With the exception of contraband and dangerous items, the lost and found custodian will take all necessary steps to locate the owner(s) of all lost and found property. Measures for locating owner(s) are:

a. Contact the CID section to determine if the item has been reported as stolen or missing.

b. Contact local police departments to determine if the property was reported as being stolen or lost.

c. Check previous Military Police blotters, unit crime prevention Identification (ID) records, and base stolen property lists to determine if the property has been reported stolen or lost.

d. If the item is engraved/marked or has other identifying marks that may be an owner's name or social security number, check base and worldwide locators, local telephone books, and/or email databases for a possible residence or leads to the owner.

e. The lost and found custodian will advertise lost items in the installation newspaper, television station, or LAN, at least once a month. The media article should provide a brief description of an item, the lost and found custodian's name and contact number. Instructions for reclamation of the property during business hours will also be included in the article. A note of the date of the advertisement will be made in the appropriate lost and found file for each item mentioned.

5. Claim and Release of Property. Any person claiming to be the owner of found or abandoned property will be required to contact the lost and found custodian for reclamation. A person(s) claiming ownership of the item(s) will be required to provide as detailed of a description of the article as possible. Proof of ownership (receipts/registration cards, etc.) will be copied and placed in the case notes. The lost and found custodian will have discretion concerning the release of property. In the event of a dispute, the matter will immediately be referred to the Provost Marshal.

a. When an owner is determined:

(1) Property may be claimed by the owner, his/her heirs, next of kin, or legal representative at any time prior to disposition in accordance with references (jj) and (z). If the property is claimed by anyone other than the owner, the Property/Custody Receipt will contain the following statement:

"The action of this installation in transmitting the property

does not vest title in the recipient. Such property is forwarded to you to be retained or disposed of as custodian, in accordance with the laws of the state of the owner's residence"

(2) In the event that known property is not claimed by the owner, or if his/her heirs, next of kin, or a legal representative, the lost and found custodian will send a letter by certified or registered mail to the owner or the last known address, which will contain the following statement:

"Under the law, 10 USC 2575, you are hereby advised that the property described above shall be sold or otherwise disposed of at (location/approximate date). A request for the return of property shall be honored, if received before the time specified herein. Requests for return of property after the specified time shall be honored, only if disposition has not been made"

(3) An owner requesting that the item(s) be shipped to a location off of the installation must be notified that he/she may have to incur part or all of the expenses for shipping.

b. Once an item has been released, the final disposition will be annotated in the found property logbook and the appropriate case file.

c. When an owner has not been determined and the property has been maintained for a period of at least 45 days, the process for disposal may begin.

6. Procedures for Final Disposal of Items. If after 45 days of diligent effort to identify the owner (which is chronologically documented) proves unsuccessful, the lost and found custodian may prepare the items for final disposition. All property that does not meet disposal requirements outlined in paragraph 3 must be presented to a Lost and Found Disposal Board for final disposition instructions as required in references (jj) and (z). No property will be maintained for a period greater than 120 days.

a. The Lost and Found Disposal Board will meet at least quarterly and will consist of a minimum of three individuals.

One commissioned officer and one or more SNCO assigned in writing by the Provost Marshal. It is the responsibility of the Disposal Board to determine fair market value of each item presented and provide disposal instructions to the lost and found custodian.

b. The Board will ensure that all efforts to ascertain or locate the owner or their heirs, next of kin, or legal representatives have been exhausted and that these efforts have been properly documented.

c. The Board will then examine each item and determine its fair market value. Once all items have been inspected, findings of the board will be prepared. A letter will provide further disposition instructions. The letter will contain results of the Board's determination and will include an inventory sheet. The inventory sheet will identify fair market value and disposal instructions. The lost and found custodian will be responsible for carrying out instructions of the board and ensuring that each item is provided a copy of the Disposal Board findings.

d. Property identified to be disposed of will be turned over to the installation Supply Office or the Defense Reutilization Marketing Office (DRMO) for further disposition. Each item turned over to DRMO will require a copy of the Disposal Board findings and a DD Form 1348-6 (DoD Single Line Item Requisition System Document).

e. After an item has been released or disposed of, the final disposition will be annotated in the lost and found property logbook and the appropriate case file.

f. All case folders, logbooks, and associated materials involved with lost and found items will be maintained for three years.

9009. Marine Corps Exchange (MCX) Crime and Loss Prevention. Marine Corps Exchange facilities, to include Convenience/7-Day stores will maintain a vigorous Crime and Loss Prevention program. MCX facilities will meet all requirements of this

Manual to include those requirements outlined in this paragraph. Further guidance concerning merchandise loss prevention requirements are provided in reference (kk).

1. Facility Requirements

a. Entry/exit doors will be kept to a minimum allowed for safety. Primary customer doors will be constructed of a shatter resistant composite. Office, storage, and warehouse doors will be constructed of solid metal. All doors will be secured to walls in metal frames. Hinge pins for all doors will be located on the interior or be constructed with non-removable hinges.

b. Fire exit doors will be equipped with a panic bars or an emergency exit device in addition to the primary locking device. Panic bars and emergency exit devices will be equipped with an audible alarm. Signs must be posted on fire doors indicating that it is an emergency exit only and warning of alarm.

c. Cash handling areas, high value storage, and arms and ammunition doors will be constructed of solid metal and will be equipped with a secondary locking device with a minimum 2 inch bolt that protrudes into the door frame.

d. MCX personnel entry doors will be posted in such a manner to identify that entry is restricted to MCX personnel.

e. Cash cage doors and external doors designated for employee entrance or exit and/or trash disposal should be equipped with a peephole to enable employees to identify person(s) outside prior to opening door. Security glass may be used, but will be of the type that does not allow a view to the interior from the exterior of the facility.

f. Warehouse Doors. Doors to warehouses should be secured with strong metal hasps and heavy-duty padlocks, except for those designated as fire exits. Overhead doors should be of the metal, rollup type, and secured at night from the inside with high quality padlocks. At exchanges with non air-conditioned warehouses, especially in warmer climates, metal, overhead rollup grill-type doors will be installed. These doors may be kept in a lowered position during working hours, yet provide for

the circulation of outside air within the facility. The grills should be secured at night with a high quality padlock. This arrangement will provide double protection during nonworking hours when used in conjunction with the regular doors. Roll-up doors will be constructed of at least 1 inch metal plating and secured to the exterior walls with a metal frame.

g. The activity manager or authorized representative will ensure that locking devices, other than panic bars, are unlocked when the building is occupied.

2. Accessible Openings. All windows will be equipped with locking devices. Windows located within 14 feet of the ground that provide entry into cash handling, high value storage, arms and ammunition storage, and warehouse areas will be provided with protective coverings (rod and bar grills, metal mesh screens, etc.). Skylights, vents, transoms, and other openings that may provide access to the interior of the store will be equipped with a locking device. Locking devices include deadbolts, hasps and pad locks, or crossbars.

3. Lighting. Facility lighting will meet requirements outlined in paragraph 3010 of this Manual.

4. Electronic Security Systems. Exterior doors, windows, and accessible openings must be equipped with electronic security. MCX Managers will coordinate installation, maintenance and testing with the installation PMO. Systems, including duress alarms will be tested quarterly. Added protection may be afforded by installing contacts on interior doors that can be "zoned" to permit deactivation of facility areas while maintaining active alarms in other areas. This arrangement would allow clean-up and stock crews to work in a portion of a facility without compromising security in cash offices, warehouses, stock rooms, etc. All alarm tests will be coordinated with the PMO. A record of these tests will be maintained for three years.

5. Key and Lock Control. Key and lock control will be established in accordance with paragraph 3005 of this Manual. Security can be maintained only if keys to exchange spaces are properly safeguarded and if access is controlled. Locking

devices on exterior doors must be equipped with a cylinder type dead-bolt locking device; except for those doors designated as emergency exits which will be equipped with a detex-type panic bar and alarm. The exterior door cylinder may be of the interchangeable core variety for cost effectiveness. The exchange officer or designee must be responsible for key control. Accurate records must be kept of all keys and locks, including padlocks. This record must reflect the location of each lock, the keys assigned to each employee, and the date issued. Lock cores must be changed whenever the system is compromised through theft or loss of keys, or through employee termination. The records must be continually updated to reflect these changes. Keys should be marked with an identity number so that personnel responsible for key security can tell where they are usable. Duplicate or spare keys should be kept in a locked cabinet in a secure area. Locks shall be changed immediately whenever the custodian of a space is relieved, or when the keys are lost or compromised.

6. Opening and Closing Procedures. When an activity is opened, an inspection will be immediately conducted to include, but not be limited to safes, doors, security room windows, and stockroom merchandise. Any noted irregularities will be reported to the Exchange Officer immediately. Any evidence of burglary or attempted burglary will be reported to the Military Police immediately. Nothing will be touched or disturbed until Military Police have completed a preliminary investigation.

a. A supervisor and at least one other employee will be responsible for the daily opening and closing of an activity.

b. At the close of each business day, the ranking supervisor and/or authorized representative will make an inspection of the premises. The inspection will assure that all safes, doors, windows, etc., have been secured, and that no person is hiding in bathrooms, stockrooms, warehouse, or any area of the exchange. The supervisor will set alarms and exit the premises.

c. Persons assigned as security officers, or other designated personnel will make periodic checks to ensure all

access points are secured. All alarm systems are operable, and opening and closing procedures are being complied with.

d. If the alarm cannot be activated at the conclusion of business, security and exchange personnel will notify Military Police. In the event that an off-base alarm company monitors the alarm, the alarm company will be contacted for immediate response to correct the problem. Exchange officials should be alerted to the possibility that the alarm system has been deliberately tampered with to prevent activation. Under no circumstances should an activity be secured until the alarm system is operable.

e. Alarm systems will be tested no less than monthly, to ensure that the proper alarm signals are being received for the correct activity by Military Police and/or the alarm monitoring company. Logs will be maintained of all tests.

f. Unauthorized personnel (friends, relatives, etc.) will not, at any time, be authorized access to any area of the exchange not open to the public.

7. Cash Handling. The exchange officer or designee will establish written procedures for handling and safeguarding cash instruments and ensure familiarity with those procedures by all employees. Included in the written instructions will be procedures for reducing cash on hand to a minimum and the control of alarm-system keys.

a. Transporting Funds. Transportation of funds to or from a banking facility will be accomplished by at least two employees. Transportation will be accomplished during daylight hours to avoid unnecessary exposure of funds and exchange personnel during hours of darkness. A receipt, in duplicate, will be made out and signed by cash courier and activity manager, for the correct number of cash bags picked up at each activity. The activity manager will retain one receipt and one copy turned into the main cash office with the cash bags. Activity managers will positively identify all cash couriers and lock cash bags before relinquishing possession. Couriers will maintain a log of each bag by number and activity.

(1) At no time will a cash courier vehicle containing cash and/or negotiable instruments be left unattended. In case of breakdown, the couriers will remain with the vehicle until the cash and/or negotiable instruments have been adequately safeguarded. All cash courier vehicles will be equipped with two-way radios or cell phone. Radios or cell phones should be used to report locations, times of arrival, and departure from activities and in cases of emergency to alert Military Police.

(2) At the discretion of the exchange officer, exchange-owned vehicles that frequently transport large amounts of cash instruments may have courier safes installed. A courier safe is one in which cash bags may be dropped but not retrieved by the cash courier. The head cashier may open the courier safe only. Courier safes will be fastened to the vehicle frame with carriage bolts installed with the retaining nuts on the interior of the safe to preclude removal from the exterior. Printed signs reading, "The courier does not possess keys/combo to this container" shall be affixed to the door to deter robbery.

5. Cash Handling Spaces. Cash cages and check cashing offices must receive special attention due to the large amounts of money generally on hand.

a. Cage Construction. Cashier cages, booths, and other areas where large sums of cash and checks are kept will be constructed from true floor to true ceiling of solid materials. Doors will be provided with automatic inside-locking devices and kept locked at all times. Solid doors to cashier cages will be provided with a view panel glazed with security glass or with peepholes to enable cashiers to identify persons desiring entry.

(1) Cashier cages in facilities not equipped with a vault will be arranged in such a fashion that safes and cashiers are visible to the public to avoid concealment of possible holdup or burglary. Windows will be constructed of ballistic resistant security glass with recessed cash trays.

(2) Access doors to cashier cages will be kept to the absolute minimum. Access to cashier cages will be limited to those persons assigned in writing by the Exchange Officer.

Security or supervisory personnel will escort unauthorized persons requiring entry. Doors will be posted to identify entry is prohibited by unauthorized personnel.

(3) The door in cash office will be equipped with magnetic door contacts connected to existing alarm system. This door must be on a separate "zone" to allow the cash office to remain activated while the rest of the alarm system is deactivated. The safe in the cash office will also be alarmed and "zoned". All cash cages will be provided with a duress button.

(4) Cash register funds will be kept in individual securable containers, i.e., lockable register trays or lockable zipper secured canvas moneybags. Each bag will be clearly marked with the applicable register number.

(5) All safes must be kept locked at all times.

b. Prior to opening, and at the close of business daily when cashiers and other designated personnel are engaged in disbursing, collecting, and consolidating cash receipts and change funds, all external doors except employees' entrance/exit and activity doors in use for trash disposal will be closed and locked. Those doors will be controlled to preclude access to the facility by unauthorized personnel. Only authorized exchange and security personnel will be permitted in the facility.

8. Cash Storage Containers. A GSA approved burglar, tool, torch, and fire-resistant safe will be provided for the storage of all exchange funds. Each individual responsible for major accounts will be provided a safe. Exceptions will be cashiers and salesclerks who have custody of the funds only for daily working purposes. Safes weighing less than 750 pounds will be secured to the structure by encasing in concrete or steel strapped to floor or wall supports, when practicable. Safes will be included in the overall alarm system coverage and keyed separately from the building alarm system. This will prevent safe alarms from being deactivated when building alarms are turned off when management enters the building.

a. Safes will be located in a properly secured area that will be illuminated at night and, where possible, visible to security patrols for checking when activity is secured.

b. Safes will never be left in day-lock position with dial turned slightly off last combination letter for convenience. Unless opened for withdrawals or deposits therein, safes will be fully locked at all times with combination dial spun at least three full revolutions.

c. When a safe is opened, the dial will be shielded to prevent compromise of the combination.

d. The Exchange Officer will assign each safe custodian in writing. Safe combinations will be issued only to the assigned custodian. The combination shall be recorded, placed in an envelope, securely sealed in such manner that it cannot be opened without mutilating the envelope or seal, and delivered to the Exchange Officer. The Exchange Officer will issue a receipt for the envelope. Sealed envelopes, containing safe combinations entrusted to the exchange officer, shall be retained in a safe under the exchange officer's direct control until returned to the responsible person or opened in the case of emergency. The safe will be opened, only in an emergency situation, by the exchange officer and in the presence of at least one witness.

e. Combinations changes to safes shall be in accordance with paragraph 3005.11.

f. Safe combinations will be set only by an accountable exchange official or by an employee whose duties require knowledge of safe/vault combinations. Where practicable, a responsible employee may be trained to assist in changing safe/vault combinations. The responsible employee will prepare the combination mechanism for the new setting and after it has been set by the accountable exchange official or other employee required to know the new combination, will lock the mechanism in place without knowledge of the new combination. Where more sophisticated locking devices are employed, the services of a professional locksmith may be required. If a locksmith is used, exchange management will ensure that the locksmith does not have

access to the new combination numbers after the exchange officer has set it.

g. The numbers used for safe combinations should be randomly selected rather than based on birthdays, telephone numbers, or addresses, etc., of persons having the combination.

h. Safe/vault combinations will be memorized and not left in or on desks or hidden in or around the facility.

i. After the combination has been reset, the lock will be tried four times with the door open to ensure that the new combination functions properly.

