



Headquarters, U.S.
Marine Corps

MCO 5530.14A
PCN 10208597900

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

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



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

MCO 5530.14A
PS
JUN 05 2009

MARINE CORPS ORDER 5530.14A

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

- Ref:
- (a) DODI 5200.08, "Security of DOD Installations and Resources," December 10, 2005
 - (b) DOD 5100.76-M, "Physical Security of Sensitive Conventional Arms, Ammunition and Explosives," August 12, 2000
 - (c) DOD 4160.21-M, "Defense Materiel Disposition Manual," August 18, 1997
 - (d) SECNAVINST 5510.36A
 - (e) SECNAVINST 5510.30B
 - (f) SECNAVINST 5239.3A
 - (g) DODD O-5210.41, "Security Policy for Protecting Nuclear Weapons," November 1, 2004
 - (h) DODI 2000.16, "DOD Antiterrorism (AT) Standards," October 2, 2006
 - (i) UFC 4-010-01, "DOD Minimum Antiterrorism Standards for Buildings," January 22, 2007
 - (j) UFC 4-021-01, "Design and O&M: Mass Notification Systems," April 9, 2008
 - (k) MCO P11000.5G
 - (l) MCO P11000.12C
 - (m) MCO 3302.1D
 - (n) DOD O-2000.12-H, "DOD Antiterrorism Handbook," February 2004
 - (o) EKMS 1A (NOTAL)
 - (p) MCO 5110.1D
 - (q) MIL-HDBK-1013/1A, "Military Handbook Design Guidelines for Physical Security of Facilities," October 9, 1987
 - (r) MCO 5090.4A
 - (s) CJCSI 3121.01A, "Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces (U)," January 15, 2000
 - (t) DODD 5210.56, "Use of Deadly Force and the Carrying of Firearms by DOD Personnel Engaged in Law Enforcement and Security Duties," November 1, 2001

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

- (u) MCO 5500.6G
- (v) MCO 3574.2K
- (w) MCO 5580.2B
- (x) UFC 4-022-01, "Security Engineering: Entry Control Facilities/Access Control Points," May 25, 2005
- (y) DODD 8190.3, "Smart Card Technology," August 31, 2002
- (z) DODD 1000.25, "DOD Personnel Identity Protection (PIP) Program," April 23, 2007
- (aa) DOD 5200.08-R, "Physical Security Program," April 9, 2007
- (ab) NAVMED P-117
- (ac) DOD 6055.9-STD, "DOD Ammunition and Explosives Safety Standards," July 1999
- (ad) NAVSEA OP 5 Volume 1
- (ae) MCO P8020.10B
- (af) OPNAVINST 5530.13C
- (ag) NAVSUP P-724
- (ah) DOD 4500.9-R, "Defense Transportation Regulation (DTR)," August 2008
- (ai) DOD 5200.2-R, "Personnel Security Program," January 1987
- (aj) MCO 8023.3A
- (ak) DOD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," February 28, 2006
- (al) MCO P4400.150E
- (am) MCO P4400.151B
- (an) DOD 4140.1-R, "DOD Supply Chain Materiel Management Regulation," May 23, 2003
- (ao) OPNAVINST 8015.2B
- (ap) MCO 8300.1C
- (aq) MCO P8020.11
- (ar) DOD 4160.21-M-1, "Defense Demilitarization Manual," August 18, 1997
- (as) MCO 8373.2E
- (at) NAVSEA OP 3565 Vol II
- (au) MCO P5750.1G
- (av) NAVSEA SW020-AG-SAF-010
- (aw) NAVSEA SW023-AG-WHM-010
- (ax) MCO 1620.2D
- (ay) MCO P4066.17
- (az) DOD 7000.14-R, "DOD Financial Management Regulations (FMRs)," September 17, 2008
- (ba) SECNAV M-5214.1
- (bb) SECNAV M 5210.1

Encl: (1) Marine Corps Physical Security Program Manual

- Reports Required:
- I. Physical Security Survey Form (NAVMC 11121) (Report Control Symbol EXEMPT). Encl (1) Chap.3, par 3001.4 and App E
 - II. Missing, Lost, Stolen and Recovered (MLSR) Reporting (Report Control Symbol DD-5530-01). Encl (1), Chap 10, par. 10001.5 and App M
 - III. Law Enforcement and Physical Security Activity Report (LEPSAR) (Report Control Symbol (EXEMPT). Encl(1), Chap 10, par. 10004.1 and App N

1. Situation. Physical security is a primary command responsibility. Reference (a) requires commanders to establish and issue regulations for the security of property and places under their command. This Order constitutes the Marine Corps Physical Security Program and prescribes policy, assigns responsibilities, and presents requirements. The Order also provides uniform procedures, standards, supporting details, and outlines requirements to support commander's efforts. To be effective, a physical security program must receive attention from all echelons within the chain of command.

2. Cancellation. MCO P5530.14, MCO 5510.15A, MCO 5500.18, MCO 1630.4A, MCO 5500.14A, MARADMIN 601-02, MARADMIN 360-01, and participation with OPNAVINST 5530.13.

3. Mission. Establish the Marine Corps Physical Security Program and provide policy to support commander's efforts to maintain a robust physical security program. Ensure all personnel are aware of and involved in protecting United States Government and Marine Corps personnel and property, per references (a) through (bb).

4. Execution. The Marine Corps Physical Security Program must receive attention from all echelons within the chain of command. Emphasis is placed on the commander/commanding Officer's (CO) responsibility to ensure that the command security posture is accurately and consistently addressed and resources are afforded to execute and support these programs. Marines, Sailors, and civilian employees will be actively involved and vigilant in the security of United States (U.S.) Government and Marine Corps personnel and property. Commanders will develop and maintain an operational capability to present and preserve a sound, secure physical security posture throughout their areas of responsibility (AOR).

a. Commander's Intent and Concept of Operations

(1) Commander's Intent

(a) Enhance unit, base, and installation physical security by maintaining an effective physical security program.

(b) Integrate physical security planning, requirements, procedures, and equipment in all force protection (FP) and antiterrorism (AT) efforts.

(c) Provide physical security guidance and requirements.

(d) Control access to Marine Corps installations to prevent injury to personnel and/or damage to assets in accordance with reference (a).

(2) Concept of Operations. This Order establishes a formal physical security program within the Marine Corps and applies to all Marine Corps commands. This Order further:

(a) Identifies that the Commandant of the Marine Corps (CMC) is responsible for establishing and maintaining the Marine Corps Physical Security Program, to include the promulgation of appropriate and applicable directives, in accordance with reference (a).

(b) Directs commanders to support the provost marshal to ensure the physical security program is provided adequate command attention and assistance through proper staffing, retention of experienced personnel, and training.

(c) Directs and assists those responsible for physical security in their efforts to carry out the mission.

(d) Provides requirements for physical security for Marine Corps installations and organizations, as well as:

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

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

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

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

(e) 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.

(f) Installation commanders/commanding officers are responsible for physical security within their commands.

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

(h) 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 accordance with the commanding officer's guidance and in coordination with the provost marshal.

b. Subordinate Element Missions

(1) Deputy Commandant, Plans, Policies, and Operations (PP&O) (DC PP&O). The DC PP&O is responsible for the Marine Corps Physical Security Program. The DC PP&O serves as the Service level point of contact for coordination, development, and execution of Marine Corps Physical Security policies.

Director, Security Division. The Director, Security Division (PS) is responsible to the DC PP&O for providing direction, supervising development, articulating emerging concepts and advocating Marine Corps capabilities for issues pertaining to Marine Corps physical security efforts. In this capacity, the Director, Security Division (PS) will:

(a) Exercise overall staff cognizance for matters relating to physical security.

05 Jun 09

(b) Develop Marine Corps physical security policy and oversee its execution.

(c) Coordinate with the Deputy Commandant Installations and Logistics (DC I&L) and Commander, Marine Corps Systems Command (COMMARCORSYSCOM) for physical security of Arms, Ammunition, and Explosives (AA&E) in accordance with reference (b).

(d) Provide policy, guidance, and assistance to commanders to enable them to develop and maintain effective physical security programs.

(e) Manage a program to assess the level of security afforded installations and assets, and develop plans for security upgrades.

(f) Coordinate with the Deputy Commandant Programs and Resources (DC P&R) for all funding in support of physical security programs and initiatives.

(g) Ensure a review of all Military Construction (MILCON) projects is coordinated with the DC I&L and DC P&R. This review serves to ensure that physical security, AT, and FP measures and costs are identified at the installation and incorporated in MILCON cost estimates.

(h) Direct the Marine Corps Physical Security Program.

(i) Plan, program, and budget requisite resources in support of the Marine Corps Physical Security initiatives to include:

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

2. Installation Physical Security Site Assistance Visits.

3. Physical Security Upgrade Projects.

(j) Provide applicable updates to the Inspector General of the Marine Corps (IGMC) Automated Inspection Reporting System (AIRS) checklist, pertaining to physical security, in support of the Command Inspection Program.

05 Jun 09

(k) Represent Marine Corps interests in physical security related working groups.

(l) Serve as the exception and waiver authority for AA&E physical security deficiencies

(2) Deputy Commandant, Installations and Logistics (DC I&L)

(a) Develop policy for installation master planning that factor in and documents physical security requirements.

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

(c) Coordinate review of all Physical Security Upgrade Project (PSUP) funding requests with DC PP&O (PS).

(d) Coordinate with Naval Facilities Engineering Command (NAVFACENGCOM) to ensure that all physical security, AT, and FP measures are included in the design and construction of Marine Corps facilities, as applicable.

(e) Provide requirements to support physical security of ordnance material.

(3) Commander, Marine Forces (COMMARFOR). The Commander of U.S. Marine Corps Forces Africa, Command, Central, Europe, Korea, North, Pacific, Reserves, and South, (COMMARFORAF, COMMARFORCOM, COMMARFORCENT, COMMARFOREUR, COMMARFORKOR, COMMARFORNORTH, COMMARFORPAC, COMMARFORRES, and COMARFORSOUTH respectively) will ensure that all requirements of this Order are executed within their headquarters, subordinate commands, and area of responsibility (AOR). COMMARFORS will serve as the exception and waiver authority for crime prevention and physical security deficiencies not relating to AA&E.

(4) Inspector General of the Marine Corps (IGMC)

(a) Coordinate with the Director, Security Division (PS) regarding the integration of the provisions of this Order in the AIRS checklist.

(b) Coordinate Command Inspection Program support with the Director, Security Division (PS).

05 Jun 09

(5) 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. Installation commanders will implement, execute, and administer requirements of this Order. In this effort, the installation commander will:

(a) Establish and maintain an installation physical security program that encompasses requirements outlined in this Order.

(b) Draft and maintain an installation physical security plan as part of the installation AT Plan.

(c) Appoint the provost marshal, in writing, as the staff officer responsible for security and law enforcement matters in accordance with this Order.

(d) Publish an annual consolidated list of all restricted areas aboard the installation, including all tenant command restricted areas. Figures 7-1 and 7-2 are available to assist commanders in prioritizing asset protection efforts.

(e) Integrate security efforts to ensure continuity in providing an effective installation physical security program and posture.

(f) Establish and maintain an installation Physical Security Council (PSC).

(g) Review, endorse, and forward, via the chain of command, to higher headquarters, all requests for exceptions and waivers. Ensure that the provost marshal provides comments to all exception/waiver requests concerning the impact to the overall installation security posture.

(h) Report Missing, Lost, Stolen, and Recovered (MLSR) reportable items, via the chain of command, to CMC (PS/LPC).

(i) Review, endorse, and forward, via the chain of command, to higher headquarters, all request for physical security related funding.

05 Jun 09

(j) Incorporate subordinate and tenant organization physical security plans in the installation physical security plan.

(k) Coordinate Flight Line Security (FLS) measures and procedures with Marine Corps Air Station, Marine Corps Air Facility, and Marine Air Wing (MAW) commanders, as applicable.

(l) Ensure that substantial command-wide emphasis is placed on the security of AA&E.

(m) Establish and maintain an installation-wide crime prevention program.

(n) Provide policy and guidance to installation and tenant commands, including commercial carriers and contractors regarding the control, storage, and transportation of personal weapons and ammunition aboard the installation in accordance with reference (b).

(o) Maintain an installation-wide barrier plan in support of the physical security program. Ensure all command and tenant activity plans are included.

(p) Assign the provost marshal as the primary coordinator for all flight line security matters.

(q) Develop installation master plans that incorporate appropriate AT, FP, and physical security requirements.

(r) Ensure all installation MILCON projects address, incorporate, and integrate AT, FP, and physical security requirements. MILCON project must include infrastructure requirements.

(s) Budget for base security and identify funding shortfalls to the comptroller for appropriate action.

(t) Notify Security Division (PS), via chain of command, when planned construction or upgrades require modification to existing MCESS.

(6) Marine Corps Air Facility (MCAF) and Marine Corps Air Station (MCAS) Commanders. MCAS commanders, designated as an installation commander, are required to carry out those

05 Jun 09

function listed in paragraph (6). However, there are air stations and air facilities located within the confines of a Marine Corps Base that must address additional security requirements. MCAS and MCAF commanders will:

(a) Coordinate aircraft and FLS measures with MAW headquarters components, installation commanders and provost marshals/security officers.

(b) Approve all plans for restricted areas within or adjacent to flight lines. This information will be forwarded to the installation commander (where applicable) for inclusion in the installation restricted area list.