9. Warehouse/Stockroom Operation. Warehouses are a vital element in retail business. However, the nature of warehouse and stockroom operations creates a high vulnerability to criminal losses. Pilferage by employees causes a large percentage of warehouse/stockroom accountability losses. The number of personnel assigned to warehouse/stockroom operations should be sufficient and procedures adequate, for the protection and prompt movement of merchandise.

a. Internal Controls. Physical security of warehouses is primarily directed toward the prevention of loss resulting from break-ins. The determination of adequate physical security for warehouses is a management decision taking into consideration location, structural integrity of the building, value of assets involved, and periods of exposure (unmanned or unguarded). The following measures must be incorporated in an effort to maintain internal controls:

(1) Proper documentation is highly important in controlling shrinkage warehousing facilities.

(2) Incoming shipments must be checked for accuracy. All shortages, overages, and damages must be noted and signed for before the carrier leaves.

(3) All shipments must be posted to the freight register immediately upon receipt.

9009 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

(4) All incoming and outgoing shipments must be accomplished by proper documentation completely filled out and signed.

(5) Merchandise must be checked carefully against the purchase order to determine correct cost and sell price.

(6) On direct delivery items, only authorized personnel will receive the merchandise and check direct delivery contracts to ensure proper cost and sell price. It must be the responsibility of the merchandisers to ensure that all deviations from the original prices on the direct delivery contracts are forwarded as soon as possible to the concerned activities.

(7) Activity and department managers must ensure that price marking is accomplished accurately.

(8) Incoming shipments must be kept segregated from outgoing merchandise.

(9) Transfer documents must accompany merchandise at all times.

(10) All vehicles, delivering goods, must be secured with adequate locking devices and secured with a numbered seal. Seals will be examined and compared to seal numbers listed on the trip ticket by the receiving activity manager. Trucks delivering goods to more than one activity should be compartmentalized by loading last delivery first, sealing that area with a numbered seal before loading merchandise for next activity, etc. Separate store deliveries will not be stored together and each activity manager may, by comparing seal numbers, be responsible for only that activity's merchandise. Seal numbers must be listed for each activity on trip manifest.

(11) Price marking will be accomplished in accordance with applicable directives.

(12) All marking and ticketing supplies must be carefully controlled.

(13) All trash boxes must be flattened and trash removal carefully supervised by management.

(14) All surveyed merchandise must be accompanied by proper documentation and disposed of in accordance with established procedures.

(15) Warehoused merchandise must be carefully arranged to preclude having the same merchandise in more than one location.

(16) Warehouse personnel must be instructed in the proper method of stacking and picking merchandise to prevent damage to merchandise and accidents to personnel.

(17) Stock record cards must be kept current and accurate.

(18) Overdue merchandise purchase orders must be brought to the attention of buyers for possible cancellation.

(19) All warehouse areas must be secured by the supervisor, ensuring that all access areas are locked and the alarm is operable before leaving facility at the end of the day

b. Pilferage Control. A fundamental element of effective pilferage reduction is controlling the movements of employees and visitors, thereby limiting access to warehouse merchandise. Another method of controlling pilferage is to eliminate, to a large extent, in-store stockrooms wherever possible. These stockrooms can be a constant problem and are usually redundant, especially in exchanges with attached warehouses. Part of the problem in warehouse security arises because there is generally not the same close supervision of a warehouse as there is of the main store. When a warehouse is not located adjacent to the principal buildings, it poses additional security problems.

(1) Three pilferage methods unique to warehousing are:

(a) Circumventing the normal security procedures for critical merchandise by diverting it to a general storage

location, with the intent of stealing the merchandise from a less secure area.

(b) Conspiring with drivers to steal merchandise by failing to completely unload an incoming conveyance or overloading an outgoing truck without proper documentation.

(c) Conspiring with a driver and/or employee of an activity by adding undocumented merchandise to shipments.

10. Employee Guidance

a. Employee Lockers. All exchange employees should be provided with an area where personal gear may be secured. These lockers will be of sufficient size and strength and secured with a built-in combination lock for which the combination may be changed upon reassignment or termination of the employee. Employees are not permitted to take personal belongings to their workstations.

b. Employee Package Area. Ideally, this secure area will be located adjacent to the employee entrance/exit. Employees will not be permitted to bring merchandise, purchased in the exchange, to their workstation. A secure area will be provided for these packages. All packages, brought in by employee with the intention that they are to be taken out, will be secured until the employee is ready to leave the premises at the conclusion of the work shift. All purchases and packages brought into the exchange will be secured in this area until redeemed at the conclusion of the employees' work shift. At small branches or facilities, the package area may be a portion of the manager's office.

c. Employee Parking Area. Employees must be provided with a clearly marked parking area, a reasonable distance from all exchange and warehouse entrances and exits. This serves a dual purpose. First, it does not allow for easy access from an exchange warehouse exit or loading dock to the employees' auto. Second, it allows patrons to park closer to the facility in spaces that might normally be taken by exchange employees. Printed rules should be conspicuously displayed in the employee area regarding lockers, packages, and parking.

d. Employee Entrance/Exit. Employees will be instructed to use this door upon entering and exiting the facility. Exchange employees must use only one door for entrance and exit. The Exchange Officer will designate the entrance/exit and the policy must be strictly enforced. Employees will not be allowed to exit and enter through fire doors, back doors, warehouse loading docks, etc., based on convenience. Employee designated entrances/exits must be controlled and monitored especially before the facility opens for business and after closing until all employees leave.

11. Store Loss Prevention

a. Surveillance Devices. Judicious location and proper use of two-way mirrors and observation platforms can serve as both a deterrent to internal theft and as an aid in shoplifting detection. Surveys have shown that amateur shoplifters, especially teenagers, fear observation booths more than any other anti-shoplifting device. These booths have an additional cost-effective advantage. They are relatively inexpensive to install, and need not be constantly manned to act as a deterrent to shoplifters. When manned, at least two security persons are required to form an effective communications link between the observer and the activity floor.

b. Surveillance devices, which may be installed at minimum expense, include two-way mirrors, one-way glass, convex mirrors, and peepholes.

c. Closed circuit television (CCTV) camera systems are relatively expensive to install and maintain since the system must be constantly monitored for maximum efficiency. The most judicious use of this system is when it is employed to monitor employee activities in areas such as warehouses, loading docks, and cash offices. An unmanned CCTV system may also act as a deterrent. Whichever type of CCTV system used, all video feeds should be recorded.

d. The decision to install surveillance devices will be the responsibility of the exchange officer, bearing in mind the cost effectiveness of the surveillance program.

e. Security Communications. To provide effective security surveillance of exchanges, warehouses, and stockroom areas, and the employment of surveillance devices, consideration must be given to communications capabilities between security personnel and the exchange management. Basically, there are three methods of security communication adaptable to exchange requirements. Selection of equipment should be a management decision, based on the type of surveillance devices, if any, in use.

(1) Signals. Signal lights are located at strategic points within an exchange for use in requesting assistance of security personnel. Advantage of this system is simplicity and minimal costs. The main disadvantage is that signals may become known to shoplifters, causing them to avoid apprehension by discarding merchandise.

(2) Telephone Intercom. Basic extensions of existing telephone system are installed at remote observation points that are used for surveillance. The system offers direct communication between observation point and security or exchange management on sales floor. The main disadvantage is that security/exchange management must normally be paged phonically over exchange public address system. Paging should be coded to avoid alerting suspects. Installation cost is usually minimal. Periodic dummy security announcements ("Security please report to area b") over the public address system may act as a deterrent and serve notice to potential shoplifters that there is a security force on the premises.

(3) Two-Way Radios. Effective for both pilferage and shoplifter control. Mobility of these devices makes them most effective in stockrooms, warehouses, and other open areas. Major disadvantage is that the obvious use of two-way radios becomes detrimental to the effectiveness if security officers are posing as customers while maintaining surveillance. Other considerations include static, interference, restrictions created by terrain, and building configuration.

11. Service Station Operation. Service stations are likely targets for fraud, waste, and abuse. This may be due, in part to the fact that service stations are generally located away from the main exchange where employees are not under constant

surveillance by exchange management. Losses at service stations may be attributed, for the most part, to loose or nonexistent controls. Exchange management must make every effort to closely monitor service station operations and controls on a constant basis. At least weekly visits to the station should be made, more often if necessary. These inspection visits will reinforce exchange management's concern for honest, efficient operation of the service station. In addition to management visits, the following controls should be instituted and maintained:

a. Managers or designees will retain keys to fuel pumps and storage tanks.

b. Cash Control. All cash register controls discussed in this manual apply to registers in service stations. The widespread use of credit cards at Marine Corps service stations, together with the large amount of currency handled on a daily basis, mandates that all applicable control procedures be followed at all times.

(1) The number of personnel authorized to record cash add credit card sales on cash registers should be kept to a minimum for increased cash accountability.

(2) Where practicable, a register with a cash key, charge key, and at least four departmental keys should be utilized for proper sales analysis. One key is for recording of fuel sales, one for motor oils, one for parts and accessories, and one for labor and service charges.

(3) Unexplained cash shortages and overages will be investigated by the exchange officer or designee, to determine cause of discrepancy.

(4) Work orders must be validated by the activity manager or designee at the cash register to support proper recording of sales.

(5) At the end of each business day, the service station daily report and original job sheets for all rendered services will be submitted to the accounting office to be verified against the money turned in.

(6) On a daily basis, the service station manager will verify, record, and reconcile the total fuel pump dollar-meter reading to the net cash register reading for fuel sales.

(7) When service station hours extend past dusk, a minimum of cash should be detained in the cash register. Excess cash will be deposited in a bank night repository, or if that is impractical, in a locked safe within the station.

(8) The service station manager for all credit card forms issued and used, including voids, will maintain an accountability logbook daily. Credit card forms must be issued and used in numerical sequence.

(9) Service station managers must be aware of potential credit card fraud by station employees. A check should be made daily of credit card sales to determine if the same name and number appear more than once in the same day. This occurrence may be a sign of potential fraud. Credit cards must be returned to patrons after validation. In the event a credit card is left behind, that credit card will be locked securely in the station safe in a sealed envelope and the patron contacted as soon as possible.

(10) Trash must be inspected by service station managers or designee prior to removal to ascertain that saleable merchandise is not being disposed of. Cartons should be broken down and folded flat.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 10

REPORTING

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	10000	10-1
DEPARTMENT OF DEFENSE AA&E ANNUAL REPORT.	10001	10-10
OTHER AA&E REPORTING REQUIREMENTS	10002	10-10
LAW ENFORCEMENT AND PHYSICAL SECURITY ACTIVITIES REPORT.	10003	10-11

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 10

REPORTING

10000. GENERAL. The loss of government property due to inadequate accountability measures, negligence, and theft results in significant monetary loss and directly impacts on unit readiness. Efficient management of Marine Corps resources is a matter of high priority and requires effective loss prevention and physical security programs. Each person is charged with safeguarding government under their jurisdiction. Property issued to individuals does not become private property by act of issuance or possession, but remains public property which must always be safeguarded. Property losses frequently occur because regulations relating to proper safeguarding and handling are not followed.

10001. MISSING, LOST, STOLEN, AND RECOVERED (MLSR) REPORTING. The MLSR reporting system was designed to enable the USMC to centrally track material losses and to identify trends and areas where security enhancements may be required.

1. Unit commanders and military police agencies should promptly receive all pertinent information concerning losses of government property. Physical security deficiencies, and operating practices which contributed to such losses need to be investigated and corrective action taken.
2. MLSR reporting assists the provost marshal in determining the adequacy of command loss prevention and physical security program reporting requirements. 
3. MLSR reports do not waive the requirements for loss/gain reports prescribed by other Marine Corps directives, nor for causative research and vouchering requirements prescribed by reference (cc).
4. MLSR reports are required only if actual gains or losses may have occurred.
5. MLSR reports will be generated as soon as possible but not

later than 48 hours after the occurrence. Delayed reporting will include the reason for the delay (e.g., loss discovered during deployment, geographic separation of the responsible officer from the commanding officer for 5 days prevented prompt submission of the report). If causative research can, within a reasonable amount of time (15 days), prove that discrepancies are due to errors in records and not actual loss, then an MLSR report should not be submitted (unless to correct an earlier mistaken MLSR report).

6. A thorough investigation will be made of missing, lost, or stolen AA&E to determine the circumstances and to correct responsibilities as appropriate. Inventory and accountability losses must be investigated thoroughly. BEFORE ANY LOSS CAN BE ATTRIBUTED TO AN INVENTORY OR ACCOUNTABILITY DISCREPANCY, IT MUST BE DETERMINED THROUGH INVESTIGATION THAT THE LOSS WAS NOT THE RESULT OF THEFT OR MISAPPROPRIATION. Under no circumstances will investigative reports for AA&E identify "inventory" or "accounting" error as a probable cause for missing AA&E until a NCIS or command investigation so indicates. Note: MLSR reporting does not apply to privately-owned weapons.

7. MLSR Reportable Items. The following types of government property are reportable under the MLSR reporting program:

a. All AA&E and similar incendiary, or destructive devices regardless of value. Quantities which require an MLSR message report are set forth in Appendix J.

b. All Marine Corps Ground Equipment Resource Reporting (MCGERR) reportable equipment as published in the Marine Corps Bulletin (3000 series), regardless of dollar value.

c. Precious metals valued over \$100 and presentation or commemorative silver. Enclosure (1) contains a listing of reportable precious metals.

d. Losses of controlled substances (e.g., narcotics, barbituates, amphetamines, etc.) are not included under the MLSR program and shall be reported as prescribed in chapter 21 of reference (11). For losses aboard Marine Corps installations,

also submit a copy of Drug Enforcement Administration (DEA) Form 106 to the provost marshal.

e. Classified printed material losses are not included under the MLSR program and will be reported as prescribed in reference (b). Cryptographic items accountable within the COMSEC Material System are not included in the MLSR program except Controlled Cryptographic Items (CCI). Incidents involving MLSR CCI material will be reported within 48 hours.

8. MLSR Reporting Requirements

a. Navy activities holding Marine Corps Class V(W), and Marine Corps activities will submit reports of all MLSR to CMC (PS/LPC) with copies to the chain of command, NAVSURFWARCENDIV Crane (Code 4044), and MARCORSSYSCOM (AMMO) for ammo items. NAVSURFWARCENDIV Crane will promptly report loss, theft, or recovery of arms to the DoD Central Registry.

b. Marine Corps commands will promptly submit appropriate information relating to theft or suspected theft of AA&E to the local PMO or NCIS office for reserve commands not located aboard a Marine Corps Installations.

c. Commands must report all MLSR incidents involving the reportable items outlined in paragraph 10001 above. This report will be in the message format as prescribed in Appendix C. An example report is provided in Figure 10-1.

d. The reporting of MLSR incidents via message is independent of normal supply survey/adjustment procedures, command investigations, or requests to law enforcement agencies for investigative assistance. Commanders will initiate appropriate investigations per chapter 6 of reference (cc).

e. Recovered reportable items must be reported via message by all commands regardless of whether the command reported the property as missing, lost, or stolen.