(c) Notify the provost marshal of planned aircraft parking areas, to include transient aircraft, and any changes to the parking areas, in order for physical security requirements to be coordinated.

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

(e) Coordinate and approve plans for flight line Entry Control Facilities (ECF) and Access Control Points (ACP). Include policy concerning runway use by security and safety personnel.

(f) Procure, install, and maintain physical barriers (automated, portable, fences, etc.) to deter, delay, and deny entry to unauthorized persons to flight line restricted areas.

(g) Incorporate FLS issues in the facility or station physical security plan and ensure the plan is included in the installation physical security plan (where applicable).

(h) Address FLS issues at MCAF/MCAS or installation Physical Security Council meetings.

(i) Notify Security Division (PS), via chain of command, when planned construction or upgrades require modification to existing MCESS.

(j) Coordinate off installation, downed aircraft security requirements and support procedures with the MAW component commander, provost marshal and installation commander (where applicable).

(k) Coordinate and provide security, as required, when and where Marine Corps assets are staged and/or stored in an off-installation location.

(l) Review, endorse, and forward, via the chain of command, all requests for physical security exceptions and waivers. All requests will contain an endorsement, or comments from the provost marshal, concerning the impact to the installation/facility security posture. Where applicable, forward to the installation commander for review/comment.

(m) Review, endorse, and forward, via the chain of command, all requests for physical security related funding.

(n) Draft and maintain a physical security plan and ensure it is included in the installation AT plan.

(o) Assign a command security officer as the primary coordinator for flight line security matters.

(p) Budget for adequate base security and identify funding shortfalls to the comptroller for appropriate action.

(7) Commanding Officer (CO)(Battalion/Squadron and higher). Commanding officers are responsible for physical security within his/her organization. Commanding officers will:

(a) Establish and maintain a command physical security program that encompasses requirements of this Order.

(b) Appoint a command security officer in writing. Provide sufficient resources, staff assistance, and authority to implement, manage, and execute an effective physical security program.

(c) Identify, in writing, all designated restricted areas within the command and provide the information, in writing, to the provost marshal annually. Commanding officers of MARFORRES sites will identify, in writing, and maintain a copy of all restricted areas under their cognizance.

(d) Report Missing, Lost, Stolen, and Recovered reportable items, via the chain of command, to CMC(PS/LPC) and ensure that a copy of the MLSR report is provided to the installation Provost Marshal's Office (PMO).

05 Jun 09

(e) Ensure that there is a strong, viable and visible command emphasis with regard to the security of AA&E.

(f) Ensure that all personnel who account for, maintain, dispose of, distribute, and provide security for AA&E, are screened in accordance with this order and reference (b).

(g) Designate, in writing, an AA&E officer who will be responsible for all AA&E accountability and security matters.

(h) Develop and maintain an organization barrier plan in support of the installation barrier plan.

(i) Ensure that all AA&E is accounted for, inventoried, maintained, and reported in accordance with this Order.

(8) Provost Marshal (PM). The provost marshal serves as the staff officer responsible for coordinating physical security and law enforcement programs. The provost marshal is responsible for ensuring that these programs complement the overall installation security effort. In this capacity, the provost marshal will:

(a) Conduct law enforcement operations and crime prevention efforts in support of the physical security program, including measures to enhance security during periods of increased threat and crisis situations.

(b) Determine the adequacy of the installation physical security posture with a physical security survey program.

(c) Maintain liaison with installation and/or regional Naval Criminal Investigative Service (NCIS) personnel in support of criminal investigations.

(d) Maintain liaison with federal, state, local, other military activities, and host nation officials regarding law enforcement/physical security concerns.

(e) Provide commanders with technical assistance and recommend equipment, procedures, and methods to enhance physical security.

05 Jun 09

(f) Support the installation commander in developing and maintaining a comprehensive Physical Security Plan.

(g) Coordinate and support the PSC.

(h) Review, comment, and ensure the implementation of compensatory measures, and endorse all requests for physical security waivers and exceptions from command and tenant organizations.

(i) Ensure physical security programs complement FP, AT, Critical Infrastructure Protection (CIP), Chemical Biological, Radiological, Nuclear, and high-yield explosives (CBRNE), Safety, Fire, and Crime Prevention programs.

(j) Supervise the operation of, and coordinate all efforts regarding, the Security Division (PS) centrally managed MCESS aboard the installation.

(k) Assist command/organization security officers in physical security, FP, CIP, AT, and crime prevention efforts.

(l) Supervise the FLS program.

(m) Maintain the FLS access database and issue badges.

(n) Publish an FLS order.

(o) Assign patrol zones in and around flight lines.

(p) Screen and train non-military police personnel assigned to augment the FLS program prior to assignment.

(q) Coordinate off installation, downed aircraft security requirements and support procedures with the MAW commander and installation commander.

(r) Investigate MLSR incidents when appropriate and refer to NCIS for investigation, as required.

(s) Publish and staff a recommended installation restricted areas list to the installation commander, no later than 31 February, annually.

(t) Ensure that all personnel within the Provost

Marshal's Office who account for, maintain, dispose of, distribute, and provide security for AA&E, are screened in accordance with this Order and reference (b).

(u) Publish and maintain security force orders, to include post specific orders. Update and review the orders on an annual basis.

(v) Coordinate and maintain a robust crime prevention program that includes:

1. Supervision for the conduct of crime prevention surveys for installation organization.

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. Reporting annual crime statistics to the installation commander and Security Division (PS).

4. Supporting the Commander's Welcome Aboard Brief.

5. Provide unit crime prevention briefs as requested.

6. Establishment and maintenance of a Lost and Found Property Program in accordance with reference (c).

(w) Review all plans for facility construction or modification and provide comments as required.

(x) Support commands in establishing and updating barrier plans.

(9) Physical Security Chief. The physical security chief serves as the provost marshal's resident protection professional. The physical security chief is responsible for establishing, implementing, and managing the installation physical security and loss prevention programs. In this capacity, the physical security chief will:

(a) Supervise the Provost Marshal's Physical Security Section.

(b) Support the provost marshal by establishing, implementing, and maintaining:

1. 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 safeguard against acts of terrorism, espionage, sabotage, damage, and theft.

2. Crime and loss prevention programs that increase personal safety, protect government and personal property from theft, misuse and unlawful destruction. In this effort, focus on reduction of manpower, time, and cost expended by the government in the investigation, pursuit, and prosecution of criminal activities.

3. Procedures for timely submission of required reports.

(c) Act as the manager and systems administrator for the Security Division (PS) centrally managed MCESS aboard the installation.

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

2. Coordinate, assist, and ensure that all required MCESS training is conducted.

(d) Assist tenant commands in physical security related training.

(e) Ensure physical security programs encompass the security efforts of tenant activities.

(f) Ensure tenant activities have security programs that complement the overall installation security effort.

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

(h) Ensure that the installation Public Affairs Office (PAO) is provided crime prevention media on a monthly

basis for release in the installation paper or other media sources.

(i) Ensure that installation crime statistics are maintained in order to identify trends and areas of increased criminal activity.

(j) Conduct unit level crime prevention briefs as directed.

(k) Conduct crime prevention and community relation programs as directed by the provost marshal.

(l) Review all plans for facility construction or modification and provide physical security, AT, and crime prevention comments as required.

(m) Assist commands in planning and carrying out barrier plans.

(10) Command/Organization Security Officer. The command/organization security officer serves as the focal point for command physical security matters and will report directly to the commanding officer in matters pertaining to physical security. Security officers will be appointed in writing by the commanding officer. In the performance of their duties, security officers will:

(a) Plan, manage, implement, and direct the organization's physical security program.

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

(c) Develop, implement, and maintain an organization physical security plan to support the host installation AT plan.

(d) Develop and maintain a security education program.

(e) Identify assets (property and structures) requiring protection by priority and location. Particular

basis for release in the installation paper or other media sources.

(i) Ensure that installation crime statistics are maintained in order to identify trends and areas of increased criminal activity.

(j) Conduct unit level crime prevention briefs as directed.

(k) Conduct crime prevention and community relation programs as directed by the provost marshal.

(l) Review all plans for facility construction or modification and provide physical security, AT, and crime prevention comments as required.

(m) Assist commands in planning and carrying out barrier plans.

(10) Command/Organization Security Officer. The command/organization security officer serves as the focal point for command physical security matters and will report directly to the commanding officer in matters pertaining to physical security. Security officers will be appointed in writing by the commanding officer. In the performance of their duties, security officers will:

(a) Plan, manage, implement, and direct the organization's physical security program.

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

(c) Develop, implement, and maintain an organization physical security plan to support the host installation AT plan.

(d) Develop and maintain a security education program.

(e) Identify assets (property and structures) requiring protection by priority and location. Particular

05 Jun 09

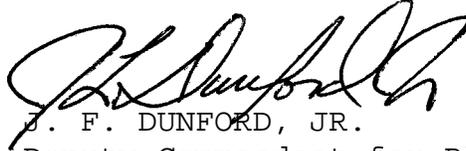
(11) In addition to the requirements identified above, commanding officers of Marine Corps organizations not located aboard Marine Corps installations will ensure that all requirements of this Order are established and maintained, as applicable and appropriate. Commanding officers will coordinate physical security requirements and support with the host and higher headquarters.

5. Administration and Logistics. Recommendations for changes to this Order are encouraged. All recommendations will be forwarded via the chain of command to the Commandant of the Marine Corps, Security Division (PS).

6. Command and Signal

a. Command. This Order is applicable to the Marine Corps Total Force.

b. Signal. This Order is effective the date signed.



J. F. DUNFORD, JR.
Deputy Commandant for Plans,
Policies and Operations

DISTRIBUTION: PCN 10208597900

COPY TO: 7000260 (1)
8145004 (2)

MCO 5530.14A
05 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

MCO 5530.14A
05 Jun 09

LOCATOR SHEET

Subj: MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

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

RECORD OF CHANGES

Log completed change action as indicated.

| Change Number | Date of Change | Date Entered | Signature of Person Incorporating Change |
|---------------|----------------|--------------|--|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

TABLE OF CONTENTS

CHAPTER

| | |
|----|--|
| 1 | INTRODUCTION |
| 2 | SECURITY PLANNING |
| 3 | SECURITY MEASURES |
| 4 | SECURITY FORCES |
| 5 | BARRIERS AND OPENINGS |
| 6 | ELECTRONIC SECURITY SYSTEMS |
| 7 | CRITICAL ASSET PROTECTION |
| 8 | SECURITY OF ARMS, AMMUNITION, AND EXPLOSIVES (AA&E) |
| 9 | CRIME PREVENTION |
| 10 | REPORTING REQUIRMENTS |
| 11 | EXPEDITIONARY PHYSICAL SECURITY |

APPENDIX

| | |
|---|--|
| A | DEFINITIONS |
| B | ACRONYMS |
| C | WAIVER AND EXCEPTION REQUEST FORMAT |
| D | PHYSICAL SECURITY PLAN (FORMAT) |
| E | PHYSICAL SECURITY SURVEY FORM (NAVMC 11121) (EXAMPLE) |
| F | INSTRUCTIONS FOR PREPARATION, COMPLETION, AND DISTRIBUTION OF A PHYSICAL SECURITY SURVEY |
| G | KEY AND LOCK CONTROL FORMS |

| | |
|---|--|
| H | SECURITY RISK CATEGORIES |
| I | AA&E SCREENING PACKAGE |
| J | AA&E FACILITY MINIMUM CONSTRUCTION REQUIREMENTS |
| K | AA&E SURVEILLANCE REQUIREMENTS |
| L | MLSR AA&E REPORTABLE QUANTITIES |
| M | MISSING, LOST, STOLEN AND RECOVERED (MLSR) PREPARATION GUIDE |
| N | INSTRUCTIONS FOR COMPLETING THE LAW ENFORCEMENT AND PHYSICAL SECURITY ACTIVITY REPORT (LEPSAR) |

FIGURES

| | |
|-----|---|
| 2-1 | MARINE CORPS PHYSICAL SECURITY CREDENTIAL |
| 2-2 | EXAPMPLE REQUEST FOR ISSUANCE OF PHYSICAL SECURITY CREDENTIALS |
| 2-3 | EXAMPLE ACKNOWLEDGEMENT OF RECEIPT OF PHYSICAL SECURITY CREDENTIALS |
| 2-4 | RISK MANAGEMENT PROCESS |
| 3-1 | LIGHTING SPECIFICATIONS |
| 3-2 | ILLUMINATED AREA SPECIFICATIONS |
| 5-1 | SECURITY BARRIERS AND FUNCTIONALITY |
| 5-2 | EXAMPLE AUTHORIZED PERSONNEL/VISITORS ECF |
| 5-3 | EXAMPLE COMMERCIAL TRAFFIC ECF |
| 5-4 | ECF ZONES |
| 5-5 | EXAMPLE HINGE PROTECTION |
| 7-1 | RESOURCE AND ASSET PRIORITIZATION CHART |

| | |
|------|---------------------------------------|
| 7-2 | PHYSICAL SECURITY THREAT MATRIX |
| 7-3 | LIMITED WATERWAY AREAS |
| 7-4 | WATERSIDE SECURITY ZONES |
| 7-5 | COMBINATION LOCK REPLACEMENT PRIORITY |
| 8-1 | ARMORY DAY GATE |
| 8-2 | TUFLOC DOOR LOCK |
| 10-1 | EXAMPLE MLSR REPORT |

MCO 5530.14A
05 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 1

INTRODUCTION

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|---|------------------|-------------|
| GENERAL | 1000 | 1-3 |
| THE SECURITY CHALLENGE | 1001 | 1-4 |
| MARINE CORPS PHYSICAL SECURITY PROGRAM . | 1002 | 1-5 |
| SECURITY OF MARINE CORPS INSTALLATIONS AND RESOURCES | 1003 | 1-6 |
| SECURITY RESPONSIBILITIES | 1004 | 1-6 |
| PHYSICAL SECURITY OF ORGANIZATIONS NOT LOCATED ABOARD MARINE CORPS INSTALLATIONS | 1005 | 1-6 |
| PHYSICAL SECURITY OF TENANT AND CIVILIAN AGENCIES/ORGANIZATIONS ABOARD MARINE CORPS INSTALLATIONS | 1006 | 1-7 |
| PHYSICAL SECURITY COUNCIL | 1007 | 1-7 |
| EXCEPTIONS AND WAIVERS | 1008 | 1-8 |
| HOST NATION CONFLICT | 1009 | 1-10 |
| PROJECT PLANNING | 1010 | 1-10 |
| PHYSICAL SECURITY UPGRADE PROJECTS (PSUP) PROGRAM | 1011 | 1-11 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 1

INTRODUCTION

1000. GENERAL. Physical security is the utilization of active and passive security measures and management protocol that are designed to prevent unauthorized access to personnel, equipment, material, documents, and safeguards against espionage, sabotage, acts of terrorism, damage, and theft. Physical security is an integral part of all Force Protection (FP), Antiterrorism (AT), Critical Infrastructure Protection (CIP), Safety, Fire, Chemical, Biological, Radiological, Nuclear, (high yield) Explosives (CBRNE)), and crime prevention programs.

1. This Order provides guidelines for the application of physical security programs for Marine Corps commands and installations. Physical security guidelines are applicable to Marine Corps organizations not located aboard a Marine Corps installation, and tenant and civilian agencies/organizations aboard Marine Corps installations. Applicable definitions and acronyms are contained in Appendix A and B, respectively. This Order further:

a. Expands on responsibilities and discusses various security vulnerabilities, details protective measures, and identifies management actions that must be employed to provide and sustain an acceptable physical security posture.

b. Establishes uniform physical security requirements. The language separates recommended physical security measures from required measures and eliminates conflicting guidance.

c. Identifies physical security requirements not covered by other specialized security programs, or issues more stringent guidelines. Protection of classified material, information assurance security, and nuclear weapons security are specifically addressed in references (d) through (g), respectively. Those requirements augment the basic guidance contained in this Order.

d. Establishes 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 (a).

1001. THE SECURITY CHALLENGE

1. Protection of personnel and property is accomplished by:

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. There are a number of factors involved in the security challenge. The geographic location, size, type, jurisdiction, and mission of an identified property form a basis for security requirements. Procedures, plans, policies, and agreements directly impact security. Physical security systems, resources and measures assist in safeguarding personnel, protection of property, and preventing loss. All of these factors must be addressed in forming a physical security program. The physical security program is concerned with means and measures designed to achieve a sound physical security posture; thereby, allowing installation AT and FP goals to be achieved more easily. 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 and criminal 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. It is imperative that commands assign security officers to address physical security

issues. Security officers will use the guidance and policies contained in this Order and reference (a), in determining security and/or protective measures deemed essential for their particular spaces, areas and/or buildings.

4. Military activities located within leased space facilities have unique challenges in addressing physical security issues (commercial firms/contractors located in same building(s), public facilities, shared entranceways and common spaces, etc.). Liaison with appropriate authorities (General Services Administration (GSA), building administrators, lessors, etc.) is essential to outline security measures necessary for protection of lives and property, tailored to the individual characteristics of the leased space. Commands located within leased facilities will ensure that security is properly addressed in all lease agreements. Requirements outlined in this Order, references (a) and (h) through (j), will be thoroughly addressed and annotated in all lease agreements.

1002. MARINE CORPS PHYSICAL SECURITY PROGRAM. Physical Security is the foundation of, and an integral part of all force protection (AT, CIP, Fire, Safety, CBRNE) and crime prevention programs. While the other security programs rely heavily on physical security for success, the success of the physical security program does not depend on any other security program. Physical security specialists are requisite experts in the area of AT, CIP, FP, and crime prevention.

1. Commanders must place emphasis on ensuring that the Provost Marshal provides adequate support to the physical security program through proper staffing, retention of personnel, training, and continued education.

2. Marine Corps physical security specialists serve as the combatant commander's and installation commander's resident subject matter expert in the ambit of physical security and crime/loss prevention. The physical security chief serves as the resident protection professional responsible for establishing, implementing, and managing the physical security and crime/loss prevention programs. Physical security personnel provide commanders:

a. Risk management and mitigation skills necessary to conduct a risk analysis of an asset, facility, area, and provide the commander with a defense in depth approach against all identified and perceived threats.

5 Jun 09

b. A working knowledge of physical security equipment, to include functionality, application, sustainability, in both expeditionary and garrison environments.

c. Best practice principles and equipment that focus on Reducing manpower, time, and cost expended by the government.

d. Expertise in integrating physical security planning, requirements, procedures, and equipment in all FP and AT efforts.

1003. SECURITY OF MARINE CORPS INSTALLATIONS AND RESOURCES. Installation commanders are authorized to issue regulations for the protection and security of property and places under their command pursuant to the provisions of reference (a), 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 (a) provides penalties for violations of such regulations or orders as have been promulgated or approved by the installation commander for the protection and security of DOD property or places.

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

3. Particular attention and effort will be afforded to those areas/assets involving national security and assets not involving national security but inherently dangerous to others.

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

1004. SECURITY RESPONSIBILITIES. Security is the direct responsibility of all Marines, Sailors, and civilian employees.

1005. PHYSICAL SECURITY OF ORGANIZATIONS NOT LOCATED ABOARD MARINE CORPS INSTALLATIONS. Commanders of Marine Corps organizations not located aboard a Marine Corps installation are required to establish and maintain a physical security program. Organizations located aboard other DOD service/agency sites will coordinate physical security requirements with the host. Host service/agency requirements will impact security requirements,

however all Marine Corps organizations must ensure that the following is accomplished in accordance with this Order:

- a. Establish a command physical security program.
- b. Appoint a command security officer in writing.
- c. Establish a command physical security survey program per paragraph 3001.
- d. Marine Corps organizations will establish an Inter-Service Support Agreement (ISSA), Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) with the host service that address physical security issues, as directed by higher headquarters. Organizations located in foreign countries must ensure that physical security issues are addressed in Status of Forces Agreements (SOFA) or Host Nation (HN) agreements. Topics to be addressed include property boundaries, Intrusion Detection System (IDS) monitoring, available response forces, deadly force training and issues, physical security support, etc. The Commanding officer is required to coordinate all such agreements through higher headquarters, to include Staff Judge Advocate (SJA) and/or legal offices.

1006. 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/ISSA, where applicable and as directed, with tenant and civilian agencies that incorporate or recognize a physical security survey program. Commanders of installations located in foreign countries must ensure that physical security issues are addressed in SOFA or HN agreements, as applicable, with foreign tenant and civilian agencies. All agreements will be coordinated with all special staff offices, particularly the SJA and/or Legal Office. Tenant organizations will be made aware of all installation physical security initiatives to include the Physical Security Council (PSC), AT contingency drills, and other initiatives that affect the installation or organization.

1007. PHYSICAL SECURITY COUNCIL. Installation commanders will establish, in writing, a physical security council that will meet on a quarterly basis. The PSC may be combined with the AT Working Group (ATWG) to alleviate any duplication of effort. The PSC assist commanders in coordinating and implementing

initiatives that support the installation's physical security, FP, CIP, and AT programs. The PSC provides a means for the commander to gain maximum participation from organizations throughout the installation in support of physical security interests. The installation commander or a designated representative will chair the PSC.

1. The PSC will consist of those personnel who are most suited to materially assist the installation commander in the physical security effort. Examples of personnel who must attend are the provost marshal, operations officer, facilities officer, comptroller, SJA representative, and others as designated by the commander.

2. PSC subject matter is focused on, but not limited to, the installation's physical security, FP, CIP, and AT posture. The council will conduct a review of physical security, FP, CIP, and AT deficiencies and recommend corrective action, that may include fiscal and/or logistical solutions. Physical security challenges, especially those emanating from DOD minimum standards for AT, requiring facility/infrastructure projects will be documented (for the short, intermediate, and/or long term) and incorporated into installation master planning updates.

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. Minutes will be maintained on file for a period of three years.

5. Physical Security Working Group (PSWG). The PSWG will include a representative from the installation Physical Security section, facilities, comptroller, and the ATO. The PSWG is responsible for research and action on those issues requiring action as designated by the physical security council. The PSWG should meet as often as necessary to address project matters, but will meet at least twice a year. The PSWG will report all findings to the PSC.

1008. EXCEPTIONS AND WAIVERS. Exceptions and waivers serve to permit deviations from requirements of this Order. Security Division (PS) serves as the sole authority for exceptions and waivers to physical security requirements of Arms, Ammunition,

and Explosives (AA&E) of reference (b) and this Order. COMMARFORS serve as the exception/waiver authority for all other physical security and crime prevention requirements, unless otherwise identified herein. Exceptions, waivers, or extension requests will be assigned an exception or waiver number, and completed in the Naval Letter format outlined in Appendix C.

1. All requests for waivers or exceptions will contain an organization plan of action and milestones (POA&M).
2. Non-applicable elements shall be noted as N/A.
3. Requests will contain an analysis of the problem and a detailed description of compensatory security measures that the commanding officer has implemented.
4. All requests will be staffed through the installation provost marshal. The provost marshal is responsible for endorsing all requests and ensuring the most recent physical security survey for that facility is attached. Additionally, the provost marshal will identify if and/or how the exception or waiver impacts or may impact the overall installation security posture.
5. Exception or waiver requests will be forwarded via the chain of command, including the installation commander, for comment, to the appropriate COMMARFOR for approval/disapproval.
6. Requests for an exception or waiver to an AA&E deficiency will be forward via the chain of command, including the installation Commander and cognizant COMMARFOR, to Security Division (PS) for approval/disapproval.
7. Exceptions are granted for three years when corrective action of a security deficiency is beyond the capability of the organization, or the condition necessitating the request cannot be corrected in the near-term. Waivers are granted for a one-year period when corrective action of a security deficiency may be accomplished by the organization in the near-term.
8. Permanent (long term/greater than 3 years) exceptions will not be granted.
9. Blanket (listing several different facilities which have the same deficiencies) exceptions or waivers will not be granted.

5 Jun 09

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

11. Exceptions and waivers are self-canceling at the end of the allocated time. Requests for an extension will be submitted prior to the date of expiration, and will be staffed in the same manner as the original request.

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

13. Waivers or Exceptions will not be granted for new construction, MILCON, or renovations exceeding the fifty percent threshold with the exception of facilities listed on the Historical Registry.

1009. HOST NATION CONFLICT. Organizations located outside of the United States may not be able to implement certain requirements of this Order. In those instances, commanders must address physical security requirements and compensatory measures in a SOFA or HN Agreement.

1010. PROJECT PLANNING. All plans for construction, MILCON, and facility sustainment, repair, and modernization (FSRM) must incorporate physical security, AT, and FP features, in accordance with references (a), (h) through (j), and (k) and (l).

1. All plans for MILCON and FSRM construction must be reviewed by the Provost Marshal or designated representative, and the installation Security Officer during the design process, all subsequent design review phases, and the final (100%) drawings.

2. All construction projects, to include MILCON and FSRM projects will be reviewed by the installation physical security chief and Antiterrorism Officer (ATO) and verified by Security Division (PS) and CMC(I&L) during validation, to ensure physical security and force protection requirements have been addressed.

3. Contract for bid will not be processed without documentation of design review by security and AT representatives.

4. In those instances where construction projects require

Electronic Security Systems (ESS), (including Intrusion Detection, Mass Notification Systems (MNS), Closed Circuit Television (CCTV), etc.) commands must ensure that the installation physical security chief forwards a request for support and/or cost estimates to Security Division (PS). This will provide notification of a requirement and allow sufficient time for planning and funding. Security Division (PS) manages a centrally funded program that provides security services and equipment to the installations. These systems and equipment are considered collateral equipment and cannot be funded with MILCON funds but can be included in the MILCON project contract for contracting efficiency provided the funding is separate and distinct from MILCON funds.

5. Commands must ensure that infrastructure requirements are coordinated with and reviewed by installation communications and information management and public works offices.

1011. PHYSICAL SECURITY UPGRADE PROJECTS (PSUP) PROGRAM

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

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), via the chain of command, in accordance with the procedures outlined in reference (k). Once received at CMC(LFF-2), the project will be reviewed and validated by Security Division (PS) and CMC(LFF-2) and will compete for funding against security projects initiated throughout the Marine Corps. Approved projects 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 submit 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 references (k) and (l).

3. The status of PSUP projects can be reviewed on line via the Facilities Integration Website at <https://www.hqmc-facilities.org/>. Any questions or concerns must be properly routed through the appropriate chain of command, to include the MARFOR, Marine Corps Installation (MCI), and HQMC (I&L and PS).