9. Notification to Law Enforcement Activities. Timely notification of all reportable losses and recoveries, as well as losses which are not reportable under this directive will enable

10001 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

From:	CG MCB QUANTICO VA
Sent:	Wednesday, June 04, 2004 2:48 PM
To:	CMC WASHINGTON DC PPO PS (uc) CMC WASHINGTON DC LLPC (uc); CG MARCORSYSCOM AMMO (uc) NAVSURFWARCENDIV Crane (Code 4044)
Subject:	R 041718Z JUN 04 MLSR SENSITIVE MATERIAL REPORT (RCS MC #4340-1)
Importance:	Low

MSGID/GENADMIN//
SUBJ/MLSR SENSITIVE MATERIAL REPORT (RCS MC #4340-1)
(MIN: CONSIDERED)
MLSRP/MLSRP/USMC
ACC. M00264
RUC. M00213
RPT. 2004/06-INITIAL
AAA. VIRGINIA
BBB. A-04-06-04
CCC. 1. (1) ARMS (2) MISSING (3) M60 MACHINE GUN, 1 EA (4) SACO INC. (5)
765432 (6) 1005-00-726-5661 (7) MACHINE GUN M60E3 (8) \$6630.00 (9) 2 (10)
ARMORY, BLDG 3000
DDD. LIABILITY: (1) YES (2) YES (3) SGT (4) AWAITING RESULTS OF
INVESTIGATION
EEE. INVESTIGATION: (1) NCIS QUANTICO (2) 04-06-03 ASSUMED (3) CASE
OPENED
FFF. SUMMARY: (1) DURING ARMORY INVENTORY ON 01 JUN 04, ASSET COULD
NOT BE LOCATED. MACHINE GUN AND AMMUNITION WERE IN SEPARATE BOXES
BOUND TOGETHER WITH METAL STRAPS. ASSETS WERE NOT ON DAILY INVENTORY
LIST (2) 04-06-01 (3) SECURITY DEFICIENCY EXISTED SINCE ASSETS WERE NOT
LISTED ON DAILY INVENTORY LISTING (4) INVESTIGATION INITIATED (5) COMMAND
ARMORY INVENTORIES WILL BE CONDUCTED TWICE MONTHLY. ARMORY OFFICER
WILL SUPERVISE COMPILATION OF DAILY INVENTORY LIST AND CROSS REFERENCE
WITH CMR AND AMMO ACCOUNTING RECORDS.
GGG. POINT OF CONTACT: (1) CAPTAIN (2) BRYON J. DIDNTLOSEIT (3) DSN 278-
5678 (4) COMM (703) 784-9843 (5) DIDNTLOSEITBJ@QUANTICO.USMC.MIL

Figure 10-1. - Example MLSR Report

prompt action by military or civilian police. Law enforcement agencies not only investigate thefts, but check pawn shops, military surplus stores, and flea markets for stolen or diverted property, maintain criminal intelligence and loss prevention files, etc.

a. For thefts observed while in progress or immediately afterwards, telephonic reports will be made immediately to the military (or civilian) police with descriptions of suspects, vehicles, and property involved.

b. All commands having an installation provost marshal will immediately make telephonic notification to the provost marshal upon discovery of an MLSR reportable incident. This notification is independent of the MLSR reporting process and should not be construed as meeting the requirements described in paragraph 10001. The provost marshal will make further referral to the NCIS when appropriate, and coordinate with NCIS on reporting to local police.

(1) When NCIS declines to investigate missing AA&E, they will immediately notify the security officer or provost marshal of the accountable or host command, who will perform an investigation. The AA&E Accountability Officer will ensure all applicable documents and personnel are available. The security officer/provost marshal will:

(a) Investigate the circumstances surrounding the loss, including inventory and custody records, applicable security procedures and hardware, spaces where the AA&E was last seen, and applicable key control/access logs;

(b) Interview the individual specifically accountable for the lost AA&E, as well as those with recent access or security-related responsibilities in the area;

(c) Using the data from investigation, interviews, and records, determine the most likely cause of the loss; and

(d) Report findings in writing, with recommended corrective action, to the commanding officer. Corrective action may include disciplinary action, appropriate training of personnel or procedural changes in AA&E handling. The security officer's report must reflect the final disposition of investigative action, including recoveries and disciplinary action, as appropriate.

2) All command investigation reports will be maintained for 3 years.

10001 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

c. Commands not aboard Marine Corps installations will refer MLSR incidents to the nearest NCIS office for investigation or further referral to outside agencies.

10. Notification to DoD, Director of Security. CMC(PS) will notify DoD (Director of Security, OASD(C3I) DASD(S&IO)) not later than 72 hours after occurrence or discovery. Losses of the following will be considered significant and will be reported:

- a. One or more Category I or II missiles or rockets;
- b. One or more machine guns;
- c. One or more automatic fire weapons;
- d. 25 or more manually operated or semi-automatic weapons;
- e. Over 5000 rounds of ammunition smaller than 40mm;
- f. 20,000 rounds or more of .38 caliber ammunition;
- g. Five rounds or more of 40mm and larger ammunition;
- h. Any fragmentation, concussion, or high explosive grenades;
- i. One or more mines (antipersonnel and antitank);
- j. Ten pounds or more of demolition explosives including detonation cord, blocks/sticks of explosives (C-4, dynamite, etc.);
- k. Armed robberies or attempted armed robberies of AA&E facilities;
- l. Forced entries or attempted forced entries into AA&E facilities;
- m. Evidence of terrorist involvement in the theft of AA&E;
- n. Incidents involving AA&E that cause significant media coverage, or appear to have the potential to cause such

coverage; and

o. Evidence of trafficking or bartering involving AA&E, illegal drugs, etc., regardless of the quantity of AA&E involved.

11. Responsibilities

a. CMC(PS) will review all MLSR message reports involving AA&E and other sensitive government property losses for physical security deficiencies. When required, CMC(PS) will assist commands to correct problems which necessitated the MLSR submission. The CMC(PS) will maintain statistics on MLSR reporting of theft, report all related information to concerned Department of Defense (DoD) activities. CMC(PS/LPC) will conduct a joint annual trend analysis to determine whether losses result from criminal acts.

b. CMC(LPC) will review all MLSR message reports involving AA&E. CMC(LPC) will maintain statistics on MLSR reporting losses and recoveries and when required, to conduct trend analysis of government property losses to identify trends and areas where property management procedures might be enhanced.

c. The Commanding General, Marine Corps Logistics Base, Albany, Georgia will maintain the Quarterly Automated Reporting System (QARS) including system design specifications, documentation and data requirements changes. The functional sponsor for QARS is CMC(LPC).

(1) QARS is an automated system which extracts gain/loss adjustment transactions from automated formal property management and stock record balances. As a central repository of gain/loss statistics for the Marine Corps, QARS contains the information needed to conduct detailed analysis of non-sensitive item losses.

(2) The QARS specifically excludes ammunition inventory adjustments processed separately by MARCORSYSCOM(PM-AMMO). Ammunition inventory record adjustments will be accumulated separately and retained for 3 years by MARCORSYSCOM.

d. All statistics will be generated using a database or

10002 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

similar type system capable of conducting queries on any of the information entered into the database system.

(1) Statistical databases or similar type systems will maintain information for 10 years.

(2) Statistical databases or similar type systems will contain, at a minimum, the information in paragraphs ACC through DDD, and paragraph GGG of the standard MLSR Report, see Figure 10-1 for familiarization with the requirement.

10002. DEPARTMENT OF DEFENSE (DOD) AA&E ANNUAL REPORT. The DoD Components shall provide the Director of Security, OASD(C3I), DASD(S&IO) a written annual (calendar year) analysis of AA&E thefts and losses as well as actions taken to reduce such incidents. The analysis shall reflect and compare the previous year's losses and thefts with the latest reporting year analysis. Such analyses shall be submitted to the Director, Security Programs not later than 30 January. The DoD Components shall present their analyses annually at the DoD Physical Security Review Board meeting.

10003. OTHER AA&E REPORTING REQUIREMENTS

1. CID when notified of a theft, loss, or recovery of DoD AA&E will work with NCIS to ensure prompt reporting of required information to the National Crime Information Center (NCIC) upon discovery of such incidents.

2. CID will work with NCIS on submitting reports within 72 hours to the Bureau of Alcohol, Tobacco and Firearms (ATF), Intelligence Division, BATF Headquarters, Department of the Treasury, Washington, DC 20226 of all confirmed thefts and losses of AA&E as described in paragraph 10002. BATF shall also be advised of the recovery of previously reported AA&E thefts and losses. Appendix K provides an example of the ATF Form 3270.19, "Munitions Loss Worksheet," that is to be used when reporting such information.

10004. LAW ENFORCEMENT AND PHYSICAL SECURITY ACTIVITIES REPORT (LEPSAR). Marine Corps commands with an installation provost marshal will submit Law Enforcement and Physical Security Activities reports to CMC(PS) as follows (Report Control Symbol DD-1630-02 has been assigned to this report):

1. Installation Crime Statistics for the period of 1 January to 31 December of any given calendar year will be submitted not later than 30 January of the following calendar year. This report will be cumulative in nature.
2. Installation provost marshals will maintain quarterly statistics to be available to the CMC(PS) upon request. All criminal offenses brought to the attention of Marine Corps commands aboard Marine Corps installations will be reported to the installation provost marshal for appropriate action.
3. Installation annual crime statistics will be submitted using NAVMC 11197 (LEPSAR Report), see an example of the form in Appendix L, which is available in an electronic format or automatically generated via the Consolidated Law Enforcement Operations Center (CLEOC). Instructions on completing the NAVMC 11197, whether in the paper or electronic form, are further discussed within Appendix L. Blank, paper or electronic, copies of NAVMC 11197 should be requested from CMC(PS).
4. All LEPSAR Reports will be retained by CMC(PS) and the installation provost marshal for a period of 3 years after the date of submission, and thereafter destroyed.
5. CMC(PS) will compile all of the statistical data, submitted by the installations, and generate one annual report that encompasses all Marine Corps criminal activity. From this report CMC(PS) initiatives can be implemented that will assist installation commanders in reducing the crime.

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 11

PHYSICAL SECURITY IN THE OPERATING FORCES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	11000	11-3
RESPONSIBILITIES	11001	11-3
CHALLENGES	11002	11-4
AGGRESSOR OBJECTIVES AND TACTICS	11003	11-4
THREAT FACTORS.	11004	11-6
THREATS SOURCES	11005	11-6
LEVELS OF PROTECTION	11006	11-7
PROTECTIVE MEASURES	11007	11-7
SYSTEMS APPROACH	11008	11-8
PHYSICAL SECURITY SURVEYS	11009	11-9
PHYSICAL SECURITY ASSESSMENT.	11010	11-10
REFERENCES	11011	11-10

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 11

PHYSICAL SECURITY IN THE OPERATING FORCES

11000. GENERAL. Physical security is a vital tool for Commanders in garrison or an operational environment in support of Operating Forces (OPFORS). It must be included and integrated in all capabilities of operations in pursuit of a seamless connection between the strategic, tactical and operational levels of the OPFORS during combat operations and Military Operations Other Than War (MOOTW). A fundamental component of force protection, the program supplements the effort to protect Marines, sailors, civilian Marines, family members, and resources.

1. Commanders at all levels and environments have an inherent security requirement that includes: protecting personnel, equipment, and facilities; preventing or minimizing disruption of support operations; protecting lines of communications; preventing or minimizing disruption of command and control; defeating, containing, or neutralizing any rear area threats.

2. Physical security programs deny, delay, deter, and detect criminal and terrorist activity. Physical security employs physical and management protective measures designed to safeguard personnel, prevent unauthorized access to equipment, material, and documents, and safeguard against espionage, sabotage, damage, and theft. Application of these measures mitigates and in some cases, prevents threats.

11001. RESPONSIBILITIES. Physical Security personnel will deploy with the Military Police structure in support of the Marine Air Ground Task Force (MAGTF). Commanders at all levels must understand the role of Military Police (MP), to include physical security, in order to sustain tactical and combat operations. The following paragraphs identify roles and responsibilities as they apply to physical security support to the MAGTF Commander.

1. The MAGTF Commander may designate a MAGTF Provost Marshal as identified in reference (mm).

11003 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

2. MAGTF Provost Marshals provide MAGTF Commanders with MP employment subject matter expertise, and coordinate all MP activity to ensure the proper allocation of resources. Provost Marshals will coordinate all security responsibilities with the Area Operations Center (AOC), the MAGTF Antiterrorism/Force Protection (AT/FP) Officer, and supporting security elements, including Host Nation (HN) personnel. Additional doctrinal guidance is contained in reference (mm).

3. Physical Security personnel, under the purview of the MAGTF Provost Marshal, assess threats based on supported credible intelligence, identify Physical Security and MEVAs, vulnerabilities, and recommend the employment of protective measures. These actions are intended to mitigate the threat to vulnerable assets/areas.

11002. CHALLENGES. There are ranges of challenges in providing a sound physical security posture during strategic, tactical, and combat operations. The challenges include traditional and non-traditional threats, tactics employed by terrorists, criminals, and natural and man-made disasters. Commanders may minimize the challenges through proactive measures, security procedures, random changes to the area, and the site security posture.

11003. AGGRESSOR OBJECTIVES AND TACTICS. Aggressor's objectives include:

1. Inflicting injury or death, destroying and/or damaging facilities, property, equipment, and resources, stealing equipment, materiel and information, and creating public adversity. These objectives are completed with tactics, tools, and weapons, which are the basis for threats to Marines and the mission. Although terrorist and aggressor tactics present an asymmetrical threat, there are a number of tactics that are common and commanders must plan and protect against:

- a. Bombings.
- b. Assassination.

c. Armed Raids or Attacks by groups employing use of small arms or stand off weapons.

d. Sniper attacks.

e. Improvised Explosive Devices.

f. Hostage taking.

h. Kidnapping.

i. Hijacking.

j. Skyjacking.

k. Arson.

l. Sabotage or subversive tactics.

m. Homicide or Suicide Bombers.

n. Standoff Weapons.

o. Forced/Covert Entry.

p. Insider Compromise.

q. Visual Surveillance.

r. Mail-bomb delivery.

s. Supply bomb delivery.

t. Airborne Contamination.

u. Waterborne Contamination.

2. The above tactics present threats to personnel and facilities. There are designs that provide levels of protection through the use of a systems approach that may mitigate the threat(s). There are a number of additional tactics that commanders must be aware of (including kidnappings,

11004 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

assassinations, and hijackings) that occur away from fixed, high population facilities. Commanders must ensure that all personnel have been fully briefed in regards to Individual Protective Measures (IPM), and suspicious activity reporting as required by reference (gg).

3. One proven terrorist method of attack is use of a Vehicle Borne Improvised Explosive Device (VBIED). This is a vehicle laden with explosives that is both employed with explosives set to detonate at a specific time and left unattended or driven by a homicide bomber.

a. VBIED's are normally employed next to a facility or driven through the facilities Vehicle Entry Control Point (VECP), to breach the facilities perimeter to attack a high value target with the intent of causing high casualty yield and maximum sustained damage to the facility.

b. A more common terrorist tactic is the use of two vehicles one as an assault vehicle to breach the facility perimeter, while the other vehicle attacks an objective within the perimeter.

4. Terrorists have employed the use of Boat Borne Improvised Explosive Device (BBIED), as seen in the attack on the USS Cole 13 Oct 2000 in Yemen.

11004. THREAT FACTORS. The following threat factors also need to be considered by commanders when planning for Physical Security:

- a. Operational capability.
- b. Intentions.

Activity.

- d. Operating environment.

11005. THREAT SOURCES. Security threats are acts and/or conditions that may result in the compromise of sensitive information; loss of life; damage, loss, and destruction of

property; or disruption to the mission. Physical security personnel, CID, AT/FP Officers, intelligence, and NCIS personnel all provide information and services relevant to the MAGTF Commander establishing threat levels and FPCONs. In an effort to counteract the threats, commanders must use the information provided to determine levels of protection.

11006. LEVELS OF PROTECTION. The level of protection, per reference (i) is the degree to which the protective system(s) will protect the asset against applicable threats. The higher the level of protection, the lower the risk of asset compromise from an attack. Levels of protection are defined as:

- a. Low. The protected facility or space will sustain a high degree of damage but should not collapse.
- b. Medium. The protected facility or space will sustain a significant degree of damage, but the structure will be reusable.
- c. High. The protected facility or space will sustain only superficial damage.

11007. PROTECTIVE MEASURES. Commanders have assets and personnel, such as Military Working Dogs (MWD), EOD, and Engineers that provide specific resources that have a significant role in the security posture. Commanders must engage these organizations for their specific training and resourcefulness, as well as the ability to improvise to counter threats. Protective measures are also based on a systematic process resulting in an integrated system. The system focus is intended to identify specific assets against perceivable threats, that is organized in depth, and contains mutually supporting elements. These elements and procedures prevent gaps or overlaps in responsibilities and performance. Protective measures can be divided into five elements; site-work; building; detection; notification; and procedures.

1. Site-work elements include the area surrounding a facility or asset, and are associated with exterior points of the building. Site elements include perimeter barriers, standoff distances, and landforms, both natural and man-made.

11007 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

2. Building elements are directly associated with the facility structure (including walls, doors, roof/ceiling, and windows).
3. Detection elements are used to detect or assess intrusion into a facility. Detection elements include ESS, Closed Circuit Television (CCTV), and metal detectors.
4. Notification elements are used to alert personnel in the vicinity of a facility during emergency situations.
5. Procedural elements are measures required by Department of Defense (DoD), Naval, and Marine Corps orders. Included are post orders, standard operating procedures, etc.
6. Effective systems integrate development procedures, and supporting elements.
 - a. Development procedures include:
 - (1) Available resources.
 - (2) Assets to be protected.
 - (3) Threat(s) to the assets.
 - (4) Applicable risk levels.
 - (5) Applicable regulatory requirements.
 - (6) Applicable level of protection for the assets against the threat.
 - (7) Additional asset vulnerabilities, based on the threat.
 - b. Supporting elements include:
 - (1) Physical measures; barriers, lighting, and electronic security systems (ESS).
 - (2) Procedural measures; Standard operating procedures, including facility/asset requirements along with those of guards, that address pre-indent and post incident procedures.

(3) Terrorism counteraction measures.

11008. SYSTEMS APPROACH

1. In order to meet functional requirements of security systems, several components need to be identified, including the following:

- a. Entry and circulation control.
- b. Barrier systems.
- c. Access delay and denial systems.
- d. Notification Systems.
- e. Dedicated security forces.
- f. Designated immediate response forces.

2. Combining these components into an integrated protection system can achieve appropriate levels of protection for resources. Use of the systems approach to the evaluation and design of systems allows a commander to make tradeoffs among physical security measures. Where threats are infrequent and the level of physical security threat small (such as small arms or hand tool), the ability to increase the size of the guard force, vacate particularly vulnerable locations or buildings for a brief period, and change day-to-day operations may be a far more cost-effective solution to a physical security problem than a time consuming major project.

11009. SURVEYS. Surveys are utilized to identify violations of regulatory instructions and vulnerabilities to threats. Physical security personnel will conduct physical security surveys on the following areas:

1. Arms, ammunition and explosive sites, to include field ammunition supply points and other expeditionary support sites.
2. Flight lines, expeditionary airfields, and other aviation assets in support of the aviation combat element.

11011 MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

3. Naval assets including piers, wharfs, port facilities, and waterfront areas used in logistics support, including preposition areas.
4. Petroleum, oil, and lubricant facilities such as fuel depots and issue points.
5. Command, control, communications, computers, and information facilities.
6. Entry Control Points.
7. Critical infrastructure.
8. Officer and enlisted quarters.
9. Motor pools.

11010. PHYSICAL SECURITY ASSESSMENT. Physical security assessments will be utilized in support of operating forces, and included in the Force Antiterrorism Plan. Physical security assessments are similar in nature to a installation physical security plan, but are designed to support the MAGTF Commander with a brief, concise, and adaptable document.

1. Physical Security Specialist will provide and physical security assessment upon establishment of an expeditionary base camp. Physical security assessments will encompass a threat assessment (normally obtained from NCIS or other intelligence activities), vulnerability assessment, and a risk assessment.
2. These elements are commensurate for the Commander to consider during Physical Security planning.

11011. REFERENCES. There are a number of references Physical Security personnel must be familiar with in order to correlate physical security, antiterrorism, and operational requirements. Reference (nn) through (pp).

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX A

DEFINITIONS

For the purpose of this manual, the following definitions apply:

a. Administrative Vehicle Inspection. A cursory inspection of the contents of a vehicle with full consent of the operator or owner. Administrative inspections are conducted with prior written authorization and direction by the installation or activity commanding officer as to the methods and procedures to be employed.

► b. Airborne Contamination. Contamination of a facility air system by introducing chemical, biological, or radiological agents into the Heating Ventilation Air Conditioning (HVAC) system.

c. Antiterrorism. Defensive measures used by the United States Marine Corps to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

d. Armed Guard. A person equipped with a firearm and ammunition whose primary function is to protect property and who has received training in accordance with reference (l) and qualified with the firearm in accordance with reference (m).

e. Auxiliary Security Force (ASF). A local, non-deploying military asset derived from host and tenant commands. The ASF is used to augment the installation Provost Marshal Office (PMO) during increased threat conditions. The auxiliary security force may fall under the control of the Provost Marshal or an officer designated by the Commanding Officer.

► f. Ballistics. An attack using various small arms (pistols, submachine guns, shotguns, rifles) from a distance, with a goal of firing numerous rounds to injure or kill occupants and damage facilities, assets, and positions.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- ▶ g. Code "Q" Items. Drugs or other controlled substances designated as Schedule III, IV or V items, per 21 Code of Federal Regulations, Part 1308.
- h. Code "R" Items. Precious metals and drugs or other controlled substances designated as Schedule I or II items per 21 Code of Federal Regulations, Part 1308.
- i. Commanding Officer. The term commanding officer used throughout this Manual refers to, yet is not limited to, installation commanding generals and commanding officers, organization officers and officers in charge.
- j. Counter-terrorism. Offensive measures taken to prevent, deter, and respond to terrorism.
- ▶ k. Covert Entry. Entry into a facility using stealth or false credentials.
- ▶ l. Critical. Those facility or infrastructures that have been designated as crucial to mission accomplishment and essential to the continuity of installation operations.
- ▶ m. Egress. Location in a perimeter, boundary, barrier, or designated restricted area that lends itself to an exit point from which the asset being protected, can be gained.
- n. Espionage. Acts directed toward the acquisition of information through clandestine operations.
- o. Exception. A written, approved long-term (36 months or longer) or permanent deviation from a specific provision of this manual.
- ▶ p. Exterior Attack. An attack against a facility, asset, or position at close range.
- ▶ q. Forced Entry. Entry into a facility using hand, power, or thermal tools to create a man passable opening or operate a device within the interior.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

r. Force Protection. Security programs designed to protect Service members, civilian employees, family members, facilities, and equipment in all locations and situations, accomplished through the planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

s. High-Risk Billet. Personnel billet external to the Marine Corps (such as UN observer, counterintelligence, or similar duties) that exists in a designated country. This billet may make personnel filling it an especially attractive or accessible terrorist target.

t. High-Risk Personnel. U.S. personnel and their family members whose assignment or symbolic value may make them especially attractive or accessible terrorists target.

u. High-Risk Target. U.S. material resources and facilities, because of mission sensitivity, ease of access, isolation, and symbolic value, may be especially attractive accessible terrorist targets.

▶ v. Homicide/Suicide Bombers. **Persons that carry and/or wear explosives on their body and self detonate the explosives.**

▶ w. Ingress. **Location in a perimeter, boundary, barrier, or designated restricted area that lends itself to an entry point from which the asset being protected, can be gained.**

x. Inhabited building. Buildings or portions of buildings routinely occupied by five or more DoD personnel and with a population density of greater than one person per 40 gross square meters (430 gross square feet). This density generally excludes industrial, maintenance, and storage facilities, except for more densely populated portions of those buildings such as administrative areas. The inhabited building designation also applies to expeditionary and temporary structures with similar population densities. In a building that meets the criterion of having five or more personnel, with portions that do not have

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

sufficient population densities to qualify as inhabited buildings, those portions that have sufficient population densities will be considered inhabited buildings while the remainder of the building may be considered uninhabited, subject to provisions of these standards. An example would be a hangar with an administrative area within it. The administrative area would be treated as an inhabited building while the remainder of the hangar could be treated as uninhabited.

y. Insider Compromise. Persons authorized access, compromise, or attempt to compromise, a facility or asset by taking advantage of their access.

z. Loss Prevention. Part of an overall command security program dealing with resources, measures and tactics devoted to care and protection of property on an installation. It includes identifying and reporting missing, lost, stolen, or recovered (MLSR) government property. Loss prevention requires developing trend analyses to plan and implement reactive and pro-active loss prevention measures.

- ▶ aa. Mail-bomb delivery. Bombs or incendiary devices placed in letters packages, or parcels and delivered through the mail postal system.
- ▶ bb. Moving Vehicle Bomb. An explosive laden vehicle driven directly into a facility and detonated by remote control or time delay.
- ▶ cc. National Defense Area (NDA). An area temporarily established on non-Federal lands located within the United States, U.S. possessions, or U.S. territories which places such non-Federal lands under the effective control of the DoD. The establishment results only from an emergency event.

dd. Physical Security. That part of security concerned with physical measures designed to safeguard personnel, prevent unauthorized access to equipment, facilities, material, computer media, and documents.

ee. Physical Security Program. Part of the overall security posture at an activity including policy and resources

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

committed to safeguard personnel, protect property, and prevent losses. Physical security is further concerned with means and measures designed to achieve force protection and anti-terrorism readiness.

ff. Physical Security Inspection. An examination of the physical security programs of an organization to determine compliance with physical security policy. Physical security inspections are normally conducted by the Inspector General of the Marine Corps (IGMC) or as part of the command inspection program and should not be confused with annual physical security **assessment surveys** as discussed below. Commanding officers will establish local physical security inspection programs for their subordinate commands.

gg. Physical Security Survey. A specific on-site examination of any facility or activity conducted by a trained physical security specialist (MOS 5814) to identify security weaknesses and recommend corrective measures.

▶ hh. Precious Metals. Refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium in bar, ingot, granule, liquid, sponge or wire form.

▶ ii. Primary gathering building. Inhabited buildings routinely occupied by 50 or more DoD personnel and family housing with 13 or more family units per building. This designation applies to the entire portion of a building that meets the population density requirements for an inhabited building. For example, an inhabited building that has an area within it with 50 or more personnel is a primary gathering building in its entirety. The primary gathering building designation also applies to expeditionary and temporary structures with similar population densities.

jj. Sabotage. An act or acts with intent to injure, interfere with, or obstruct the national defense of a country 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. For crimes of sabotage see Title 18, United States Code, Sections 2151-2157.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- ▶ **kk. Selected Sensitive Inventory Items.** Those items security coded "Q" or "R" in the Defense Integrated Data System (DIDS) that are controlled substances, drug abuse items or precious metals.

ll. Special Reaction Team. An element of the PMO organized, trained and equipped to provide rapid armed response to critical incidents beyond the normal capability of the military police.
- ▶ **mm. Standoff Weapons.** An attack where military weapons or improvised military weapons are fired against a facility, asset, or position from long range.
- ▶ **nn. Stationary Vehicle Bomb.** A vehicle covertly parked near a facility and detonated by remote control or time delay.
- ▶ **oo. Supply bomb delivery.** Bombs or incendiary devices concealed in various containers and delivered to supply and material handling points.

pp. Terrorism. The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

qq. Visual Surveillance. Using ocular and photographic devices (binoculars, cameras) to monitor operations in or around facilities, assets, or positions.

rr. Waiver. A written temporary relief, normally for a period of one year, from specific standards imposed by
- ▶ **ss. Waterborne Contamination.** Contamination of a facility water system by introducing chemical, biological, Toxic Industrial Chemicals (TIC) or radiological agents into the water system internal or external to a facility.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX B

****CLASSIFICATION****

PHYSICAL SECURITY PLAN

Activity:

Date:

1. Purpose. State the purpose of the plan.
2. General. Mission and size of the installation, average population of Marines and family members, overall daily population including civilian personnel.
3. Area Security. Identify overall size of the installation, to include inhabited and uninhabited areas. Identify restricted and non-restricted areas, buildings, and other structures considered critical. Provide requirements for resource protection and established priorities for their protection.
4. Control Measures. Detail established restrictions on ingress/egress into critical areas (e.g., guards, badge systems, etc.) in accordance with applicable orders.
 - a. Access Control
 - (1) Installation access control requirements.
 - (a) Individual
 - 1) Military personnel.
 - 2) Family members.
 - 3) Civilian Employees.
 - 4) Maintenance personnel
 - 5) Contractor personnel.
 - 6) Vendors.

****CLASSIFICATION****

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

****CLASSIFICATION****

(b) Vehicle. (Registration, including state and/or host country. Policy on administrative inspection of military and privately owned vehicles.

(2) Restricted and non-restricted areas.

(a) Restricted area access requirements for individuals:

1) Military personnel.

2) Family members.

3) Civilians.

4) Maintenance.

5) Contractors.

6) Vendors.

(b) Restricted area access requirements for vehicles:

1) Military and government owned vehicles.

2) Privately owned vehicles.

3) Emergency vehicles.

4) Taxis, buses, etc.

b. Material Control

(1) Inbound

(a) Requirements for admission of material and supplies.

****CLASSIFICATION****

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

****CLASSIFICATION****

- (b) Search and inspection of material for possible sabotage/terrorist hazards.
- (c) Special controls on delivery of supplies and/or personnel shipments in restricted areas.
- (d) Established controlled holding areas and safe havens for classified, AA&E, and hazardous material.

(2) Outbound

- (a) Required documentation.
- (b) Transfer areas for controlled, classified, AA&E, and hazardous material.

5. Aids to security

a. Protective barriers

- (1) Natural.
- (2) General.
 - (a) Fencing.
 - 1) Clear zone requirements.
 - 2) Maintenance.
 - 3) Perimeter ingress/egress points (gates).
 - 4) Gatehouses. (Location, hours of operation, construction)
- (3) Specific barriers.

****CLASSIFICATION****

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

****CLASSIFICATION****

(a) Stationary

- 1) Type.
- 2) Current placement.
- 3) Maintenance requirements.

(b) Mobile

- 1) Type.
- 2) Current placement and/or staging area.
- 3) Deployment schedule.
- 4) Support requirements for deployment.
- 5) Maintenance requirements.

b. Protective Lighting

- (a) Placement.
- (b) Maintenance.
- (c) Power failure contingency plan.
- (d) Uninterrupted Power Sources.
- (e) Emergency Lighting systems.
 - 1) Stationary.
 - 2) Mobile.
 - a) Staging Area.
 - b) Maintenance requirements.

****CLASSIFICATION****

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

****CLASSIFICATION****

c) Deployment schedule.

d) Support requirements for deployment.

c. Electronic Security Systems

(1) Alarm Control Center.

(2) Use and monitoring.

(3) Alarm response policy.

(4) Alarm response drills.

(5) Training requirements.

(6) Component testing requirements.

(7) Component testing schedule.

(8) Maintenance responsibilities.

(9) Power failure contingency plan.

(10) Uninterrupted power sources.

6. Security Forces

a. Table of organization.

b. Tour of duty.

c. Posts.

(1) Stationary.

(2) Mobile.

d. Available resources (e.g., SRT, MWD, CID, Auxiliary.)

****CLASSIFICATION****

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

****CLASSIFICATION****

e. Equipment.

(1) Weapons.

(a) Training.

(b) Qualification requirements.

(2) Vehicles.

(3) Support Equipment (hand irons, flashlight.)

f. Communications.

(1) Monitoring location.

(2) Authorized users.

(3) Authorized frequencies.

(4) Shared frequencies.

(5) Mobile Assets (vehicle & portable.)

(6) Location of support equipment (repeaters, etc.)

****CLASSIFICATION****

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX C

MLSR PREPARATION GUIDE

1. Reporting Procedures

a. An INITIAL report will be submitted as soon as a loss or recovery of a sensitive item is discovered, not to exceed 48 hours. The fact can be established by discovery of an incident, receipt of a loss claim, completion of an inventory, or by any other means. A FINAL report will not be submitted until completion of all appropriate financial, administrative, investigative, survey, and disciplinary action. A SUPPLEMENTAL report may be submitted to provide any additional pertinent information whenever a FINAL report has previously been submitted.

b. FINAL and SUPPLEMENTAL reports must reference the INITIAL and any other associated reports submitted on the same incident by report number, date time group (DTG), or correspondence identification.

c. Whenever AA&E items have been reported, and are subsequently recovered by the reporting command, an appropriate FINAL or SUPPLEMENTAL report must be submitted including circumstances of recovery.

d. Commands in receipt of recovered government property item(s) (from sources other than through official supply or procurement channels) for which they were not previously responsible, must submit an INITIAL/FINAL report so the recovered items may be checked against the NCIC and accountability data bases for correlation to any prior MLSR reports submitted by other commands. If property item(s) recovered is identified as belonging to another service, the MLSR report should be submitted to the service owning the property rather than the reporting organization's headquarters. Initial/final MLSR reports will only be submitted for the purposes as outlined above.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

2. Reporting Format

a. Initial FINAL and SUPPLEMENTAL Marine Corps MLSR sensitive material reports are to be submitted in the following format:

FM: (Reporting Command)
TO: CMC WASHINGTON DC PPO PS (uc)
CMC WASHINGTON DC L LPC (uc)
CG MARCORSYSCOM AMMO (uc)
NAVSURFWARCENDIV CRANE IN (uc)
CC: (Chain of Command to include responsible command having custody at the time of loss or recovery)
INSTALLATION MILITARY POLICY AGENCY

b. Subject line of all organization's reports will be:

MLSR SENSITIVE MATERIAL REPORT (RCS MC #4340-1) (MIN: CONSIDERED)

c. Only prior MLSR property reports on the same incident will be referenced. References should be indicated by the DTG or correspondence identification on the prior report(s) and by the "incident report number."

d. The first line of text after references (if any) must be:

MLSRP/MLSRP/USMC

e. ACC. The Unit Identification Code (UIC) and name of the activity. The ACC/UIC should be identical to that used by the accountable command for MILSTRIP and MILSTRAP purposes. The ACC/UIC must be indicated on every report.

f. RUC. The Reporting Unit Code and name of the actual using nit responsible for accounting for the reportable item.