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 2

SECURITY PLANNING

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|---|------------------|-------------|
| GENERAL | 2000 | 2-3 |
| PHYSICAL SECURITY CREDENTIALS | 2001 | 2-3 |
| PHYSICAL SECURITY PLAN | 2002 | 2-6 |
| RISK MANAGEMENT | 2003 | 2-7 |
| COST OF SECURITY | 2004 | 2-12 |
| COORDINATION | 2005 | 2-13 |
| SECURITY CONSIDERATIONS | 2006 | 2-13 |
| SECURITY EDUCATION AND TRAINING | 2007 | 2-13 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

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 Plan. Tenant activity physical security plans will be submitted to the installation Provost Marshal to be integrated into the installation plan. Classification of the plan will be established per reference (d). Further guidance on physical security plans is available in paragraph 2002.

2001. PHYSICAL SECURITY CREDENTIALS. In the performance of their assigned duties, physical security specialists, both military and civilian, must be permitted access to all designated restricted areas and other facilities containing critical assets. Physical security specialists will possess an official means to identify themselves to unit commanders with facilities/areas requiring physical security support as prescribed herein. Security Division (PS) will issue physical security credentials to school-trained military police and civilians assigned to the provost marshal's physical security Section performing the duties of a physical security specialist. An example of the official credentials is provided in figure 2-1.

1. Security Division (PS) will maintain strict accountability of Marine Corps physical security inspector credentials by central issuance.

2. Prior to requesting credentials, installation provost marshals must certify that the individual meets each of the following criteria:

a. Successful completion of the U.S. Army Conventional Physical Security Course, the Federal Law Enforcement Training Center (FLETC) Physical Security Course, or a Physical Security Professional (PSP) Certificate from ASIS International.

b. Entry of a course completion certificate into the Service Record Book (SRB), and assignment of the additional Military Occupational Specialty (MOS) 5814 (military personnel only).

c. Assignment to the physical security unit, and performing the duties of a physical security specialist.

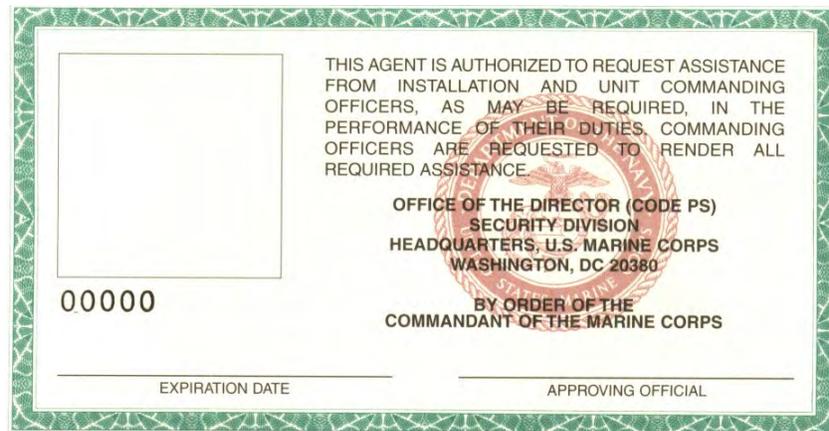
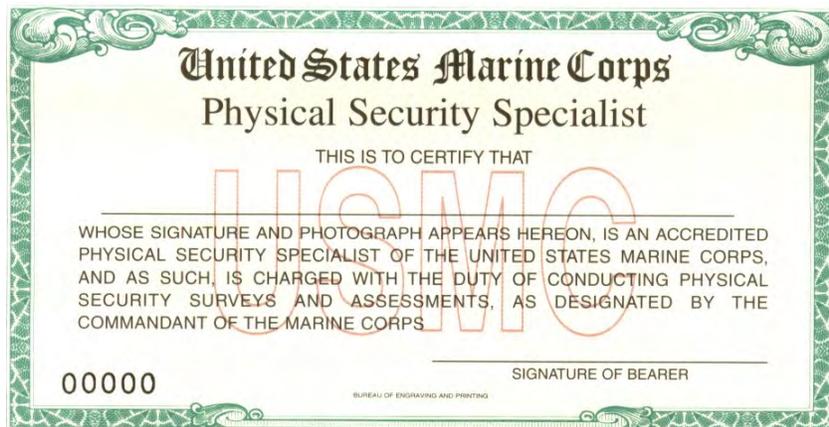


Figure 2-1.--Marine Corps Physical Security Credential

2. Installation provost marshals will request physical security credential issuance in the format prescribed in figure 2-2. Each individual requiring credentials will enclose a passport identification photograph, approximately 1-1/4 inches square, and a copy of the following certificates with each request.

a. U.S. Army Conventional Physical Security Course Completion Certificate (military or civilian).

b. FLETC Physical Security Course Completion Certificate.

c. ASIS International Physical Security Professional Certificate.

| UNIT HEADING | | | | |
|---|-------------|-----------------------|---------------|--------------------------|
| | | | | 5530 Org Code Date |
| From: Provost Marshal, (Base or Station) | | | | |
| To: Commandant of the Marine Corps (PSM) | | | | |
| Subj: REQUEST FOR ISSUANCE OF PHYSICAL SECURITY SPECIALIST CREDENTIALS | | | | |
| Ref: (a) MCO 5530.14A | | | | |
| Encl: (1) U.S. Army Conventional Physical Security Course Completion Certificate, Federal Law Enforcement Training Center Certificate or ASIS Certificate (2) Passport Photo | | | | |
| 1. In accordance with the reference, it is requested that physical security credentials be issued for the following personnel: | | | | |
| <u>NAME</u> | <u>RANK</u> | <u>LAST 4 SSN/MOS</u> | <u>BILLET</u> | <u>SCTY CLNC</u> |
| | | | | |
| 2. Personnel identified above have successfully completed the required training, as identified in reference (a). Enclosure (1) is provided to document subject named individuals attendance at the required course of instruction. Enclosure (2) is provided as directed. | | | | |
| 3. Upon completion of physical security duties and responsibilities or reassignment, credentials will be returned to the Commandant of the Marine Corps (PSM) for voidance. | | | | |
| 4. Point of contact information | | | | |
| | | | | |
| SIGNATURE | | | | |

Figure 2-2.--Example Request for Issuance of Physical Security Credentials

3. Upon receipt of credentials, an acknowledgement of responsibilities, figure 2-3, will be completed. This document will be promptly returned to Security Division (PS).

4. It is the responsibility of the provost marshal and physical security chief to ensure that credentials are returned to Security Division (PS) for voidance when individuals are no longer assigned to the physical security unit or performing the duties of a physical security specialist.

| UNIT HEADING | |
|--|--------------------------|
| | 5530 Org Code Date |
| From: Rank, Full Name, Last 4 SSN/MOS, Duty Station To: Commandant of the Marine Corps (PSM) | |
| Subj: RECEIPT OF PHYSICAL SECURITY SPECIALIST CREDENTIALS | |
| Ref: (a) MCO 5530.14A | |
| 1. I hereby acknowledge receipt of Marine Corps Physical Security Credentials, serial number _____ . I agree to safeguard these credentials and prevent their loss or misuse. | |
| 2. I understand that the credentials are to be used only in the performance of official duties and that under no circumstance will they be used for personal use. | |
| 3. I understand that the credentials are the property of the U. S. Marine Corps. Upon completion of physical security duties and responsibilities, or reassignment, the credentials will be returned to the Commandant of the Marine Corps (PSM) for voidance. | |
| SIGNATURE | |

Figure 2-3.—Example Acknowledgement of Receipt of Physical Security Credentials

2002. PHYSICAL SECURITY PLAN. A model physical security plan format is provided in Appendix D. The intent of the plan is to clearly identify how the installation/activity conducts day-to-day security as well as how it responds to security incidents. The plan will reflect the detailed implementation of Marine Corps policy at the installation/activity and should not be philosophical or a verbatim reiteration of this Order. The physical security plan will be included as an annex or appendix in the installation AT Plan which is detailed in reference (m). The physical security plan is not intended to replace the AT 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 plan.

2003. RISK MANAGEMENT. Risk analysis is a process used by commanders to identify, assess, and mitigate risks from operational factors, and assists in the decision making process that balances risk costs with mission accomplishment. Commanders can use the information derived from the risk analysis process to determine which assets require increased protection and where future expenditures are required to minimize risk of attack, or lessen the severity of the outcome of such an attack.

1. The fundamental goal of risk management is to enhance operational capabilities and mission accomplishment, with minimal acceptable loss.
2. Risk management assists commanders by:
 - a. Enhancing operational mission accomplishment;
 - b. Supporting a well-informed decision-making process;
 - c. Providing assessment tools to support operations;
 - d. Preserving and protecting personnel, combat weapon systems, and related support equipment, while avoiding unnecessary risk;
 - e. Identifying where feasible and effective control measures need to be implemented because specific standards do not exist.
3. Risk management does not replace sound decision making, remove risk altogether, support a zero defect mindset, justify violating the law, nor should it inhibit the commander's flexibility, initiative, or accountability.
4. Commanders should conduct an installation level risk analysis on an annual basis.
5. Principles of Risk Management. There are basic principles that must be applied when implementing the risk management process. They include:
 - a. Accept No Unnecessary Risk. The most logical choices for accomplishing a mission are those that meet all mission requirements while exposing personnel and resources to the lowest acceptable risk. Risk analysis identifies threats that

5 Jun 09

might otherwise go unidentified and provides tools to reduce or offset risk. The corollary to this axiom is "accept necessary risk" required to successfully complete the mission or task.

b. Make Risk Decisions at the Appropriate Level. The appropriate level for risk decisions is the one that can make decisions to eliminate or minimize the vulnerability to a threat, implement controls to reduce the risk, or accept the risk. Commanders at all levels must ensure that subordinates know how much risk they can accept and when to elevate the decision to a higher level. The risk management process must identify clear accountability, and ensure that risk decisions are made at the appropriate level. If during execution of the mission or task, it's determined that the controls available will not reduce risk to an acceptable level, the decision to accept risk must be elevated to the next level in the chain of command.

c. Accept Risk When Costs Outweigh the Benefits. The process of weighing risks against opportunities and benefits helps to maximize mission success. Balancing costs and benefits is a subjective process and must remain the commander's decision.

d. Anticipate and Manage Risk by Planning. Integrate risk management into planning at all levels. Commanders must dedicate time and resources to apply risk management effectively in the planning process, where risks can be more readily assessed and managed. Integrating risk management into planning as early as possible provides the greatest opportunity for making well-informed decisions and implementing effective risk control measures. During execution phases of operations, the risk management process must be applied to address previously unidentified risks while continuing to evaluate the effectiveness of existing risk control measures and modify them as required.

6. Types of Risk Analysis. There are two types of risk analysis: crisis and deliberate. Time is the basic factor that contributes to the selection of the type used.

a. Crisis. Crisis risk analysis is an "on-the-run" mental or verbal review of the situation using the basic risk analysis process. The crisis process of risk management is employed to consider risk while making decisions in a time-compressed situation. This type of risk analysis is used during the

execution phase of training or operations as well as in planning and execution during crisis responses. This type of analysis is particularly helpful for choosing the appropriate course of action when an unplanned event occurs.

b. Deliberate. Deliberate risk analysis is the application of the complete process when time is not critical. It uses experience and brainstorming to identify threats and develop controls and is most effective when done in a group.

7. Risk Analysis Elements. The risk analysis contains key elements that, when performed in sequence, systematically identify and evaluate resources, facilities, and activities in terms of various factors. The following elements must be present to determine risk. The key elements of the risk analysis are:

a. Threat Assessment. The threat assessment is used to identify threats (including, but not limited to, acts of terrorism, espionage, sabotage, wrongful destruction, malicious damage, and theft and the direct impact of each threat on resources, facilities, and activities. Threat information gathering is diverse and includes foreign intelligence, open source materials, domestic criminal information, and information from federal, state, and local authorities.

b. Criticality Assessment. This is done to determine which assets need to be protected. The criticality assessment determines the importance of each asset and its necessity to complete the mission, the effect of the threat on the asset, and the recoverability of the asset from the attack. Consideration should therefore be given to the resources that must be expended to recover an asset, repair it for return to service, or implementing contingency plans and acceptable alternatives.

c. Vulnerability Assessment. The vulnerability assessment is the process the Commander uses to determine the susceptibility of assets to attack from threats identified by the threat assessment. Vulnerabilities are always there, no matter the policies, procedures, and protective measures in place; however, the key is to mitigate asset vulnerabilities based on threat. Identifying and understanding vulnerabilities is important in determining how well an asset must be protected from loss. Vulnerabilities are the one component, in the risk assessment process, over which the commander has the most control and greatest influence.

d. Risk Assessment. Risk assessment combines the threat, criticality, and vulnerability ratings given to each asset. The risk assessment methodology is further discussed in reference (n). In order for there to be risk, each one of the elements must be present; therefore, Risk = Threat x Criticality x Vulnerability. Risk is based on the value of the asset in relation to the threat and vulnerabilities associated with it. Risk is derived by combining the relative impact of any loss or damage to an asset (Criticality) with the relative probability of an unwanted event (Threat x Vulnerability).

e. Cost Benefit Analysis. In order to complete the risk analysis, mitigation options must be identified. Appropriate controls must be determined, decisions must be made, controls must be implemented, and after implementation, controls must be supervised and reviewed. Because risk should be mitigated only to the point where it becomes cost-prohibitive, a cost benefit analysis needs to be used to determine appropriate controls. Cost Benefit Analysis = Risk/Cost Benefit (mitigation options x risk reduction x cost). The cost and effectiveness of each mitigation option should be identified so decision-makers can see the cost and benefit of each option. The success of risk analysis in the risk management process is contingent on:

(1) Commanders weighing risk versus benefits, and making and/or implementing decisions to accept risk or reduce unacceptable risk.