Incident Report Number (RPT). Consists of the Incident report Number assigned by the reporting command and the Incident Report Status. Year and number separated by a diagonal slash. umber and status separated by a hyphen. The RPT must be indicated on every report. Each incident may involve one or more property

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

items. Incident reports will be numbered consecutively by each reporting activity for each year. Examples: 1994/03-INITIAL, 994/03-FINAL, 1994/03-SUPPLEMENTAL.

AAA - Location of the Incident. Indicate only the name of the State/territory if incident occurred in one of the 50 United States and its Territories. Indicate only the name of the foreign country if the incident occurred there. Indicate the name of the ocean area if the incident occurred there.

BBB - Date of Incident. (Mandatory). Use the actual date of theft, loss, disappearance, recovery, if known; otherwise use the date the item(s) was last seen or inventoried. Indicate, with an "A" or "L", whether the date is actual or last. Denote the date in year-month-day order. "A-94-06-25" for an actual date of 25 June 1994, or "L-94-01-08" for a last inventory or last sighted date of 8 January 1994.

Block CCC - Material Description. List each type separately and indicate whether the material is arms, ammunition, explosives, MARES reportable (other than arms), precious metals, or classified equipment.

(1) Specify ARMS, AMMUNITION, EXPLOSIVES, MARES REPORTABLE OTA, PRECIOUS METALS, or CLASSIFIED EQUIPMENT.

(2) Indicate whether the material is MISSING, LOST, STOLEN, or RECOVERED.

(3) Indicate the type of material and quantity. Examples: Rifle (1) air to air missile (3), radio (1), hand grenade (2).

(4) Indicate the make or manufacturer.

(5) Indicate the manufacturer's serial number or lot number.

(6) Indicate the National Stock Number (NSN).

(7) Indicate the full name/description of the item.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

Example - AN/PCS-3, Manpack Satellite comm terminal, M249, Squad Automatic Weapon.

(8) Indicate the actual or estimated replacement value of the item(s)

(9) Indicate the security risk category listed in the Marine Corps Stocklist (AA&E only).

(10) Indicate the last (first for recoveries) known location.

k. DDD - Liability. Has individual liability been established:

(1) Answer "Yes" or "No".

(2) Indicate whether there was disregard of established policies, neglect, or dereliction of duty on the part of responsible individual(s).

(3) Identification of Liable Personnel. (Use ranks of military personnel and grades of civilian personnel, if applicable. DO NOT REPORT NAMES.)

(4) Disciplinary/administrative action taken (e.g., referred to courts-martial; NJP; process for discharge; warning; suspension; letter of reprimand; etc.) state whether Military Justice or Civil Service procedures. If negligence, disregard of established policies or dereliction of duty is indicated in paragraph 2k(2), preceding, the liable person is described in paragraphs 2k(3), preceding, and no formal disciplinary, administrative, or punitive action is taken, a full explanation must be provided concerning the reasons for not taking action.

l. EEE - Investigation (Mandatory). All sensitive material losses shall be reported to the security officer/provost marshal. Where no security officer/provost marshal exists at an activity, the nearest supporting NCIS field component shall be notified.

(1) Identify NCIS or security officer/provost marshal concerned.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

(2) Date incident referred to NCIS or security officer/provost marshal, and indicate assumed or declined.

(3) Preliminary action taken by NCIS or security officer/provost marshal, if known.

(4) If the incident is not referred outside the command, indicate actions taken by the command and a status report (e.g., investigating officer appointed and investigation ongoing).

m. FFF - Summary. Comments concerning available details about the incident to include:

(1) Detail circumstances of loss (e.g., forcible/surreptitious entry to storage area; robbery/assault of personnel; etc.). (Detail any security devices/measures/procedures breached.)

(2) Date of last command inspection/inventory.

(3) Narrative comments concerning any real or perceived security deficiencies derived from incident analysis, trends analyses, or resulting physical security/crime prevention surveys.

(4) Status of investigation (e.g., initiated/continuing/closed; suspects identified/not identified, etc.)

(5) Specific security measures taken as result of the incident (e.g., increased sentries; changed locks/combination; etc.). (Stock phrases such as "improved administrative procedures," "improved recordkeeping," etc., will not be used.)

n. GGG - Point of Contact. Individual, who can provide detail information about the incident, information to include:

(1) Rank

(2) First and middle initial, and last name

(3) DSN Phone Number

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

(4) Commercial Phone Number

(5) E-Mail address

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX D

**INSTRUCTIONS FOR PREPARATION AND
DISTRIBUTION OF PHYSICAL SECURITY SURVEY**

1. **GENERAL.** The following instructions are intended to provide guidance for the uniform preparation and distribution of physical security surveys.

2. **BLOCK PREPARATION INSTRUCTIONS.** Each block appearing in the United States Marine Corps Physical Security/Crime Prevention Survey (NAVMC 11121), identifies, controls and records each survey and therefore will be filled in completely. A NAVMC 11121 example is located on page D-7. The blocks listed below identify required information. Provided examples are not all inclusive.

Block 1 - Date. This block is completed on the date of final typing and should be entered as follows: day, month and year.

Block 2 - Status. Completed.

Block 3 - Survey Control Number. This block contains the control date of the survey, identification of the organization (Monitored Command Code (MCC)) conducting the survey, survey number, and project code identifier (Physical Security (PS), Crime Prevention (CP), Marine Activity (MA), Navy Activity (NA), etc.). (Example: 3AUG00-008-0001-PSMA)

Block 4 - Inspecting Unit. The provost marshal's office preparing the physical security/crime prevention survey. (Example: Provost Marshal Office, Marine Corps Base Quantico, VA.)

Block 5 - Requesting Unit. This block contains the title of the commanding officer of the organization requesting the survey. (Example: Commanding Officer, Headquarters and Service Battalion, Marine Corps Base, Quantico, VA.)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

Block 6 - Organization and Address of Unit Inspected/Surveyed. Organization, activity or area to be surveyed;
(Example: H&S Battalion Armory, Bldg 2171, MCB Quantico, VA.)

Block 7 - Distribution. An original and one copy will be typed and disseminated as follows:

- a. Original - Commanding Officer of activity surveyed.
- b. File - Local installation provost marshal office.

Block 8 - Type of Survey. Surveys will be titled "Physical Security."

Block 9 - References. List all references.

Block 10 - Basis for Survey.

(Example: As set forth in references (a) and (b), the provost marshal directed that a physical security survey be conducted (date, building, unit/activity, and base/station.) Contact was made with (grade, name, and title) and a survey was initiated.)

Block 11 - Synopsis of Survey. This is a summation of deficiencies identified during the survey and will serve as the basis for prioritizing corrective action should be accomplished. This block may also be used to provide recommended actions. (Example: The following deficiencies were identified during the course of the survey and require corrective action:

Block 12 - Data Affecting the Survey Site. This includes a canvass of local provost marshal office crime analysis records affecting the survey site and surrounding area. (Example: The following crimes have been reported in the vicinity of Bldg. 25 during the previous 12 month period: (3) Larceny of Private Property.)

Block 13 - Building and Area. Identify the building by number and type of construction (stories and type of material) and location (describe surrounding area, industrial, business,

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

residential, barracks, etc., and location in relation to the installation). (Example: Building 2111 is a three-story building constructed of brick veneer. The building is located in a business section in the southwest area of the installation.)

Block 14 - Physical Security Barriers. Address each category separately and fully.

1. Walls - Describe material, type of construction, and any deficiencies. (Example: Exterior walls for the facility are constructed of eight-inch mortar reinforced brick. Interior walls are constructed of plaster mounted on metal studs.)
2. Doors - Describe number, material, type of construction, and any deficiencies. (Example: There are five doors in the exterior walls of this facility. The main entrance exit door is constructed of 1-3/4 inch hollow metal secured to the walls in a metal frame, hinge pins are located on the interior of the door. (describe locking devices in Block 15, section d)).
3. Floor - Describe material, type of construction, and any deficiencies. (Example: The floor of this facility is constructed of an eight inch poured concrete pad.)
4. Ceiling/Roof - Describe material, type of construction, and any deficiencies. (Example: The ceiling of the facility is constructed of metal I beams with an exterior covering of tar and gravel.)
5. Windows/Other Openings - Describe number, material, type of construction, and any deficiencies. (Example: There are sixteen windows in the exterior walls of the facility. The windows are constructed of standard pane glass in wood frames, secured to the walls in metal frames (describe locking devices in Block 15, section d)).
6. Natural - Describe and indicate whether there are natural barriers.

Block 15 - Physical Security Aids, Equipment and Devices. These items provide protection in relationship to the

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

sensitivity of the property being protected. Address each category separately.

1. Lighting (Exterior/Interior) - Describe type, location (exterior location in relation to the facility), mount type, and any deficiencies. Include a night light survey. (Example: There is an incandescent light fixture located above the main entrance/exit door. There are exterior building mounted high pressure sodium fixtures located on the east and west walls.)
2. Fencing - Describe type, type of construction, number of personnel/vehicle gates in the fence line, and any deficiencies. (Example: There is a fence surrounding the facility. The fence is constructed of nine-gauge chain link and is seven feet high with an outrigger. There are four personnel and one vehicle gate within the fenceline.)
3. Locks - Describe type for windows and doors, and any deficiencies. (Example: The main entrance/exit door is secured with a mortise lock supported by a deadbolt assembly with a one-inch throw. Windows for the facility are secured with a crescent sash lock.)
4. Vaults/Safes/Containers - Describe to include number in the facility, make, type, weight, use, and any deficiencies. (Example: There is one safe in use in the facility. The safe is a Mosler brand five-drawer safe weighing approximately 750 pounds. The safe is utilized to store negotiable instruments).
5. Electronic Security System (ESS) - Describe type, interior components, where the system annunciates, and any deficiencies. (Example: There is an intrusion detection system in use in this facility. The interior system is comprised balanced magnetic switches and passive infrared motion detectors. There is also a duress switch utilized in the facility. The system annunciates at the Provost Marshal Office, which is staffed on a 24-hour basis.)
6. Key and Lock Control - Describe the program and any deficiencies. (Example: Key control has been established for this facility. All keys to the facility are signed out in a key control logbook that is maintained by the SNCOIC.)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

7. Security Force - Describe. (Example: There are no guards posted at this facility. Military Police provide a response to all alarms received from this facility. Military police have been provided training concerning the use of force in accordance with reference ().

Note: Provide adequate protection in relationship to the sensitivity of the property being protected.

Block 16 - Preventive Measures and Procedures. Address each category separately and provide recommendations accordingly.

1. Security Orders/SOP. Will include site specific security orders that address security in conjunction with MCO 5530.14, and any deficiencies. (Example: Reference () provides detailed information concerning security of disbursing currency and negotiable instruments).

2. Access control. Describe facility access control to include locally alarm fire doors, buzzer assemblies, and any deficiencies. (Example: Access to the facility is the responsibility of and controlled by personnel assigned to the facility. Two of the doors are provided additional protection by local "fire door" alarms that annunciate in the event the door is opened).

3. Property accountability. Includes inventories required by specific directives, installation CMR requirements, and any deficiencies. (Example: Inventories on all currency and negotiable instruments are conducted by disinterested personnel on a monthly basis. Plant property is inventoried on a semi-annual basis.)

4. Robbery/burglary procedures. Addresses installation crime prevention orders, local SOPs that identifies Robbery/Burglary Procedures, and any deficiencies. (Example: Robbery/Burglary procedures are outlined in references () and ().

5. Crime/Loss Prevention Awareness Training. Identify training provided by the command or by the Provost Marshal's

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

Office, and any deficiencies. (Example: Crime/Loss Prevention training is conducted on an annual basis in conjunction with the Provost Marshal Office Crime Prevention Office.)

Block 17 - Action/Comment. Example:

1. Questions concerning comments or recommendations contained in this report may be addressed to the Provost Marshal's Office Physical Security Section, extension 614-1414.
2. Action taken as a result of this survey will be forwarded to the installation Provost Marshal's Office, via the chain of command, within 90 days of receipt.

Block 18 - Typed Name and Grade of Inspector. Name of individual who conducted the survey should be entered as first and middle initials, last name and grade. (e.g., G.E. Davis, Sgt.)

Block 19 - Typed Name and Grade of Approving Officer. Name of officer approving the survey should be entered as first and middle initials, last name and grade; e.g., P.M. Grow, Capt.

3. IDENTIFIED DEFICIENCY REQUIREMENTS. For all deficiencies identified in a survey category, the requirement and the applicable reference should be listed. (Example: Requirement - The intrusion detection system has no emergency backup power. Reference (a), paragraph 0803 requires that all IDS be provided emergency backup power.)

4. RECOMMENDED CORRECTIVE ACTIONS. Physical Security Inspectors identify deficiencies and provide the requirement as directed by applicable orders. Unit Commanders are given the latitude to correct identified deficiencies as long as those corrective measures employed meet the requirements of the applicable orders. Recommended Corrective Actions are just that, a recommendation that will assist the Unit Commander in alleviating the deficiency and coming in compliance with the applicable order. (Example: Recommendation - A Key Control log Book should be utilized vice single sheet Key Control log in order to prevent the surreptitious removal of log pages.)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

5. SURVEY COVER SHEET. The Survey Cover Sheet is intended to provide a means of control during the distribution, filing, and disposal of Crime Prevention/Physical Security Surveys. Each survey will be accompanied by a Survey Cover Sheet. A Survey Cover Sheet example is located on page D-10.

WARNING

SURVEY REPORT COVER
DOCUMENT



SURVEY REPORT COVER
DOCUMENT

**THE ATTACHED DOCUMENTATION IS A REPORT FROM THE
PHYSICAL SECURITY/CRIME PREVENTION SECTION**

This document must not be left unattended or where an unauthorized person may have access to it. When not in use, it must be stored in a safe place. While this document is in your possession, it is your responsibility that the information contained therein is not released to unauthorized persons. Requests for access to or disclosure of the attached document(s) must be referred to the originating command's Physical Security Unit.

DATE:

SURVEY CONTROL NO.:

FROM:

TO:

1. THIS DOCUMENT IS FURNISHED FOR YOUR INFORMATION OR/AND ACTION AS DEEMED APPROPRIATE.
2. WHEN THIS DOCUMENT IS NO LONGER NEEDED IT SHOULD BE DESTROYED BY BURNING OR SHREDDING.

1

Releasing Authority

FOR OFFICIAL USE ONLY

IF CLASSIFIED - SECNAVINST 5510.36 APPLIES

MCB FORM 5530/3 FEBRUARY 1997 (EF)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

UNITED STATES MARINE CORPS PHYSICAL SECURITY/CRIME PREVENTION SURVEY (1600) NAVMC 11121 (10-82) SN: 0000-00-006-8761 U/I: 100 SH PER PAD	DATE <i>(See Block 1 For Guidance)</i> <hr/> STATUS <i>(See Block 2 For Guidance)</i>
SURVEY CONTROL NO. <i>(See Block 3 For Guidance)</i>	DISTRIBUTION <i>(See Block 7 For Guidance)</i>
INSPECTING UNIT <i>(See Block 4 For Guidance)</i>	
REQUESTING UNIT <i>(See Block 5 For Guidance)</i>	
ORGANIZATION AND ADDRESS OF UNIT INSPECTED/SURVEYED <i>(See Block 6 For Guidance)</i>	TYPE OF SURVEY <i>(See Block 8 For Guidance)</i>
REF: <i>(See Block 9 For Guidance)</i>	
BASIS FOR SURVEY <i>(See Block 10 For Guidance)</i>	
SYNOPSIS OF SURVEY <i>(See Block 11 For Guidance)</i>	
DATA AFFECTING SURVEY SITE <i>(See Block 12 For Guidance)</i>	
SIGNATURE OF INSPECTOR	SIGNATURE OF APPROVING OFFICER
TYPED NAME AND GRADE OF INSPECTOR <i>(See Block 18 For Guidance)</i>	TYPED NAME AND GRADE OF APPROVING OFFICER <i>(See Block 19 For Guidance)</i>

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

SURVEY CONTROL NUMBER (See Block 3 For Guidance)

BUILDING AND AREA

(See Block 13 For Guidance)

PHYSICAL SECURITY BARRIERS

(See Block 14 For Guidance)

1. Walls -
2. Doors -
3. Floor -
4. Ceiling/Roof -
5. Windows/Other Openings -
6. Natural -

PHYSICAL SECURITY AIDS, EQUIPMENT, AND DEVICES

(See Block 15 For Guidance)

1. Lighting (Exterior/Interior) -
2. Fencing -
3. Locks -
4. Vaults/Safes/Containers -
5. Electronic Security System (ESS) -
6. Key and Lock Control -

PAGE 2 OF 3

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

SURVEY CONTROL NUMBER (See Block 3 For Guidance)

7. Security Force -

PREVENTIVE MEASURES AND PROCEDURES

(See Block 16 For Guidance)

1. Security Orders/SOP -
2. Access Control -
3. Property Accountability -
4. Robbery/Burglary Procedures -
5. Crime/Loss Prevention Awareness Training -

ACTION/COMMENT

(See Block 17 For Guidance)

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX E

WAIVER AND EXCEPTION FORMAT

1. WAIVER AND EXCEPTION IDENTIFICATION. This appendix provides guidance for the assignment of waiver or exception numbers for deviations from established physical security standards. This format is also applicable when requesting extensions. The objective is to provide a ready identification of any given waiver or exception with respect to the organization involved, year of issue, and current status. The following paragraphs apply to each waiver or exception in regard to identification purposes to ensure compatibility with the automated database.

a. The first character will be the letter M, followed by the Unit Identification Code (UIC) of the organization initiating the request. The letter M is required to maintain compatibility with the automated database.

b. The character after the UIC will be W for waiver or E for exception.

c. The characters after the W or E will represent subsequent numbers of request during the calendar year beginning with 01. Waiver and exception numbers will run sequentially, i.e., W-01-99, W-02-99, W-03-99 and E-01-99, E-02-99, E-03-99.

d. Original waiver and exception numbers will be utilized for all extension requests. Subsequent extension requests will be identified by successive letters of the alphabet beginning with A, i.e., W-01A-99, E-02C-99, etc.

EXAMPLE: M02222-E01-99

M - Marine Corps Organization
02222 - Unit Identification Code
E - Identifies an exception request
01 - Identifies initial exception request (Second request
 would read E01A, third request E01B, etc.)
99 - 1999 (year initial exception was requested)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

2. WAIVER FORMAT

Line 1 - Waiver number.

Line 2 - Specific statement of actual requirement with reference to chapter, section, and paragraph in the applicable security manual which cite standards which cannot be met.

Line 3 - Specific description of condition(s) that cause the need for the waiver and reason(s) why applicable standards cannot be met.

Line 4 - Complete description of the physical location of affected facilities or area. Structures will be identified by building number.

Line 5 - Identify interim **mandatory compensatory measures in effect or planned.**

Line 6 - Describe the impact on mission and any problems that will interfere with safety or operating requirements if the waiver is not approved.

Line 7 - Identify resources, including estimated cost, to eliminate the waiver.

Line 8 - Identify actions initiated or planned to eliminate the waiver or estimated time to complete, to include the organization plan of action and milestones.

Line 9 - Point of contact to include name, rank, autovon and commercial phone numbers.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

3. EXCEPTION FORMAT

Line 1 - Exception number

Line 2 - Statement of the specific requirement with reference to chapter, section, and paragraph in the applicable security manual which cite standards which cannot be met.

Line 3 - Specific description of condition(s) that cause the need for the waiver and reason(s) why applicable standards cannot be met.

Line 4 - Complete description of the physical location of affected facilities or area. Structures will be identified by building number.

Line 5 - Identify, in detail, equivalent security measures and/or compensatory measures that are being applied. Also indicate the organization plan of action and milestones.

Line 6 - Describe the impact on mission and any problems that will interfere with safety or operating requirements if the exception is not approved.

Line 7 - Point of contact to include name, rank, autovon and commercial phone numbers.

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX F

KEY AND LOCK CONTROL FORMS

KEY INVENTORY RECORD

(DEPARTMENT)

On _____ keys _____ thru _____ were inventoried by _____
(DATE) (KEY I.D.) SIGNATURE
(PRINT NAME)

On _____ keys _____ thru _____ were inventoried by _____
(DATE) (KEY I.D.) SIGNATURE
(PRINT NAME)

On _____ keys _____ thru _____ were inventoried by _____
(DATE) (KEY I.D.) SIGNATURE
(PRINT NAME)

On _____ keys _____ thru _____ were inventoried by _____
(DATE) (KEY I.D.) SIGNATURE
(PRINT NAME)

On _____ keys _____ thru _____ were inventoried by _____
(DATE) (KEY I.D.) SIGNATURE
(PRINT NAME)

On _____ keys _____ thru _____ were inventoried by _____
(DATE) (KEY I.D.) SIGNATURE
(PRINT NAME)

On _____ keys _____ thru _____ were inventoried by _____
(DATE) (KEY I.D.) SIGNATURE
(PRINT NAME)

On _____ keys _____ thru _____ were inventoried by _____
(DATE) (KEY I.D.) SIGNATURE
(PRINT NAME)

On _____ keys _____ thru _____ were inventoried by _____
(DATE) (KEY I.D.) SIGNATURE
(PRINT NAME)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX G

SEIWG-012 DATA FORMAT

As shown in the following table, SEIWG data consists of forty BCD characters, each composed of 4 data bits plus one odd parity bit plus one LRC. This will result in a total of 200 bits which will be packed into 25 Bytes. In order to comply with the requirements of most legacy equipment - at least 8 trailing zeros and 8 leading zeros should be added.

<i>SEIWG-012 Format</i>														
SS	Agency Code	FS	System Code	FS	Credential Number	FS	Series	FS	Issue	FS	SSN	Reserved	ES	LRC
1 OB h . ,	4	1 ODh =	4	1 ODh =	6	1 ODh =	1	1 ODh =	1	1 ODh =	9	7	1 OF h ?	1
All data consists of 4 bit BCD characters plus odd parity (Total of 5 bits) The LRC is the EXCLUSIVE OR of all BCD data from the SS to the ES, inclusive. A minimum of eight zero bits should precede the SS and trail the LRC for synchronization. The LRC also has an odd parity bit.														

SEIWG-012 Explanation

Special Characters:

The special characters consist of the Start Sentinel (SS), Field Separator (FS), End Sentinel (ES), and the Longitudinal Redundance Character (LRC).

Decimal Numbers:

All of the remaining codes are simple binary coded decimals (BCD). These consist of the **Agency Code**, **System Code**, **Credential Number**, **Credential Series (CS)**, **Individual Credential Issue (ICI)**, **Social Security Number (SSN)**, and the **"Reserved" Field**. Note that each user will have two unique codes on their badge (the Credential Number and the SSN). It is left to the discretion of the site security officer to determine which code

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

the Electronic Access Control System should "key on" to identify the badge holder.

- **Agency Code** - The Agency Code is a four digit code identifying the U.S. Government agency issuing the badge. **For example, "0004" represents the Marine Corps**
- **System Code** - The System Code is a four digit code identifying the specific government site or facility issuing the badge. The System Code is also commonly known as the "Facility Code". The objective is to assign System Codes so that each site within a government agency will have a System Code that is unique to that agency. **For example, if MCB Quantico as a System Code of "00014" then no other site within the Marine Corps may use that code.**
SYSTEM CODES FOR ALL MARINE CORPS INSTALLATIONS AND COMMANDS WILL BE ASSIGNED BY THE HQMC (PS) TECHNICAL SUPPORT AGENCY
- **Credential Number** - The Credential Number is a six digit code identifying the specific individual who is issued a badge. The Credential Number is also commonly known as the "**Encoded ID**". The Credential Number must be unique for each individual within a particular site. It is the responsibility of the installation provost marshal, for the MCESS, or unit security officer to ensure that all Credential Numbers are unique.
- **Credential Series (CS)** - The Credential Series (CS) is a one digit code which may be used to reflect major system changes as deemed necessary by the installation provost marshal, for the MCESS, or the unit security officer. For automated access control systems that are not an integrated part of the MCESS, the unit security officer decides how the CS will be utilized.
- **Individual Credential Issue (ICI)** - The Individual Credential Issue (ICI) is a one digit code. Although the ICI "initially encoded as a "1", will be incremented if a card is replaced due to loss or damaged (with all other information remaining the same), it is not actually being

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

used in this manner. This is because normally, when a card is lost or damaged, the Credential Number will be deactivated and the badge holder will be issued a new Credential Number along with a new badge. Therefore, there would be no need to increment the ICI. In actuality, the ICI should only be incremented if the existing badge loses its encoding and must be re-encoded. In this case the card holder will keep their existing card, the ICI will be incremented by one and all other information will remain the same.

- **Social Security Number (SSN)** - The Social Security Number (SSN) is a nine digit code used to store the Social Security Number of the badge holder.
- **"Reserved" Field** - Although it is note stated in the SEIWG-012 specification, the "Reserved" Field is a seven digit field which is presently being used to store two codes: The U.S. Government **Unit Identification Code (UIC)** and the **"Group Number"**.
- **Unit Identification Code (UIC)** - The Unit Identification Code (UIC) is a five digit field (the first five digits of the seven digit "Reserved Field" which is used to store the standard U.S. Government USC for the activity issuing the badge.
- **"Group Number"** - The "Group Number" is a two digit field (the last two digits of the "Reserved Field) which is presently not being used and may therefore be set to "00".

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX H

SECURITY RISK CATEGORIES

1. GENERAL. This appendix lists specific AA&E items in Security Risk Categories I through IV and provides table for categorizing ammunition and explosive items not specifically listed (an exception to applying this Decision Logic Table is when there is Tri-service agreement to place an item in a different security risk category than that indicated by the table).

a. Any single container that contains enough parts that, when assembled, will perform the basic function of the end item, will be categorized the same as that end item.

b. Newly developed missiles and rockets similar to those in Category I will be included automatically in that category as they come into the inventory.

2. MISSILES AND ROCKETS

a. Category I. Missiles and rockets in a ready-to-fire configuration, or jointly stored or transported with the launcher tube and/or gripstock and the explosive round, for example: Redeye, Stinger, Dragon, Javelin, Light Antitank Weapon (LAW) (66mm), shoulder-launched multi-purpose assault weapon (SMAW) rocket (83mm), M136 (AT4) antiarmor launcher and cartridge (84mm).

b. Category II. Missiles and rockets that are crew-served or require platform-mounted launchers and other equipment to function. Included are rounds of the tube-launched optically tracked weapon (TOW) and Hydra-70.

c. Category III. Missiles and rockets that require platform-mounted launchers and complex hardware and software equipment to function, such as the Hellfire missile.

3. ARMS

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

a. Category II. Light automatic weapons up to and including .50 caliber and 40mm MK 19 machine guns. Note: Marine Corps activities will treat 25mm M242 (Bush Master) chain guns (and similar newly-developed weapons) as Category II arms if they are not mounted on secured vehicles.

b. Category III

(1) Stinger missile launch tube and gripstock.

(2) Redeye missile launch tube, sight assembly, and gripstock.

(3) Dragon missile tracker.

(4) Mortar tubes up to and including 81mm.

(5) Grenade launchers.

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

(7) Flame throwers.

(8) TOW launcher, missile guidance set and optical sight.

c. Category IV

(1) Nonautomatic shoulder-fired weapons, other than grenade launchers.

(2) Handguns.

(3) Recoilless rifles up to and including 106mm.

4. AMMUNITION AND EXPLOSIVES

a. Category I. Complete explosive rounds for Category I missile and rockets.

b. Category II

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- (1) Hand or rifle grenades - high explosive and white phosphorus.
- (2) Mines, antitank or antipersonnel (unpacked weight of 50 pounds or less each).
- (3) Explosives used in demolition, C-4, military dynamite, and TNT with an unpacked weight of 100 pounds or less.
- (4) Warheads for sensitive missiles and rockets weighing less than 50 pounds each.
- (5) The binary intermediates "DF" and "QL" when stored separately from each other and from the binary chemical munition bodies in which they are intended to be employed (see DoD Directive 5210.65 of 15 October 1986 (NOTAL) for security requirements for other chemical agents).

Note: Weapon components such as silencers, mufflers, and noise suppression devices will be treated as Category II items.

c. Category III

- (1) Ammunition, .50 caliber and larger, with explosive filled projectile (unpacked weight of 100 pounds or less each)
- (2) Incendiary grenades and fuses to high explosive grenades.
- (3) Blasting caps.
- (4) Supplementary charges.
- (5) Bulk explosives.
- (6) Detonating cord.
- (7) Warheads for sensitive missiles and rockets weighing more than 50 pounds but less than 100 pounds each.

d. Category IV

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

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

(2) Fuses, except for high explosives as addressed above).

(3) Illumination, smoke, and CS grenades.

(4) Incendiary destroyers.

(5) Riot control agents, 100 pound package or less

(6) Ammunition not in another Risk Category above.

(7) Explosive compounds of sensitive missiles and rockets (except warheads).

(8) Warheads for precision guided munitions (PGM) weighing more than 50 pounds (unpacked weight).

5. DECISION LOGIC TABLE. This table helps apply physical security risk category codes to ammunition and explosives not already categorized. Rate the ammunition or explosive item in each of the four risk factors listed here, obtaining a number value for each factor. Then add these numbers to determine the appropriate security risk category using the rankings shown here.