(2) Acceptable risks being communicated to subordinates.

(3) Continuous evaluation of effectiveness of applied controls and capture of lessons learned.

8. Risk Management Process Overview

a. The risk management process requires the following:

(1) Identify threats.

(2) Prioritize criticality of assets to be protected.

(3) Evaluate asset vulnerabilities based on currently existing protection and identified threats.

(4) Determine mitigation options.

- (5) Develop controls and make risk decisions.
- (6) Implement controls.
- (7) Supervise and reevaluate controls.

b. Risk Management Process Application Guidelines. To get maximum benefit from the risk management process the following guidelines should be applied. Figure 2-4 provides a graphic depiction of the entire risk management process.

(1) Apply the Process in Sequence. Each element of the risk analysis process is a building block for the next element. For example, if the threat assessment is interrupted to focus control on a particular threat, other more important threats may be overlooked and the risk analysis process may be distorted. Until each element is complete, it is not possible to successfully move to the next.

(2) Maintain Balance in the Process. All parts of the process are important. Time must be allocated to ensure the total process can be completed. The objective is to assess the time and resources available for risk management activities and allocate them to the actions in a manner most likely to produce the best overall result.

(3) Apply the Process as a Cycle. Notice that "supervise and review" feeds back into the beginning of the process. When "supervise and review" identifies additional threats or determines that controls are ineffective, the entire risk management process should be repeated.

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. Aboard 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 and/or 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. Required 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, barriers, access control systems).
6. Key and lock control.
7. Coordination with other security agencies.
8. Designation of restricted areas.

2007. SECURITY EDUCATION AND TRAINING

1. Security is not an inherent state of mind; therefore, security responsibility must be stressed in a continuous, vigorous security education program to every Marine and civilian employee within the Marine Corps.
2. To be effective, a security program including AT and FP must be supported by a security education program for all personnel.

Commanders must place active interest and support behind installation security and security training.

3. One of the greatest challenges involves heightening personal awareness and instilling a "feeling of ownership". Historically, instances of loss, damage, and theft were in part attributable to a lack of care, concern, or awareness. Commanders can make a significant contribution to security, AT and FP by developing an awareness and conscious concern for security within their organizations.

4. A security education program will be established at each activity to ensure that all assigned personnel, military and civilian, recognize and understand their responsibilities.

a. Security education material will be written so that personnel understand the need for security, as well as the possible consequences to their co-workers of security vulnerabilities.

b. Security education programs will include all pertinent aspects of physical security, law enforcement, and crime prevention including those specifically related to AT and FP. Many aspects of these programs have a direct personal application to activity personnel.

c. All personnel, military and civilian, will receive initial security instruction.

d. Refresher security training will be given to the extent necessary to ensure personnel remain mindful of and proficient in meeting their security responsibilities.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 3

SECURITY MEASURES

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|--|------------------|-------------|
| SECURITY MEASURES | 3000 | 3-3 |
| PHYSICAL SECURITY SURVEY PROGRAM | 3001 | 3-3 |
| PERIMETER AND AREA PROTECTION | 3002 | 3-7 |
| AREA DESIGNATION | 3003 | 3-9 |
| SIGNS AND POSTING OF BOUNDARIES | 3004 | 3-16 |
| KEY/LOCK SECURITY AND ACCESS CONTROL . . | 3005 | 3-18 |
| SECURITY CONTAINERS, VAULTS, AND SECURE ROOMS | 3006 | 3-22 |
| SECURITY CHECKS | 3007 | 3-22 |
| SECURITY VIOLATIONS | 3008 | 3-23 |
| PARKING OF PRIVATELY OWNED VEHICLES (POV) | 3009 | 3-24 |
| TRAFFIC CONTROL | 3010 | 3-25 |
| PROTECTIVE LIGHTING | 3011 | 3-25 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

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 a systematic evaluation of the overall security of a given facility or activity and should not be regarded as an inspection or investigation. Surveys are intended to ensure compliance with directives, 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, and locks) and procedural (e.g., access control, lock and key control, and property accountability). The objective is to provide the commander a current depiction of the physical security posture of a selected facility/area. Some organizations have specific security requirements outlined in additional orders that complement the requirements of this Order; however, organization specific security requirements will not be surveyed.

1. School-trained military police personnel possessing the additional MOS 5814 (Physical Security Specialist) and a Secret clearance will conduct all physical security surveys aboard Marine Corps installations. Civilians (contractor or government employee), whose responsibilities include conducting physical security surveys, will possess a Secret clearance and one of the following:

a. ASIS International Physical Security Professional certification.

b. FLETC Physical Security Course certification.

c. Department of the Army Conventional Physical Security Course Certificate.

2. Personnel conducting these surveys serve as a representative of the installation commander for the purpose of evaluating the

overall installation security posture. Physical security personnel will require access to restricted areas and non-restricted areas while in the performance and scope of their duties.

3. Physical security surveys of restricted areas will be scheduled with the responsible organization. All other surveys should be scheduled with responsible organization. The command requesting/requiring the survey will assign an individual to assist the physical security specialist during the course of the survey. Briefings will be conducted with the commander or designated representative prior to and upon completion of the survey.

4. Physical security surveys will be completed using the Navy-Marine Corps (NAVMC) Form 11121 or an equivalent electronic copy. An electronic copy may be obtained at <http://www.marines.mil/units/hqmc/Pages/default.aspx> by linking to the forms library through News, Publications, then Marine Corps Forms. An example NAVMAC 11121 is provided in Appendix E. A guide for preparing, completing, and distributing physical security surveys is provided in Appendix F. This reporting requirement is exempt from reports control per reference (ba), Part IV, paragraph 7.3.

5. The following types of physical security surveys will be conducted:

a. Arms, Ammunition and Explosives

(1) Per reference (b), all Arms, Ammunition and Explosive storage facilities, (including RDT&E facilities, 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 requirements of this Order.

b. Communication Security (COMSEC)

(1) Per reference (o), all COMSEC facilities will be surveyed.

(2) COMSEC facility surveys will be conducted on a biennial basis; subsequent surveys will not exceed 730 days.

(3) A statement will be placed in Block 17 of NAVMC 11121 indicating whether the facility does/does not meet structural requirements of reference (o). Physical Security Specialists will not indicate the level of classified information a facility is authorized to store or maintain.

c. Restricted Areas

(1) All restricted areas will be surveyed.

(2) Restricted area surveys will be conducted on an annual basis; subsequent surveys will not exceed 365 days.

d. Classified Information Storage Areas

(1) Physical security surveys of classified information storage areas are not required unless the area is designated in writing a restricted area and is utilized for open storage of classified material.

(2) Physical security surveys of classified information storage areas will be structural in nature, per reference (d), chapter 10, and not administrative or procedural.

(3) The survey will include the facility ESS, because ESS is inherently the responsibility of the Provost Marshal's Office aboard Marine Corps installations. Paragraph 7006 provides additional security guidance for classified information storage areas.

(4) The installation security manager is responsible for the accreditation and validation of classified information storage areas, to include administrative and procedural inspections.

(5) Physical security personnel are not authorized to determine the types or level of information a classified information storage area can safeguard.

(6) Classified information storage area surveys will be conducted on an eighteen-month basis; subsequent surveys will not exceed 548 days.

(7) A statement will be placed in Block 17 of NAVMC 11121 indicating whether the facility does/does not meet structural requirements of reference (d). Physical security specialists will not indicate the level of classified information a storage area is authorized to maintain or store.

6. Non-restricted areas do not require a physical security survey.

7. Facilities must be resurveyed when there is evidence of penetration or tampering, modifications to the facility that change the security posture, when the facility is relocated, or reoccupied after being temporarily abandoned.

8. 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).

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

10. 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.

11. The approving officer (physical security chief or individual designated by the provost marshal) and the surveying inspector are required to sign the appropriate block. At no time will the same individual sign both blocks. The provost marshal, or designated representative, is responsible for the signature block on the survey cover page.

12. Original, signed surveys, paper and/or electronic copies will be maintained for three years by both the affected facility and the provost marshal's physical security section.

13. Within 90 days of receipt of a physical security survey, commanders are required to provide the provost marshal a corrective action report. The corrective action report provides a response to deficiencies or comments contained in the physical security survey. The corrective action report will address or include:

a. Measures taken, or to be taken, to correct identified deficiencies.

b. Compensatory measures taken as a result of identified security vulnerabilities.

c. Copies of any POA&M that resulted from identified security deficiencies.

d. Exception/waiver requests submitted for identified deficiencies that cannot be corrected immediately.

14. The provost marshal will provide the installation commander an annual (calendar year) summary that details uncorrected deficiencies, requested exceptions and waivers, security violations, commands that have not responded with a corrective action report, and any significant trends.

3002. PERIMETER AND AREA PROTECTION

1. Prior to making decisions to employ security measures, a threat assessment must be obtained from the Naval Criminal Investigative Service (NCIS), a vulnerability assessment conducted per reference (n), and a risk analysis performed to determine the degree of physical security required. Extensive and costly security measures may be necessary to protect certain items of security interest. In each case the commander is responsible for complying with established security requirements while working to achieve economy. To achieve this objective, the criticality and vulnerability of the asset must be evaluated in relationship to a ranking of a potential threat, and security requirements must be clearly understood. A specified 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 measures are the first steps in providing actual protection against certain security threats. These measures include barriers, fencing, and other security devices. Security barriers are intended to define boundaries and may be used to channel personnel and vehicular access. Security barriers may be natural or man-made and are addressed in chapter 5.

3. Physical Protection System Design Principles. Security planners need to recognize the asymmetrical threat, and trust in processes such as Risk Analysis to determine which assets are the most critical and the most cost effective means of applying security measures. The biggest challenge facing security planners is determining the most effective, yet economical, use of detection and delay measures which will provide sufficient enough time for the response force to intervene before damage to or compromise of the asset occurs. There are two basic design principles that security planners can use to determine the most effective and economical way to protect assets, personnel, or facilities.

a. Security-In-Depth (Layered) Principle. Security-in-depth involves a methodology with overarching and complementing security measures in a layered approach. Security equipment, measures, and practices are applied at the installation perimeter with additional layers deployed across or throughout the installation, up to and, including the facility/asset. It allows commanders to establish and maintain a robust security posture at the asset while applying a number of random and fixed security measures throughout the installation in support. The layers associated with the security-in-depth principle are:

(1) The first layer is applied to the true installation perimeter. This defense exists primarily of manpower, supported by measures, procedures, and equipment applied in and around the entry control facility and includes a number of natural barriers and man-made barriers along the installation perimeter. Signage is required to identify the installation as U.S. Government Property, and as required by current directives. Physical security efforts at the ECF are directed towards proper construction, to ensure that all physical security and force protection requirements are identified. Additional efforts include barriers, sensors and other devices that detect, delay, and deny any attempt to penetrate the perimeter at the ECF and other points throughout the perimeter.

(2) The second layer involves a number of measures taken directly inside of the perimeter and throughout the installation that enhance perimeter security. Efforts include natural and man-made barriers, sensors, lights and other physical security equipment and initiatives adjacent to perimeter fences. This layer incorporates military police (MP) mobile and foot patrols and other Random Antiterrorism Measures (RAM) through the base.

(3) The third layer presents heightened physical security measures with a heavy barrier presence at or around the asset(s). Barriers serve as a boundary and establish personnel and vehicle access points. Physical security measures focus on security management, increased access control, and unobstructed space directly outside of the assets. The unobstructed spaces allows for security personnel to have a clear view of the facility exterior. Heavy technology use supports access control, surveillance, detection, and notification. Manpower requirements such as increased area guards or security patrols may fluctuate based on commander's directions, threats, or increased Force Protection Conditions (FPCONS).

(4) The final layer is applied directly to the facility or area. Security within the actual facility is also applied in layers, in order to further segregate the asset to be protected. Policy dictates construction requirements, additional hardening, and heavy use of technology in support of access control, surveillance, detection, and notification. Policy may dictate maintaining personnel in the facility constantly, and in some cases, armed personnel. Interior defenses may place personnel in direct proximity of the asset(s) to be protected.

b. Enclave ("Island") Principle. Enclaving involves the 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.

3003. AREA DESIGNATION. Areas will be designated as either restricted areas or non-restricted areas. Different areas and tasks require varying degrees of security interest and importance. The degree of security is dependent upon the area mission, nature of the work performed within, and assets/material within the area. To address these issues, facilitate operations and security applications, a systems approach incorporating 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 criticality and sensitivity of an asset or area requires further segregation and a greater degree of security enhancement.

1. Restricted areas are established in writing by a commanding officer within his/her jurisdiction per reference (a).

a. Commanding officers are required to publish an annual list, in writing, of all areas under their control that are required by guiding directives to be designated a restricted area (this requirement also applies to officers in charge, and managerial civilian personnel). Particular attention will be paid to areas critical to mission accomplishment, vital to national security, and containing assets inherently dangerous to others. This list will be provided to the installation provost marshal.

b. The installation provost marshal will review and consolidate the list of all recommended restricted areas aboard the installation (including tenant commands). The consolidated list of recommended restricted areas will be provided to the installation commander for concurrence and signature.

c. Installation commanders will publish a consolidated list of all restricted areas aboard their installation. This list will be published annually, at a minimum, and as required based on changes to area designation(s). The list will be designated FOUO at a minimum.

2. Restricted Areas. There are three types of designation for restricted areas: Level One, Level Two, and Level Three. Restricted areas shall be posted simply as restricted areas per the sign provisions set forth in paragraph 3004 so as not to 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, presidential support assets, 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 areas, it contains a security interest that if lost, stolen, compromised, or sabotaged would cause damage to the command

mission and national security. It may serve as a buffer zone for Level Three and Level Two restricted areas, providing access and 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 never inside a Level Three area. Level Two restricted areas contain a security interest that if lost, stolen, compromised, or sabotaged would cause serious damage to the command mission and national security. Uncontrolled or unescorted movement could permit access to the security interest or asset.

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

d. Decisions regarding the designation of restricted areas and their levels are at the discretion of the commanding officer however, the following areas will be designated as specified below, at a minimum.

(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's Office Desk Sergeant area.
- (f) Dispatch and alarm monitoring spaces.

(2) Level Two

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

(b) Aircraft rework areas.

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

(d) AA&E RDT&E facilities, storage facilities and processing areas (including ammunition supply points, production buildings, and temporary storage in ready service magazines and lockers). (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.

(h) Military Working Dog (MWD) facility.

(3) Level Three

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

(b) Sensitive Compartmented Information Facility (SCIF).

(c) Assets and equipment in direct support of the Presidential Mission.

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 paragraph 3004. Lighting and barrier requirements are set forth in chapters 3 and 5. Points of ingress will be posted in accordance with paragraph 3004.

(2) Access of individuals (military, civil service, contractors, and official visitors) who require entry for reasons of official business, and render a service (vendors, delivery people). All visitors must be authorized by the commanding officer.

(3) A personal identification and access control system is suggested. An access control log identifying personnel, date, and entry and departure times may be used, at the discretion of the Commanding Officer.

(4) Secured during non-working hours.

(5) When secured and not adequately equipped with an operational intrusion detection system (point and area sensors), duty personnel will conduct a check of the facility/area once per 12-hour shift for signs of attempted or successful unauthorized entry, and for other activities that could compromise the security of the restricted area. Security checks are not required for areas adequately equipped with 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 paragraph 3004. Lighting and barrier requirements are set forth in chapters 3 and 5. Points of ingress will be posted in accordance with paragraph 3004.

(2) Access limited to personnel authorized in writing by the commanding officer and whose duties require entry. Controlled access of individuals (military, civil service, contractors, and visitors) conducting official business, and/or rendering a service (vendors, delivery people) is required. All visitors must be authorized by the commanding officer and will be escorted by an authorized/cleared individual at all times.

The security interest will be protected from compromise.

(3) Use of a personal identification and access control system (an Automated Access Control System (AACS) capable of recording ingress and egress may be used). If a computer log/access control system is used, it must be safeguarded against tampering. During working hours, use of an access list and entry/departure log is required to include all visitors.

(4) Secured during non-working hours.

(5) When secured, checked once per 12-hour shift if adequately equipped with an operational IDS (point and area sensors), or twice per 12-hour shift for facilities without an operational IDS. Security force personnel will check for signs of attempted or successful unauthorized entry, and for activity that could compromise 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 the defined and protected perimeter 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 paragraph 3004. Lighting and barrier requirements are set forth in chapters 3 and 5. Points of ingress will be posted in accordance with paragraph 3004.

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

(3) Access limited only to personnel whose duties require access and who have been authorized in writing by the Commanding Officer. Controlled access of individuals (military, civil service, contractors, and visitors) conducting official business or rendering a service (vendors, delivery people) is required. All visitors must be authorized by the commanding officer and will be escorted by an authorized/cleared individual at all times. The security interest will be protected from compromise.

(4) A personal identification and automated access control system with the capability of recording ingress and

egress is required. The system must be safeguarded against tampering. An access list and entry/departure log is required for all personnel at all times.

(5) Secured during non-working hours. When secured, an operational IDS (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 IDS (point and area sensors). Security force personnel will check for signs of attempted or successful unauthorized entry, and for activity that could compromise the security of the restricted area.

d. Assets considered critical to the overall mission accomplishment and national security are identified in figure 7-1. Figure 7-1 contains information to assist commanders in determining the degree of security for various types of assets beyond the standards contained in paragraph 3003(2)d.

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, personnel and vehicle administrative inspection operations must be conducted on a random basis. The activity security officer is charged with ensuring that the inspections are conducted. Procedures will be coordinated with the cognizant SJA 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. Non-restricted areas will not be located

inside restricted areas.

b. Installations and organizations contain a number of facilities where military personnel, their immediate family, and civilian employees 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. 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

2. Perimeter barriers of all restricted areas (including buildings at primary entry points) 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. 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

4. Where a language other than English is prevalent (OCONUS and areas bordering other countries), restricted and non-restricted area warning notices will be posted in both languages.

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

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

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

8. 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 required 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.

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

10. These signs may be contracted for, produced locally, or acquired through the Commanding Officer, Crane Division, Naval Surface Warfare Center (NSWC), Code GXQS, Building 3395, 300 Highway 361, Crane, IN, 47522-5001, commercial (812) 854-5812, DSN 482-5812.

11. At no time will signs be placed on the installation perimeter fencing, announcing Marine Corps Community Services (MCCS), MCCS Contracted Vendors, or local business sales events. The only signs authorized to be affixed to the installation perimeter fencing are:

a. Signs listed in paragraph 3004

b. Force Protection Conditions

c. Lettering permanently affixed to the fence identifying

the installation and/or gate by name

- d. Temporary advertisements, not to exceed thirty days (e.g. Air Show, Unit Welcome Home, Special Events)

3005. KEY/LOCK SECURITY AND ACCESS CONTROL. Each Marine Corps organization must establish a strict key and lock security and access control program supervised by the Command Security Officer. Included in this program are all keys (e.g. Personal Identification Number (PIN), combinations, Common Access Card (CAC), and physical keys), locks (to include digital and mechanical push-button), 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, and unclassified administrative or personal use.

- a. Additional key/lock and access control requirements for protection of classified material, information assurance, and nuclear weapons security are specifically addressed in references (d) through (g), respectively.

- b. In addition to this section, security of AA&E is further defined in chapter 8.

1. Access Control Officer. The access 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 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 access control officer will conduct an annual inventory of all controlled issued keys and will maintain appropriate logs and records. Appendix G provides an example key inventory form. Inventory records will be retained for three years.

2. Access Control Custodian. The head of each major functional area (e.g., department, directorate, etc.) within an organization will designate in writing an access control custodian who will be responsible to the access control officer for all keys controlled by that functional area. Each custodian will inventory keys and log accounts semiannually. Appendix G provides an example key control register and inventory form.

The record of this inventory shall be retained for three years.

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. Physical keys to restricted areas 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 organizations where the security key and lock program is too small to warrant a central key room, a security container constructed of a minimum of 20-gauge steel will be used to provide protection of duplicate keys, blanks and associated equipment. The container will be secured and provided security commensurate with the material to which the keys allow access.

b. The access control officer or custodian will strictly control access to the container.

4. Rotation and Maintenance. Security locks, padlocks, and lock cores designated as high security, will be rotated annually 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.). 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 requirement, who have been approved by the activity security officer. Convenience or status is not sufficient criteria for issue of a security key. Certain restricted areas and security assets have specific regulatory guidance concerning the issue and control of keys. The security officer is responsible for developing and enforcing guidance and procedures for key issue as part of the access control function.

6. Key Control. Continuous accountability of keys is required. The custodian/sub-custodian must develop and maintain a key control register 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 G provides an example control register. 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, in use, or in the physical possession of authorized personnel, keys will be secured in containers that 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.

e. Master keying of locks and the use of a master key system is prohibited for all restricted areas. The use of master keys and locks is highly discouraged for non-restricted areas. Possession of master keys for non-restricted areas will be limited to the installation locksmith.

f. 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 a padlock is intended to secure, is open or unsecured, 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. Seals must meet be approved and meet current Federal Specification DD-S-2738. Security personnel will be instructed that lack of free play (approximately one-eighth inch) indicates the possibility of tampering and a follow-up examination of the seal conducted. Seals will be serialized, stored, and safeguarded in the same manner as prescribed herein for keys. 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 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 required skills, and have been assigned the responsibility 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, or believed to have been compromised.

b. A completed copy of the SF 700, "Security Container Information" will be maintained on the interior of each security container or safe regardless of contents (e.g. safes storing classified information, AA&E, high value items, money, negotiable instruments, drugs, etc.). The envelope and information sheet will be sealed, placed in a marked envelope, and provided to the security officer. The security officer is responsible for storage, inventory, and safekeeping of the remaining copy and combination in accordance with this Order and applicable regulatory guidance.

12. Access Codes and Subscriber PINs. Access codes and subscriber PINs are subject to the same protective measures as keys and locks. The access control custodian will be responsible for the issuance, maintenance, and security of access codes and subscriber PINs. Records of access codes and subscriber PINs will not be printed or maintained in hardcopy of any kind. All records and copies will be retained electronically within the operating system of the automated access control system for three years.

a. Physical security personnel assigned to the Provost Marshal's Office are responsible for issuance, maintenance, and security of access codes and subscriber PINs for the MCESS.

(1) Personnel requiring access codes and subscriber PINs will submit a PIN request signed by the access control officer, and a copy of the facility unaccompanied access control roster.

(2) Commands are responsible to ensure personnel are deactivated from the system upon checking out, or as required.

13. Access Rosters

a. Access rosters identify those persons authorized to enter an area in the performance of their duties and will be signed by the commanding officer, Officer In Charge (OIC), or designated representative. Rosters will be posted on the interior wall of a designated space adjacent to the main entry point and will not be visible from the exterior.

b. Unaccompanied access rosters identify those persons authorized to enter an area in the performance of their duties. Unaccompanied access is limited to persons for essential operations and requires those persons to be cleared and/or screened prior to access being granted. These rosters will be signed by the commanding officer of the functional area. All rosters will be posted or maintained out of plain view.

3006. SECURITY CONTAINERS, VAULTS, AND SECURE ROOMS. Security containers, vaults and secure rooms will conform to the specifications contained in reference (d), and are further addressed in paragraph 7006.

3007. SECURITY CHECKS

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 installation PMO. The organization security officer will review each deficiency or violation, and maintain a record of all corrective actions taken. Records of security checks will be maintained for a period of three years.

5 Jun 09

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 will be reported to the organization security officer and the PMO for action.

3008. SECURITY VIOLATIONS. Ability and willingness to follow security regulations, requirements, procedures, and guidelines for the protection of critical assets is paramount; therefore, the significance of a security violation is not dependant solely on actual compromise of an asset or facility, but also a possible pattern of negligence. Accidental and infrequent minor violations are to be expected, however deliberate or repeated failure to comply with regulatory requirements must be reported immediately to the security officer for appropriate action. A log will be maintained of all security violators, the violation committed, and corrective action taken. Records of security violations will be maintained for three years.

1. At a minimum, the following examples of security violations will be recorded (this list is not all inclusive):

- a. Unattended or unsecured classified information.
- b. Loss of a security badge.
- c. Circumventing security policy or protocol for convenience.
- d. Failure to properly secure a facility after normal working hours.

2. Failure to report a security violation is itself a security violation and will have very serious implications.

3. A security violation may be a symptom of underlying attitudes, emotional or personality problems, or substance abuse problems that are a greater concern than the security violation itself.

4. The following includes security violations that must be reported to the Provost Marshal's Office and an incident complaint report filed (this list is not all inclusive).

5 Jun 09

a. Leaving an AA&E facility unsecured and unattended either during or after normal working hours.

b. Misuse of a security badge, such as:

(1) Use of a security badge, assigned to another individual, to access a controlled area.

(2) Failure to immediately report the loss of a security badge to a Level Two or Three restricted area.

c. Failure to properly secure facilities protected by the MCESS.

d. Use of a MCESS Operators login and password by another individual.

e. Trespassing on Marine Corps installations.

f. Failure to report security violators, identified in paragraph 4(a) through (e) above, to the Provost Marshal's Office.

5. Commanders will ensure that battalion orders address actions required upon notification of security violations within the command.

3009. PARKING OF PRIVATELY OWNED VEHICLES (POV)

1. Vehicle parking is prohibited within 33 feet of any inhabited structure or 82 feet from billeting 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 33 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 AT and FP 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.

5 Jun 09

3010. TRAFFIC CONTROL. The provost marshal will establish a traffic control program in accordance with reference (p). Chapter 5 provides additional information concerning physical security requirements to be included in the program. Those requirements include entry control facilities, access control points, patrol roads, and the use of barriers.

3011. PROTECTIVE LIGHTING

1. General. Protective or security lighting is an integral part of both the command security and safety posture. 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 solution between resource allocation, fiscal commitment, and effective security, each situation must be carefully and individually studied. The overall goal is to adequately illuminate areas in an effort to provide a safe and secure environment during hours of darkness. Security lighting assists in crime reduction as a deterrent for criminal activity while providing illumination for the security force. Lighting must be sufficient to allow security force personnel to detect and reveal the presence of unauthorized persons and criminal activity. Where lighting is impractical, additional compensatory measures must be instituted.