Total of Risk Factor Numbers	Physical Security Risk Category Code	Evaluation
4-5	II	High Sensitivity
6-8	III	Moderate Sensitivity
9-12	IV	Low Sensitivity
13-16	--	Nonsensitive

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

a. Utility

Numeric Value	Utility	Description
1	High	High explosive, concussion and fragmentation devices.
2	Moderate	Small arms ammunition.
3	Low	Ammunition items not described above--NONLETHAL, civil disturbance chemicals, incendiary devices.
4	Impractical	Practice, inert, or dummy munitions; small electric explosive devices; fuel thickening compound; or items possessing other characteristics which clearly and positively negate potential use by terrorist, criminal, or dissident factions.

b. Casualty/Damage Effect

Numeric Value	Casualty/Damage Effect	Description
1	High	Extremely damaging or lethal to personnel; devices which will probably cause death to personnel or major material damage.
2	Moderate	Moderately damaging or injurious to personnel; devices which could probably cause personnel injury or material damage.
3	Low	Temporarily incapacitating to personnel.
4	None	Flammable items and petroleum based products readily obtainable from commercial sources.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

c. Adaptability

Numeric Value	Adaptability	Description
1	Without Modification	Usable as is; simple to function without use of other components.
2	Slight Modification	Other components required; or can be used with slight modification.
3	Major Modification	Requires the use of other components which are not available on the commercial market; or can be used with modification that changes the configuration.
4	Impractical to modify	Requires specific functions or environmental sequences which are not readily reproducible, or construction makes it incapable of producing high order detonation; for example, gas generator grains, and impulse cartridges.

d. Portability

Numeric Value	Portability	Description
1	High	Items which easily can be carried by one person and easily concealed.
2	Moderate	An item whose shape, size and weight allows it to be carried by one person for a short distance.
3	Low	Items whose shape, size and weight requires at least two persons to carry.
4	MHE Required	The weight, size and shape of these items preclude movement without MHE.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX I

AA&E SCREENING PACKAGE

LOCAL RECORD CHECK (1600)

NAVMC 10482 (REV. 2-76) (Previous edition will be used)
SN: 0000-00-005-2402 U/I: 3H

DATE:

=====

NAME (Last, First, Middle)

SSN

GRADE

ORGANIZATION

DATE OF BIRTH

PLACE OF BIRTH

CITIZENSHIP

INFORMATION NOT REQUIRED

NAME OF SPOUSE (Last, First, Middle)

DATE OF BIRTH

PLACE OF BIRTH

CITIZENSHIP

CLEARANCE STATUS (Degree)

BASIS

COMPLETED BY (Agency)

DATE COMPLETED

ARMORY/AMMO SCREENING

PURPOSE FOR REQUESTING LOCAL RECORDS CHECK

RESULTS OF COMMAND SCREENING

RECORDS CHECKED: OQR/SRB HEALTH RECORD UNIT PUNISHMENT LOG

RECORDS SCREENED BY THE COMMAND REFLECT (Check appropriate block):

NO DEROGATORY INFORMATION FOLLOWING INFORMATION:

(Signature of Requesting Official)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

**PERSONNEL SCREENING FORM
FOR ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)
(REV DTD 29 JAN 00)**

Screening (circle one): initial or annual

Ref: (a) MCO P4400.150E
(b) CMC WASHINGTON DC 280101Z JAN 00

Individual being screened	Individual conducting screening
Rank/Name:	Rank/Name:
SSN/MOS:	SSN/MOS:
Billet:	Billet:
Date of screening:	Date of screening:
Signature:	Signature:

SUBJECT	YES	NO	EXPLAIN "NO" RESPONSES
Subject Marine's medical record has been screened by a competent medical authority. There are no medical conditions that would prevent this Marine from handling AA&E.			
Subject Marine's service record book or officer qualification record has been screened. There is no derogatory information that would prohibit this Marine from handling AA&E.			
Subject Marine has no pending legal action and/or convictions by court-martial, civilian courts, or non-judicial punishment that would prohibit this Marine from handling AA&E.			
Subject Marine demonstrates the requisite maturity, judgment, and leadership required to handle AA&E.			
Has the Marine had a National Agency Check (NAC) or Entrance National Agency Check (ENTNAC) completed and is the result posted in the MMS system?			
Has the Marine qualified with the required security weapon within the last 12 months?			
Has the Marine completed instruction in the use of deadly force in the last three months and signed a deadly force certification if required to be armed in the performance of his/her duties?			

Based on the above information, I have determined that the subject Marine (check one):

- does meet the personnel screening requirements to handle AA&E in performance of their regular duties.
- currently does not meet the personnel screening requirements to handle AA&E in performance of their regular duties. Subject Marine will be re-evaluated in ___ days.
- can not meet the personnel screening requirements to handle AA&E in performance of their regular duties. A summary of the findings for non-qualification are attached. If appropriate, the command will request via CMC (Code MM) that action be taken to re-train and/or reassign subject individual to an occupational field not requiring routine handling of AA&E.

Retention: This Record will be maintained for one year after termination of the individual's assignment, or one year after final interview if the individual is disqualified during the screening or re-screening process.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL



UNITED STATES MARINE CORPS

XX BATTALION XX MARINES
1ST MARINE DIVISION (REIN), FMF
PO BOX 55551
CAMP PENDLETON, CA 92055-5514

IN REPLY REFER TO:
8000
Ord
XX Date XX

From: Arms, Ammunition, and Explosives Officer
To: Medical Officer

Subj: MEDICAL SCREENING FOR AA&E DUTIES CASE OF

1. Please Screen the above individual's health record for assignment to AA&E duty. A positive response to any of the questions listed below will automatically disqualify the individual from assignment to any arroyo (ies) within this Regiment.

- a. Does the Marine have history of alcohol abuse?
YES _____ NO _____
- b. Has the Marine been the subject of psychiatric evaluation?
YES _____ NO _____
- c. Has the Marine been treated for suicidal tendencies?
YES _____ NO _____
- d. Has the Marine been treated for depression?
YES _____ NO _____
- e. Has the Marine been treated for stress?
YES _____ NO _____
- f. Has the Marine been treated for drug abuse?
YES _____ NO _____
- g. Is the Marine under any permanent medication that might degrade his mental capacity? If yes, please advise.
YES _____ NO _____

2. The above Marine's Medical Record Book has been reviewed, and found to be qualified for assignment.

MEDICAL OFFICER SIGNATURE AND DATE

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL



UNITED STATES MARINE CORPS

XX BATTALION, XX MARINE REGIMENT
1ST MARINE DIVISION, FMF
BOX 555514
CAMP PENWELTON, CALIFORNIA 92055-5514

BY REPLY REFER TO
4400
AA&E
00 Apr 04

From: Arms Ammunition and Explosives Officer
To: Personnel Officer

Subj: REQUEST UNIT DIARY ENTRY TRANSACTION CODE 489 (A&E SCREEN)

Ref: (a) MCO P4400.150E
(b) CMC WASHINGTON DC 280101Z.JAN 00

1. Per the references, request a unit diary entry be made for the below listed Marines. These Marine's medical records, Service Record Books, and Local Record Checks have been reviewed and have been found to be qualified to account for, maintain and distribute Arms, Ammunitions, and Explosives (AA&E) in the performance of their primary duties.

RANK	NAME	SSN/MOS	BILLET
GySgt	Ima Marine	123456789/21XX	Chief

2. Please annotate in the space provided below the unit diary entry number assigned. UD# _____

I. M. INCHARGE

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX J

MLSR AA&E REPORTABLE QUANTITIES

The loss, theft, recovery, or inventory adjustment of the following shall be reported by MLSR message as soon as possible but not later than 48 hours:

1. One or more missile or rocket;
2. One or more machine guns;
3. One or more automatic fire weapons;
4. One or more manually operated or semiautomatic weapons (includes revolvers and semiautomatic pistols);
5. Over 1,000 rounds or more of ammunition smaller than 20mm;
6. Individual rounds of 20mm and larger ammunition;
7. 2000 rounds or more of .38 caliber ammunition;
8. Any fragmentation, concussion, or high explosive grenades including artillery or ground burst simulators, or other type of simulator or device containing explosive material;
9. One or more mines (antipersonnel and antitank);
10. Demolition explosives and explosive detonators including detonation cord, DETA sheet, explosive cutting tape, flexible linear shaped charges, blocks of explosives (C-4, TNT), other explosives, and blasting caps.
11. Armed robberies or attempted armed robberies of AA&E facilities;
12. Forced entries or attempted forced entries into AA&E facilities;

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

13. Evidence of terrorist involvement in the theft of AA&E;
14. Incidents involving AA&E that cause significant news coverage, or appear to have the potential to cause such coverage; and
15. Evidence of trafficking or bartering involving AA&E, illegal drugs, etc., regardless of the quantity of AA&E involved.

APPENDIX K

KEY AND LOCK CONTROL FORMS

BUREAU OF ALCOHOL, TOBACCO AND FIREARMS MUNITIONS LOSS
WORKSHEET

DEPARTMENT OF THE TREASURY - BUREAU OF ALCOHOL, TOBACCO AND FIREARMS MUNITIONS LOSS WORKSHEET	ATF LOSS NUMBER (ATF use only)
---	-----------------------------------

SECTION A

1. DOD INVESTIGATIVE AGENCY SUBMITTING FORM (include specific office, case agent's name, & telephone number)

2. INVESTIGATION/CASE CONTROL # (if applicable)	3. TYPE OF INCIDENT <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">THEFT</td> <td style="width: 50%; text-align: center;">EXPLOSIVES</td> </tr> <tr> <td style="text-align: center;">LOSS</td> <td style="text-align: center;">FIREARMS</td> </tr> <tr> <td style="text-align: center;">OTHER</td> <td style="text-align: center;">AMMUNITION</td> </tr> </table>	THEFT	EXPLOSIVES	LOSS	FIREARMS	OTHER	AMMUNITION	4. DATE WHEN OCCURRED (if unknown, provide date when discovered)
THEFT	EXPLOSIVES							
LOSS	FIREARMS							
OTHER	AMMUNITION							
5. MILITARY ORGANIZATION OR DOD ELEMENT WHICH IS VICTIM OF THEFT/LOSS (name, address, city, county, state, country)	6. LOCATION WHERE INCIDENT OCCURRED (name/street address, building #, city, county, state, country)							

7. DETAILS (check all that apply)

<input type="checkbox"/> CLASSIFIED (if checked, indicate classification level) _____	<input type="checkbox"/> FORCED ENTRY
<input type="checkbox"/> INVENTORY LOSS	<input type="checkbox"/> ATTEMPTED FORCED ENTRY
<input type="checkbox"/> TRAINING LOSS	<input type="checkbox"/> NARCOTICS RELATED
<input type="checkbox"/> OPERATIONAL LOSS	<input type="checkbox"/> EVIDENCE OF TERRORIST INVOLVEMENT
<input type="checkbox"/> LOSS DURING TRANSPORTATION	<input type="checkbox"/> EVIDENCE OF FIREARMS/MUNITIONS TRAFFICKING
<input type="checkbox"/> THEFT FROM MAGAZINE, IGLOO, BUNKER	<input type="checkbox"/> EVIDENCE OF TAKING ITEMS ACROSS INTERNATIONAL BORDERS
<input type="checkbox"/> THEFT FROM ARMORY, ARMS ROOM	<input type="checkbox"/> OTHER
<input type="checkbox"/> THEFT FROM PERSON	
<input type="checkbox"/> ARMED ROBBERY	
<input type="checkbox"/> ATTEMPTED ARMED ROBBERY	

8. ADDITIONAL DETAILS (identification of suspects, unique aspects, etc.)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

INVESTIGATION/CASE CONTROL #			
SECTION B: EXPLOSIVE ORDNANCE- IN THIS SECTION ALSO INCLUDE AMMUNITION OVER .50 CALIBER, AND ALL DEMOLITION MATERIALS			
1. NOMENCLATURE	2. NSN/FSN	3. DODIC	
4. QUANTITY	5. LOT NUMBER	6. SOURCE AND/OR MANUFACTURER	7. DATE LOADED
8. ADDITIONAL COMMENTS OR PART NUMBERS			

SECTION C: FIREARMS			
1. NOMENCLATURE	2. NSN/FSN	3. TYPE	
4. CALIBER OR GAUGE	5. MODEL NUMBER	6. QUANTITY	
7. SERIAL NUMBERS		8. SOURCE AND/OR MANUFACTURER	
9. WAS AN NCIC ENTRY MADE (all firearms should be entered into NCIC as lost or stolen) <input type="checkbox"/> YES <input type="checkbox"/> NO		10. ORI CODE OF ENTERING AGENCY	
11. ADDITIONAL COMMENTS			

SECTION D: AMMUNITION- TO INCLUDE ALL AMMUNITION .50 CALIBER AND UNDER			
1. NOMENCLATURE	2. CALIBER	3. TYPE (ex: ball, tracer, AP-T, etc)	
4. NSN/FSN	5. DODIC	6. LOT NUMBER	
7. QUANTITY	8. SOURCE AND/OR MANUFACTURER		
9. ADDITIONAL COMMENTS			

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

INSTRUCTIONS

The ATF Headquarters Intelligence Branch shall be provided information by telephone (followed up in writing) from the reporting DOD components of all significant/serious incidents of theft, loss, or unaccounted for Arms, Ammunition and Explosives Material (AA&EM) as soon as possible but no later than 72 hours after occurrence or discovery. Telephone the ATF Intelligence Branch at (202)927-8000. This number will be in operation 24 hours a day. The following information must be provided: Your name, agency, location, telephone number, case control number (if applicable), date and place incident occurred. Immediately subsequent to this telephone notification, please submit the completed Munitions Loss Worksheet by FAX to: (202)927-8001, or mail to: Bureau of Alcohol, Tobacco, and Firearms (ATF), Washington, D.C. 20226, ATTN: Intelligence Branch.

Generally, loss or theft of the following AA&EM shall be considered significant/serious and shall be reported to ATF on the Munitions Loss Worksheet, ATF Form 3270.19, (appropriate sections to list munitions losses are indicated below in parentheses next to item):

1. One or more missile or rocket rounds (report in Section B - Explosives Ordnance).
2. One or more machine guns (report in Section C - Firearms).
3. One or more automatic fire weapons (report in Section C - Firearms).
4. Twenty-five or more manually operated weapons (report in Section C - Firearms).
5. Ammunition (reportable incidents do not include losses known to have been expended during training) - .50 caliber and smaller - 5,000 rounds or more, except in the case of .38 caliber ammunition, report losses of 20,000 rounds or more (report in Section D - Ammunition).
6. Ammunition which is larger than .50 caliber - five (5) rounds or more of nonautomatic weapon ammunition; 1,000 rounds or more of ammunition for automatic weapons (REPORT ALL OF THESE ITEMS IN SECTION B - EXPLOSIVES ORDNANCE).
7. Any fragmentation, concussion, or explosive grenade to include artillery or ground burst simulators, or any other type, or any other type of simulator or device containing explosive materials (report in Section B - Explosives Ordnance).
8. One or more mines - antipersonnel and antitank (report in Section B - Explosives Ordnance).
9. Demolition explosives including detonation cord, blocks of explosives (C-4) and other types of explosive materials (report in Section B - Explosives Ordnance).
10. Also reportable are: Armed robberies or attempted armed robberies of the above items; forced entries or attempted forced entries in which there is physical evidence of the attempt wherein the above items are stored; any evidence of trafficking in the above items or using same to barter for narcotics or any other thing of value to include the taking of AA&EM across international borders unlawfully, regardless of the quantity of AA&EM involved.

In order to report more than one incident, use separate worksheets. If one incident includes the loss of different types of munitions, or large quantities of the same munitions, please use additional sheets of Section B, C, and D, or list items on sheet of plain, white paper. It is not necessary to duplicate the front of the Munitions Loss Worksheet, if you are reporting on the same incident. However, please include the investigation/case control # on the continuation sheet.

Note:

Military explosives and ordnance identification: The Department of Defense identifies all explosives and ordnance by a lot number, DODIC number, and FSN/NSN. The lot number identifies the manufacturing plant, month/year of production (date loaded), and lot sequence. This code provides the military with a way to track explosives through the system from manufacture to use or destruction. The DODIC number (usually one letter followed by three numbers, i.e. G881), is a "short-hand" of identifying ordnance or explosives. It is used by the military to catalog ordnance and explosives for supply purposes. The FSN/NSN of an item is an eleven/thirteen digit number assigned to an individual item. It is the number used to order/reorder anything in the federal supply system. This number can help to identify ordnance or explosives.

Examples of Lot Numbers: LOP77M007-003; ME183J002-008;
ICP-5-25 loaded 6/89.

These reporting instructions should not preclude any continuing liaison that your office may have with the local ATF Post of Duty in regard to joint investigations.

Any questions should be directed to the Special Agent in Charge, ATF Intelligence Branch, Telephone #: (202) 927-8000.

Coordinating Draft for Review 10 June 2004

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX L

LEPSAR PREPARATION INSTRUCTIONS

1. Sections I through IV and Section VI A. To complete these sections use the following instructions for columns a through m.

2. What Offenses are Reported (column a). To complete NAVMC 11197 use every available source to include OPNAV Forms 5527/1, DD Forms 1408 and 1805, as well as traffic tickets and incident reports received from civilian police agencies.

a. Supervisors must exercise good judgment in tabulating offenses reported. For example, extremely minor incidents such as juvenile shoving matches, theft of penny candy or offenses which are not processed for further investigation or corrective action should not be counted when completing the report.

b. One purpose of offense reporting is to document the incidents occurring at each installation. In this respect, the installation at which the incident occurs reports the offense, even though the subject may be from a different installation. Units that receive incident complaints or tickets from other service installations should not count the offenses when completing their report, since they will have been previously counted by the reporting installation.

c. Count only founded offenses. Offenses are counted in the titled category when determined to be "founded offenses" by law enforcement personnel. Report an incident only once; do not report the incident again to reflect the results of a military or civilian court or administrative discharge proceedings. For example, an incident originally classified as a robbery which occurs in January should be reported in the first quarter only; it should not be reported again if a conviction or acquittal occurs in October, or if the conviction is of a lesser included offense such as larceny or assault.