2. General Principles and Guidelines. Paragraph 4.7 of reference (q) provides general principles and guidelines for exterior protective (security) lighting. Figure 3.1 (Lighting Specification (Foot Candles)), and Figure 3.2 (Illuminated Area Specification) will 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 (q), will also be applied:

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

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 away from 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).

| Lamp Type | Efficiency (Lumens/Watt) | Restrike Time (Minutes) |
|----------------------|--------------------------|--|
| Theoretical Maximum | 683 | --- |
| Ideal White Light | 220 | --- |
| Incandescent | 10-16 | <1 |
| Tungsten-Halogen | 17-25 | <1 |
| Mercury Vapor | 30-65 | 3-7 |
| Fluorescent | 33-77 | <1 |
| Metal Halide | 75-125 | up to 15 |
| High-Pressure Sodium | 60-140 | 1 (restrike) 3-4 (warm-up to Full output) |
| Low-Pressure Sodium | 180 | 7-15 |

Figure 3-1.--Lighting Specifications

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

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

f. Avoid drawing unwanted attention to restricted areas.

g. During planning stages, consideration will be given to selecting the type of lighting to be installed for future closed circuit television requirements. Where color recognition will be a factor, full spectrum (high pressure sodium vapor, etc.) lighting vice single color will be used.

h. When selecting a light system, ensure the lighting is adequate for all types of weather conditions. The 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.

| Application | | | Illuminated Width Feet (meters) | | Minimum Illumination | |
|----------------|------------|--------------------------|------------------------------------|-------------------------|--------------------------------------|--------------------------------------|
| Type | Lighting | Area | Inside | Outside | Footcandles (lux) (a) | Location |
| Boundary | Glare | Isolated | 25 (7.6) | 150 (66) | 0.2 (2.1) (b) 0.4 (4.3) | Outer lighted edge At fence |
| | Controlled | Semi- Isolated | 10 (3.0) | 70 (21) | 0.2 (2.1) 0.4 (4.3) | Outer lighted edge At fence |
| | Controlled | Non-Isolated | 20-30 (6.1 - 9.1) | 30-40 (9.1 - 1.2) | 0.4 (4.3) 0.5 (5.4) | Outer lighted edge Within |
| Inner Area | Area | General at Structures | All 50 (15) | --- --- | 0.2-0.5 (c) (2.1 - 5.4) 1 (11) | Entire Area Out from structure |
| Entry Point | Controlled | Pedestrian | 25 (7.6) | 25 (7.6) | 2 (21) | Entry pavement and sidewalk |
| | | Vehicular | 50 (15) | 50 (15) | 1 (11) | |

- (a) Horizontal Plane at ground level unless otherwise noted.
- (b) Vertical Plane, 3 feet (0.9m) above grade.
- (c) Use higher value for more sensitive areas.

Figure 3-2.-- Illuminated Area Specifications

(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 of the difficulty to see inside the area being protected. It 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. Used when necessary to limit the width of a lighted area due to 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 will 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 automatically or manually turned on. Standby lighting is activated when suspicious activity is detected or by an intrusion detection system sensor. Security personnel investigating suspicious activity may also turn on the lights manually. Lamps with short restart times are essential for this technique. 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 lights that may be lighted during hours of darkness or as needed. This system is normally used to supplement continuous or standby lighting.

d. Emergency Lighting. Emergency lighting is used during power failures or other emergencies that render the normal lighting system inoperative. It operates on alternative power sources, such as batteries or generators and may duplicate any or all of the above systems.

4. Protective Lighting Parameters. It is not the intent of this Order to prescribe specific protective lighting requirements, except for minimum standards described in paragraph 5 below. Commanding officers, in coordination with physical security, public works, facilities, and Resident Officer in Charge of Construction (ROICC) personnel must be involved in the decision regarding areas or assets to illuminate and lighting requirements. 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.

5 Jun 09

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 will 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, aircraft parking areas, 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. Security force and duty personnel will inspect protective lighting, within their area of responsibility, monthly to ensure all lights are operational. All facilities aboard Marine Corps installations must ensure that standard operating procedures address, or a system is emplaced for, inspection of exterior and security lighting. Inoperable lights will be reported to facilities maintenance/public works.

6. Emergency Power. All restricted areas with protective lighting, designated mission essential, will have an emergency power source in the event that primary power fails. However, regulatory guidance exists that requires some areas to maintain an emergency power source capable of sustaining essential equipment for a designated period of time. Emergency power sources may be an Uninterruptible Power Source (UPS) or generator. UPS provide immediate power without interruption of services. Generators may be programmed to start automatically

5 Jun 09

to minimize interruption of services. The emergency power source will be located within the restricted area and adequate to sustain security lighting, communications equipment, and other essential services. Emergency power systems will be properly maintained, tested quarterly, with maintenance and test logs recorded and maintained for a period of three years. Security Officers in those areas that suffer frequent power losses should consider alternative sources such as solar power to support essential services.

7. Protection - Controls and Switches. Controls and switches for protective lighting systems will be located inside the protected area and locked or guarded at all times. An alternative is to have controls provided with tamper protection, an intrusion detection system, and centrally located. High impact plastic shields may be installed over lights to prevent damage or destruction.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

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 | 4-5 |
| 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 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 4

SECURITY FORCES

4000. GENERAL. A Security force constitutes one of the most important elements of an organization's physical security program. Security forces consist of Marines, government service (GS) civilians, and in some cases, contract civilians. These personnel are specifically organized, trained, and equipped to provide 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 forces are one of the most effective tools in a comprehensive and 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, criminal activity, 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. The security force is integral to the physical security program and commanders have a responsibility to maintain and support the program. The following security forces may be employed:

1. Military Police. Military police are those Marines, possessing MOS 58XX, assigned to the PMO who perform installation law enforcement duties.
2. Marine Corps Civilian Police. Civilian government service personnel assigned to the PMO OR Marine Corps Police Department (MCPD) who perform installation law enforcement duties. Civilian police personnel are assigned through the Marine Corps Civilian Law Enforcement Program (MCCLEP).

5 Jun 09

3. Marine Corps Contract Security Guard. Civilian contracted personnel who perform access control and security guard duties. Contract security personnel are not authorized to conduct law enforcement duties. Current law prohibits contracting of new security guards. Additionally, the same law requires DOD to reduce and eventually eliminate contract security guards.

4. Interior Guard. An interior guard force consists of personnel organic to an organization that are trained and organized for the purpose of providing security for specific areas or assets under the cognizance of the organization's 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.

5. Other Forces. Onboard Marine Corps installations, other forces providing security functions may include unit armorers, duty watch-standers, Officer of the Day (OOD), Staff Duty Noncommissioned Officer of the Day (SDNCO), and other personnel assigned by the commanding officer as required. Commanding officers must adhere to and address security policies and regulations in battalion orders regarding duties of assigned personnel.

a. In some cases, conservation law enforcement officers and animal control officers aboard Marine Corps installations may be armed as part of their assigned duties. Reference (r) provides policy and guidance for all conservation law enforcement officers. Other forces also include personnel from other Services in support of contingency operations, special events, or general support.

b. Commanders of all other forces aboard Marine Corps installations as noted above will coordinate roles and responsibilities through PMO.

c. 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, status of forces 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

Status of Forces 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 must 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. 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 encompasses a combination of approved fencing, protective lighting, barriers, and ESS, 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 to maintain a security presence and response capability for a specified patrol zone.

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. Marine Corps Electronic Security System (MCESS) Operator. MCESS Operators/dispatchers monitor alarms, 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 the MCESS. Additionally:

- a. Operators will be armed, equipped, and trained in accordance with sections 4006-4008.
- b. Operators will be trained in the proper operation of the MCESS. Training for MCESS Operators is discussed in chapter 6.
- c. MCESS Operators will possess, at a minimum, an interim Secret clearance until their formal clearance is adjudicated.

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. Post specific and general orders will be maintained at each post for security force personnel. All orders will be brief, concise, specific, and written in a clear and simple

language. The orders will be reviewed annually and updated as required. The orders, at a minimum, will contain the following:

1. Special orders for each post that 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 references (s) through (u), and detailed guidance in the safe handling of weapons.
3. Training requirements for security personnel and designated posts.
4. Security force chain of command.
5. Required actions taken during increased FPCONs.
6. The local guard Standard Operating Procedure (SOP) must address the requirement for sentries at the AA&E facility if the ESS fails to function properly.

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

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

5 Jun 09

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 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 (u). The 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 (v).

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.
- d. Military police vehicles will conform to requirements identified in reference (w). 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

5 Jun 09

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. 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 not Reserve Centers). A duress button, in those facilities equipped with ESS, is recognized as a form of communication. A phone is recognized as a form of communication.

c. 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.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

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 CONSIDERATIONS | 5002 | 5-3 |
| ENTRY CONTROL FACILITY (ECF) | 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 |
| BARRIER PLANS | 5010 | 5-14 |
| WALLS | 5011 | 5-14 |
| CLEAR ZONES | 5012 | 5-14 |
| PATROL ROADS | 5013 | 5-15 |
| DOORS, WINDOWS, SKYLIGHTS, AND OTHER OPENINGS | 5014 | 5-15 |
| SEWERS, CULVERTS, AND OTHER UTILITY OPENINGS | 5015 | 5-16 |
| UTILITY POLES, SIGNBOARDS, AND TREES | 5016 | 5-16 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

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.
5. Channeling the flow of personnel and vehicles through designated portals in a manner that permits efficient operation of the personnel identification and control system.

5001. TYPES OF BARRIERS. The two types of barriers are natural and man-made. Figure 5-1 provides a list of both natural and man-made barriers and their functionality in security planning.

5002. GENERAL CONSIDERATIONS. Physical barriers delay, but can rarely be depended upon to stop a determined intruder. To be effective, security force personnel or other means of protection and assessment must augment such barriers. 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 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.

| Barrier Function | Natural Barriers | Man-made Barriers |
|--|--|---|
| 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 | Berms, earthworks, walls, solid fences, masonry block screens, translucent glass blocks, electric or mechanical pop-up barriers, concrete barriers |
| Minimize Ballistic Material Protection | | High Berms, earthworks, steel reinforced concrete or solid fill masonry walls, blast shields fabricated from steel-plate materials, ballistic-resistant glazing |

Figure 5-1.--Security Barriers and Functionality

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 will be separated by not less than 33 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 fence that provides additional protection and advantages with the integration 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 FACILITY (ECF). An entry control facility is the primary point of ingress and egress to Marine Corps installations. An ECF in the access control mission is extremely important to the security-in-depth and risk mitigation mission of the installation. The primary objectives of an ECF are to secure the installation from unauthorized access and intercept contraband (weapons, explosives, drugs, etc.), while maximizing vehicular traffic flow. Reference (x) provides further guidance concerning ECFs. Entry control facilities may also be established at fight lines, restricted areas, and other designated areas aboard the installation. Although this section primarily focuses on installation ECFs, the function, organization and design of an ECF, as outlined below, must be considered in all applications.

1. Function. ECFs serve as the installation's primary ingress/egress point for pedestrian and vehicular traffic. The ECF also serve as the focal point for processing visitors and inspecting vehicles prior to admission.

a. Not all functions are required at each ECF. Installation master plans and planning documents must consider establishing

ECFs that separate passenger vehicle and commercial vehicle functions. Figures 5-2 and 5-3 illustrate the general relationships between the different functions of an ECF.

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

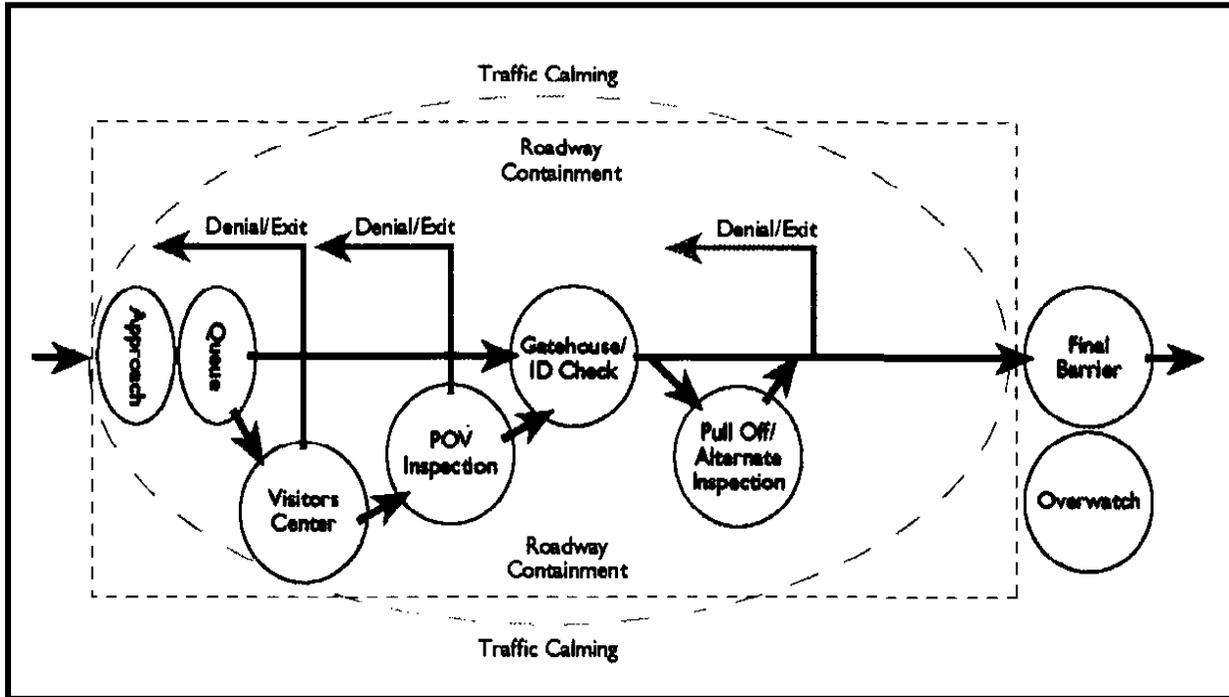


Figure 5-2.--Example Authorized Personnel/Visitors ECF

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.