3. Reporting the Number of Incidents (column b). When reporting the number of crimes or offenses, the following rules apply:

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

offenses, report each offense the person is charged with. Do not report lesser included offenses. For guidance, see the Manual for Courts-Martial, United States 1984 (MCM).

b. When a single incident involves several offenders, list only one offense for a victim or incident. For example, if five persons murder two people, two homicides have occurred, even though all five offenders would be categorized under the identified subject columns. However, the burglary of a residence would be shown as one burglary, even if three persons live in the house, and regardless of the number of suspects.

c. The number of attempts will be listed in the respective block by placing it in parentheses; i.e., 17(4) would represent 17 actual offenses, and 4 attempted offenses.

4. Location of Offenses (columns c and d). Categorize "on base" and "off base" incidents according to geography, not jurisdiction. Subjects of on base offenses will be categorized in columns e through m. Subjects of off base incidents will not be categorized for reporting on this report.

5. Identified Subjects (columns e through i). Under this section, report the suspects of the offense. Under Marine Corps and Other Service, combine officers and enlisted. Department of Defense (DoD) civilians include appropriated and non-appropriated fund employees. Military dependents include all dependents of military personnel. Report all others, such as on base contractors, civilians, etc., under the "Others" category. The fact that the subject is or is not covered by the provisions of the UCMJ is not material in classifying offenses for reporting purposes. When a subject can be classified in two categories, that is, dependent and DoD civilian, include the person in the category that reflects the closest service affiliation. This section applies only to on base offenses.

6. Unidentified Subject (column j). In this column, list each offense for which the subjects could not be identified. This category applies only to on base offenses.

7. Drug and Alcohol Involvement (columns k and l). In these columns, enter the number of incidents in which the subject(s)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

was involved with drugs or alcohol, whether or not it was part of the formal charges. Additionally, in the respective block, enter the number of incidents in which the victim(s) was involved with drugs or alcohol by placing the number in parentheses. This section applies only to on base offenses.

8. Juvenile (column m). List the number of juvenile subjects (under the age of 18). Service members under the age of 18 will not be classified as juveniles. Juvenile offenders are counted in this category in addition to having been reported in column g, h, i, or j. Also list the number of incidents which had a juvenile victim, by placing the number in parentheses.

9. Special Reporting Instructions

a. In section V, fill out column b only.

b. In section VI B, the following definitions apply:

1) Military On Base. All active duty military assigned to the installation.

2) Other Base Pers. Civilian employees and military dependents residing on the installation.

3) Others. All others, such as visitors to the installation.

10. Final Instructions for Lines 1 through 60

a. Section I - Crimes Against Persons

1) Murder. Violation of article (art.) 118.

2) Rape. Violation of art. 120; except acts of carnal knowledge under art. 120c(2).

3) Robbery. Violation of art. 122.

4) Aggravated Assault. Violation of art. 128c(4). Do not report cases of simple assault, and assaults that permit increased punishments based on rank or position of the victim under art. 128.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

5) Assault against on-duty police officer. Violation of art. 128c(3) (b). If the victim is performing law enforcement or security duties.

6) Simple assault or assault and battery. Violation of art. 128 not previously listed on line 4 or 5.

7) Manslaughter. Violation of art. 119.

8) Sex offenses. Violation of art. 120c(2), art. 125 and sex-related crimes of art. 134.

9) Suicide. List the number of suicides which resulted in death. Indicate attempts and suicidal gestures by placing the number in parentheses; i.e., 4(20) would indicate 4 suicidal deaths and 20 attempts or gestures.

10) Domestic disturbances. Any situation erupting between family or household members requiring response or intervention by police.

b. Section II - Crimes Against Property

11) Arson. Violation of art. 126.

12) Burglary/Housebreaking. Violation of art. 129 or 130.

13) Larceny and wrongful appropriation (Government property). Violation of art. 121 when the property is Government-owned, except larceny of motor vehicle, which will be reported on line 15.

14) Larceny and wrongful appropriation (Non-government property). Violation of art. 121 when the subject property did not belong to the Government, with the same exception as listed on line 13.

15) Auto Theft. Violation of art. 121. Larcenies and wrongful appropriations of any vehicles, including Government owned. "Vehicle" includes a motorized automobile, truck, bus, motorcycle, and any vehicle operating on land, but not on rails. Report total number of recovered vehicles in parentheses; i.e., 30(10) would represent 30 thefts and 10 recoveries.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

16) Willful property destruction (Government). Violation of art. 108. Vandalism to Government property.

17) Willful property destruction (Non-government). Violation of art. 109. Vandalism to non-Government property.

18) Other. Use this line to report other crimes against property not previously reported on lines 11 through 17. See Appendix A for definition of "other."

c. Section III - Miscellaneous Crimes

19) Fraud. Violation of art. 132.

20) Smuggling. Violation of art. 92, as it relates to local regulations prohibiting such activities.

21) Black market activities. Violation of art. 92, as it relates to local regulations prohibiting such activities. Black marketing is the exchange of commodities in violation of price, other pertinent regulations.

22) Trespass. An illegal entry onto a military installation, as defined by Federal Statute (50 U.S.C. 797).

23) Prowler. Cases of prowler incidents.

24) Homosexuality. List the total number of homosexual acts. This includes the same sex or with an animal. See art. 125. This also includes lewd and lascivious acts not necessarily involving copulation. See art. 134.

25) Disturbances. Violation of art. 116 or lesser offenses of art. 116, including any disturbance resulting in the initiation of an incident complaint report. For example, incidents at clubs, affrays, etc.

26) Disorderly Conduct. Acts when law enforcement personnel are called on to neutralize disturbances not meeting criteria of line 25. See art. 134.

27) Other. Other crime-related incidents not reported in lines 1 through 26, or sections IV through VI. Examples of

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

incidents reported in this line are military offenses, illegal alien detentions, provoking speeches or gestures, etc.

d. Section IV - Drug Offenses

28-30) Use/Possession. Violation of art. 112a, paragraphs b(1) and b(2). Unlawful use or possession of narcotics, dangerous drugs, or cannabis products. Includes transfer without payment or recompense. 6

31-33. Sale/Transfer. Violation of art. 112a, paragraph b(3). Unlawful sale of, or trafficking in narcotics, dangerous drugs, or cannabis products.

e. Section V - Other Security Response Activities

34) Unsecured Building. When law enforcement personnel respond to complaints of, or discover improperly secured buildings or facilities.

35) IDS/Duress. When law enforcement personnel alarm respond to intrusion detection activation systems (IDS) or duress alarms from protected facilities. For example, fund activities; conventional arms, ammunition, and explosives storage facilities; and other alarmed activities. List in parentheses the number of responses determined to be nuisance/false alarms; i.e., 75(30) would represent 75 total alarm responses, of which 30 were nuisance or false alarms.

36) Animal Control. Animal control incidents, including animal bites and control of strays.

37) Other. Any other law enforcement response activity not already covered.

e. Section VI - Traffic Law Enforcement

38-41) Alcohol related driving offenses. In the appropriate blocks, record the number of chemical breath, blood, and urine tests administered to and refused by offenders. Of this total, place the number of blood and urine tests in parentheses; i.e., 45(7) would represent 45 tests, of which 7 were blood or urine tests.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

42) Moving Violations. Record the number of offenses resulting in the issuance of a DD Form 1408 or DD Form 1805 for moving violations. Do not include those violations previously listed on lines 38 through 41.

43) Driving privileges. In blocks a and b, enter the number of personnel whose installation driving privileges were suspended or revoked during the reporting period. In the total block, report total driving privileges suspended and revoked during that reporting period.

44-45) Motor Vehicle Traffic Accidents. Enter the number of accidents reported to or investigated by law enforcement personnel. Each accident will be listed in only one category of section a. List accidents in the category of greatest significance. For each fatal accident listed, show at least one person killed under "Number of persons Killed," column b. It is possible to have more persons shown as killed, than the number of fatal accidents (that is, one fatal accident where two or more people die). The "number of persons injured" column should indicate the total number of persons injured in accidents. In column c, determine alcohol and drug involvement for drivers, pedestrians, and for those passengers whose actions are determined to have directly contributed to the accident. Regardless of the number of drivers, passengers, or pedestrians identified as being under the influence of alcohol or drugs, make only one entry for each accident in the proper column.

f. Section VII - Physical Security and Crime Prevention Activities.

46) Child Identification Program. Record the number of dependent children residing aboard the installation. Also record the number of children (under the age of 18) fingerprinted during the reporting period, and the year-to-date total.

47) Physical Security Program. In the first block, enter the number of annual physical security surveys required for the installation, per this Manual. In the remaining blocks, enter the number of physical security surveys conducted during the reporting period, and year-to-date.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

48) Crime Prevention Program. In the first block, enter the number of annual crime prevention surveys required, per this Manual. In the remaining blocks, enter the number of crime prevention surveys conducted, and crime prevention presentations given during the reporting period, and year-to-date.

g. Section VIII - Installation Population.

49) Military. All permanent personnel assigned to the installation, and those military members TAD to the installation or activity for a period in excess of 30 days.

50) Dependents Living In Base Housing. Enter the number of dependents residing in base housing.

51) Civilian Employees. Enter the number of installation civilian employees, including non-appropriated fund employees.

52) Total. Enter population total.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

LAW ENFORCEMENT AND PHYSICAL SECURITY ACTIVITIES
NAVMC 11197 (4-88)
 SN: 0000-00-888-0150 U/R: SH
 REPORT CONTROL SYMBOL NODD-1610-02

PERIOD COVERED:
DATE PREPARED:
PREPARED BY:

FROM:

TO: COMMANDANT OF THE MARINE CORPS
 HEADQUARTERS U.S. MARINE CORPS
 ATTN: POS-18
 2 NAVY ANNEX
 WASHINGTON D.C. 20380-1775

I. CRIMES AGAINST PERSONS

TYPE OF OFFENSE	NUMBER OF INCIDENTS	LOCATION		NUMBER OF SUBJECTS IDENTIFIED					INVOLVEMENT			
		ON BASE	OFF BASE	USMC	OTHER SERVICE	DOD CIV	MIL DEPEN	OTHERS	NO CASES UNIDENTIFIED SUBJECT	DRUGS	ALCOHOL	JUVE-NILES
1. MURDER												
2. RAPE												
3. ROBBERY												
4. AGGRAVATED ASSAULT												
5. ASSAULT AGAINST ON DUTY POLICE OFFICER												
6. SIMPLE ASSAULT												
7. MANSLAUGHTER												
8. SEX OFFENSES												
9. SUICIDE												
10. DOMESTIC DISTURBANCES												

II. CRIMES AGAINST PROPERTY

11. ARSON												
12. BURGLARY/ HOUSEBREAKING												
13. LARCENY GOVERNMENT												
14. LARCENY NON-GOVERNMENT												
15. AUTO THEFT												
16. WILLFUL PROPERTY DESTRUCTION GOV'T												
17. WILLFUL PROPERTY DESTRUCTION NON-GOV'T												
18. OTHER												

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

LAW ENFORCEMENT AND PHYSICAL SECURITY ACTIVITIES
NAVMC 11197 (4-88)
 SN: 0000-00-888-0150 U/R: SH
 REPORT CONTROL SYMBOL NO DD-1630-02

PERIOD COVERED:
DATE PREPARED:
PREPARED BY:

FROM:

TO: COMMANDANT OF THE MARINE CORPS
 HEADQUARTERS U.S. MARINE CORPS
 POS-18
 2 NAVY ANNEX
 WASHINGTON D.C. 20380-1775

III. MISCELLANEOUS CRIMES

TYPE OF OFFENSE	NUMBER OF INCIDENTS	LOCATION		NUMBER OF SUBJECTS IDENTIFIED					INVOLVEMENT			
		ON BASE	OFF BASE	USMC	OTHER SERVICE	DOD CIV	MIL DEPEN	OTHERS	NO CASES UNIDENTIFIED SUBJECTS	DRUGS	ALCOHOL	JUVENILES
19. FRAUD												
20. SMUGGLING												
21. BLACK MARKETING												
22. TRESPASSING												
23. PROWLER												
24. HOMO-SEXUALITY												
25. DISTURBANCE												
26. DISORDERLY CONDUCT												
27. OTHER												

IV. DRUG OFFENSES

a. USE-POSSESSION												
28. NARCOTICS											////////	
29. DANGEROUS DRUGS											////////	
30. CANNABIS PRODUCTS											////////	
b. SALES/TRAFFICING												
31. NARCOTICS											////////	
32. DANGEROUS DRUGS											////////	
33. CANNABIS PRODUCTS											////////	

V. OTHER SECURITY RESPONSE ACTIVITIES

34. UNSECURE BUILDINGS												
35. IDS/DURESS ALARMS												
36. ANIMAL CONTROL												
37. OTHER												

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

LAW ENFORCEMENT AND PHYSICAL SECURITY ACTIVITIES
NAVMC 11197 (4-88)
 SN: 0000-00-888-0150 U/R: SH
 REPORT CONTROL SYMBOL NO DD-1630-02

PERIOD COVERED:
DATE PREPARED:
PREPARED BY:

FROM:

TO: COMMANDANT OF THE MARINE CORPS
 HEADQUARTERS U.S. MARINE CORPS
 POS-18
 2 NAVY ANNEX
 WASHINGTON D.C. 20380-1775

VI. TRAFFIC LAW ENFORCEMENT

TYPE OF OFFENSE	LOCATION		NUMBER OF SUBJECTS IDENTIFIED						INVOLVEMENT			
	NUMBER OF INCIDENTS	ON BASE	OFF BASE	USMC	OTHER SERVICE	DOD CIV	MIL DEPEN	OTHERS	NO OF CASES UNIDENTIFIED SUBJECTS	DRUGS	ALCOHOL	JUVE-NILES
a. ALCOHOL RELATED DRIVING OFFENSES												
38. .10% BAC & ABOVE											////////	
39. .05%-.09% BAC											////////	
40. .04% BAC & BELOW											////////	
41. REFUSALS											////////	

CATEGORY		MILITARY ON BASE	OTHER BASE PERSONNEL	OTHERS	//////// ////////	MILITARY ON BASE	OTHER BASE PERSONNEL	OTHERS	TOTAL
42. MOVING VIOLATIONS	a. DD FORM 1408				b. DD FORM 1805				
43. DRIVING PRIVILEGES	a. SUSPENDED				b. REVOKED				
a. NUMBER OF ACCIDENTS			b. NUMBER OF PERSONS			c. INVOLVEMENT			

MOTOR VEHICLE TRAFFIC ACCIDENTS	FATAL	NON-FATAL	PROPERTY DAMAGE	KILLED		INJURED		DRUGS		FATAL		NON-FATAL	
				BASE PERS	OTHER	BASE PERS	OTHER	ALCOHOL	OTHER	ALCOHOL	OTHER		
44. ON BASE				1		1		1		1		1	
45. OFF BASE				1		1		1		1		1	

VII. PHYSICAL SECURITY/CRIME PREVENTION ACTIVITIES

46. CHILD ID PROGRAM	NUMBER OF DEPENDENT CHILDREN ON BASE		NUMBER OF CHILDREN FINGERPRINTED	QUARTER	YTD
47. PHYSICAL SECURITY PROGRAM	NUMBER OF PHYSICAL SECURITY SURVEYS REQUIRED		NUMBER OF PHYSICAL SECURITY SURVEYS CONDUCTED		
48. CRIME PREVENTION PROGRAM	NUMBER OF CRIME PREVENTION SURVEYS REQUIRED		NUMBER OF CRIME PREVENTION SURVEYS CONDUCTED		

VIII. POPULATION

IX PERSONNEL STRENGTH

49. MILITARY		53		57
50. DEPENDENTS LIVING IN BASE HOUSING		54		58
51. CIVILIAN EMPLOYEES		55		59
52. TOTAL		56		60