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.

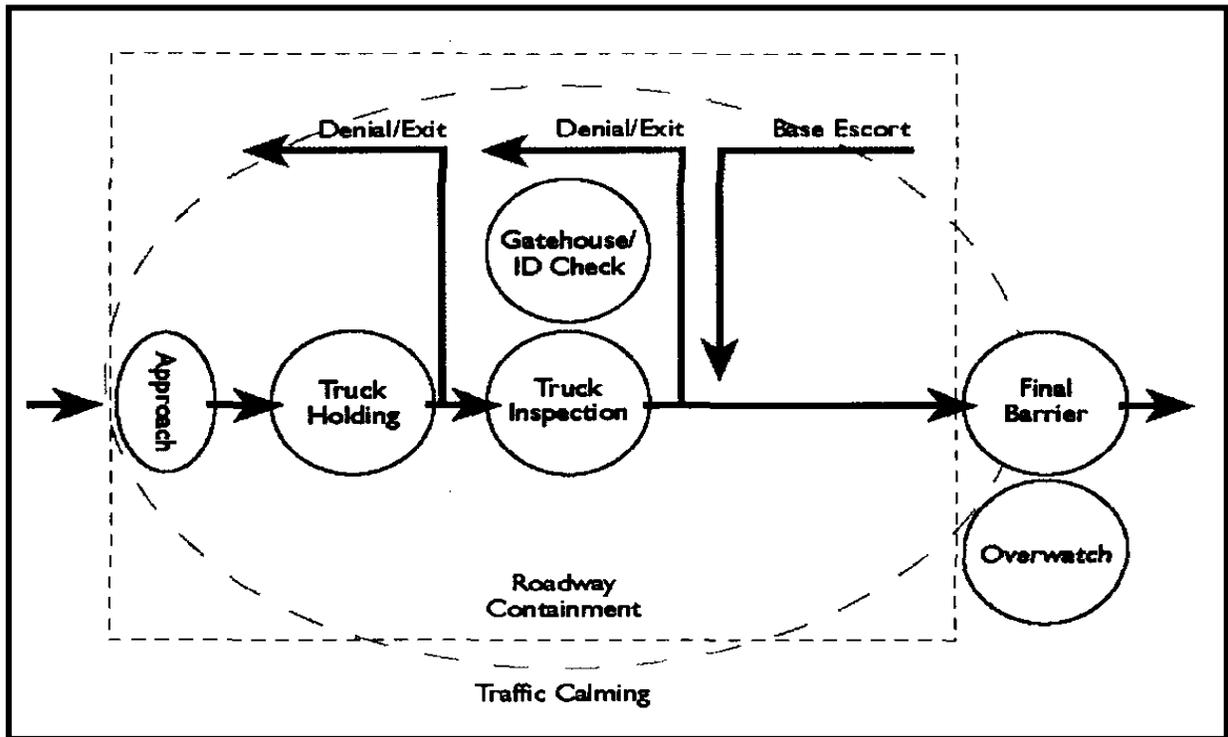


Figure 5-3.--Example Commercial Traffic ECF

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 security force 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.

3. Design Priorities. ECFs provide a first line of defense for the installation and 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.

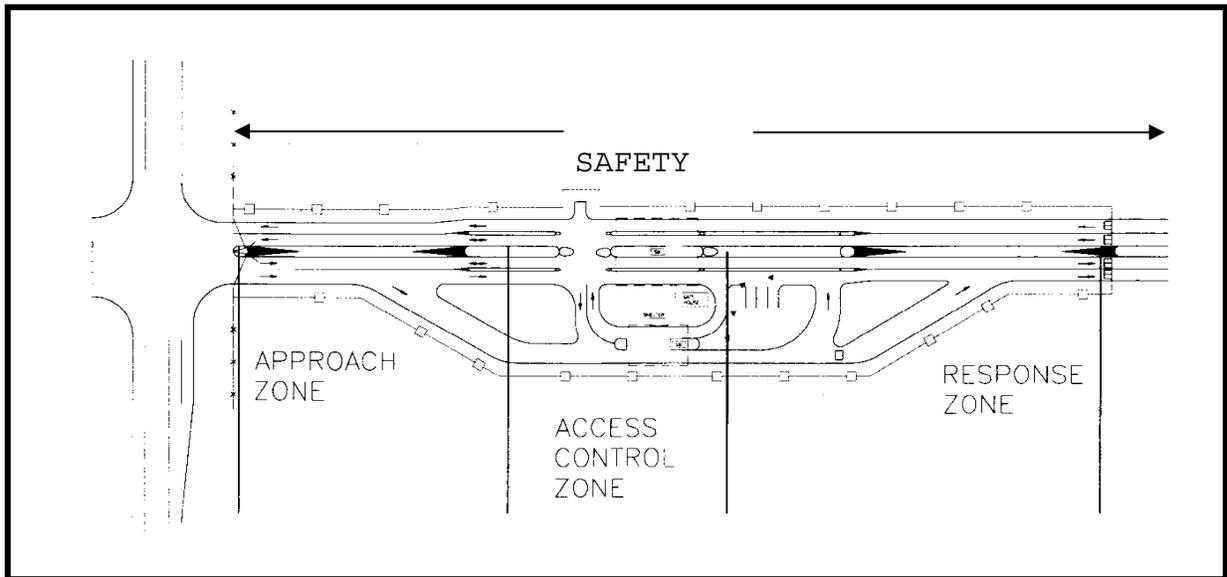


Figure 5-4.--ECF Zones

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 FPCONs and support all measures including 100% vehicle inspections. The ECF will have the capacity for supporting 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 will make every effort to separate pedestrian Access Control Points (ACP(s)) 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, 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.

5 Jun 09

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 employees 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 safe and efficient operation. Openings shall be constantly locked or secured to prevent unauthorized entry or exit. When operational, perimeter openings will be afforded security or an automated access control system may be used. When locked, 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. When considering the location of a gate, the volume and direction of personnel and vehicular traffic must be considered during planning and design phases. Alternative gates, closed except during peak movement hours, may be utilized to expedite heavy traffic flow. When operational commitments dictate, gates will be under control of a guard or appropriately trained and cleared personnel. Gates will be constructed with material equal to or greater than the fence or barrier that they are connected to in order to maintain perimeter integrity. Gates will be locked when not in use.

2. Pedestrian Gates. Pedestrian gates will be designed to allow security forces the ability to control movement of all personnel utilizing the gate. After peak operational periods, some gates may be secured. Pedestrian and vehicular gates will be separated to prevent pedestrian traffic from gaining access through vehicular gates.

3. Turnstiles. Turnstiles, a type of pedestrian gate, are generally automated to allow access to only one person at a time. However, all turnstiles will be capable of operating freely and being locked down, as required.

4. Vehicular Gates. Vehicular gates will be designed and constructed 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.

5. Inspection. When not active or 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 access control officer or access control custodian, as determined by the commanding officer.

5006. FENCES. All fencing will be posted, as required, in accordance with paragraph 3004.

NOTE: For enhanced force protection, additional reinforcement in the form of a 3/4 inch steel cable attached to support posts 30 inches above the ground, and properly anchored, will prevent lightweight vehicles from crashing through the fences and entering the protected area.

1. Chain Link Fencing. Chain link fencing is the type of man-made 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 an instance where a Commanding Officer determines application of a covering to be more advantageous to protecting the asset within the fenced area, an exception or waiver 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.

d. Fencing Posts, Supports, and Hardware. All posts, supports, and hardware for security fencing will meet the requirements of Federal Specification (Fed Spec) RR-F-191J/GEN of 22 July 1981. 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. 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 (q). All fencing, posts, support, and hardware will be coated or plated to inhibit rusting.

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

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

g. Culverts and Openings. Culverts located or constructed under or through a fence will be secured with material of equal or greater strength than the overall barrier. All openings, with a man-passable area greater than 96 square inches that penetrates the restricted area perimeter barrier, will be protected with reinforcing bars. The bars will be, at a minimum, No. 4 (12.7-mm) reinforcing bars, 9 inches on center, in each direction, securely fastened and staggered on each face to form a grid.

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. Outrigger. Outriggers must be installed on all perimeter fencing and restricted area fencing. Outriggers will be permanently affixed to the top of fence posts to increase the overall height of the fence at least 1 foot. Perimeter fencing will be equipped with a single 15-inch outrigger, with three strands of barbed wire, facing outward at a 45-degree angle or a Y configuration, with three strands of barbed wire, each installed at a 45-degree angle. Restricted areas will be equipped with a 15-inch outrigger in a Y configuration, with three strands of barbed wire, each installed at a 45-degree

5 Jun 09

angle. For additional protection, as directed by the commander, barbed tape or concertina wire may be installed between the Y of the outriggers. Outriggers for fencing bordering gates may range from a vertical height of 18 inches to the normal 45-degree protection, but only for sufficient distance along the fence to open the gates adequately. Ornamental fencing, as described below, will be constructed with outriggers or will extend outward at the top at a 45-degree angle. Barbed wire is not required on the outward portion of an ornamental fence.

2. Ornamental Fence. Ornamental fencing (also known as tubular) provides greater aesthetic qualities in comparison to chain link fencing and an increased resistance to climbing. Ornamental fencing will be constructed of steel with anti-ram reinforcement included at all vehicle gates. Freestanding facilities under high threat levels will use a smooth-faced perimeter wall or fence/wall combination to prevent personnel from using the fence as a climbing aid. In low and medium threat areas, ornamental fencing will be constructed to a height of eight feet, however, in high threat areas fences will be constructed at least 9 feet tall and extend at least 3 feet below grade. Upright supports will be spaced 9 feet apart, at a minimum, to prevent the fence from being used as a ladder. Areas with basic to medium security levels using ornamental fencing shall use welded wire, K shaped fasteners with a light wire. Medium to high security levels shall use either K or U shaped fasteners. High security levels shall use U shaped fasteners.

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

4. Welded Wire Mesh Fabric. In comparison to chain link fencing, welded wire mesh has a greater deterrence to intrusion by climbing, cutting, and tunneling and has a number of uses. Welded wire mesh fabric openings are relatively small, and generally prevent toe or finger holds. Round posts, C posts and square posts are available for welded wire mesh fabric fencing. Round or C rails are acceptable for top and bottom rail locations. Line posts shall be spaced per the manufacturer's recommendation. Fence fabric will be secured to rails with 9 gauge tie wires. Fencing panels are attached to line posts,

terminal posts, and gate frames with post brackets.

5. Expanded Metal Fencing. Expanded metal fencing is similar to welded wire mesh fabric fencing, and is suited for medium and high security applications. The mesh's small openings and wide strands deter climbing, cutting, and tunneling. Expanded metal fencing can be applied as a retrofit to existing chain link fencing and gates to provide additional protection, strength, and durability. In lieu of installing a fence topping, an expanded metal fabric cap sheet can be installed at a 45-degree angle extending outside of the perimeter and terminating with a turned up vertical section. If additional protection measures are required, barbed tape can be applied to the back of the vertical portion of the cap sheet. Expanded metal fencing can be installed directly to the existing fence utilizing the installed chain link fence fabric and framework.

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 (q) for guidance on barriers, and reference (x) for vehicle barriers at ECFs.

5009. INSPECTION OF BARRIERS. Security force personnel will inspect security barriers weekly for defects that would facilitate unauthorized entry, and report all discrepancies. 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 may afford cover for possible intruders.

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

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

5010. BARRIER PLANS. In accordance with this Order and reference (m), a barrier plan will be maintained as an appendix to the physical security plan. Barrier plans are designed to enhance the security of an area or facility aboard the installation by ensuring that the barriers are properly planned for, stored, maintained, and installed. The plan will detail specific barriers required for varied priority assets and contain comprehensive maps identifying placement. Maintenance, movement, equipment, support personnel, and staging/storage area requirements will be outlined in the plan.

5011. WALLS. Walls, floors, and roofs of buildings may 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.

5012. 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. Interior/exterior clear zones combined will be a minimum of 33 feet, with the interior clear zone being no less than 20 feet, and the exterior clear zone being no less than 10 feet. Clear zones for AA&E facilities will remain at a 30 feet interior clear zone and a 20 feet exterior clear zone. Additional standoff 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 will be provided to preclude or minimize damage from thrown objects such as incendiaries or bombs.

3. In those activities where space on government land is available, but the current fence placement does not meet clear zone requirements, relocating the fence to obtain a clear zone may not be feasible or cost effective. 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 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 will 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 will 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 feet 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 orders and directives.

5013. PATROL ROADS. When the perimeter barrier encloses a large area (one square mile or greater), an interior perimeter patrol road will be provided and adequately maintained for use by security force personnel. Where possible, patrol roads will be paved.

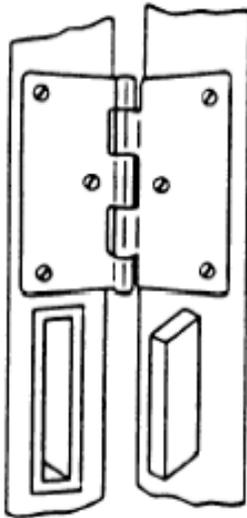
5014. DOORS, WINDOWS, SKYLIGHTS, AND OTHER OPENINGS. Building exterior doors will provide protection commensurate with the requirement for proper protection of the assets accessible through those doors. Hinges to all doors will be located on the interior of the door. In locations where the hinge pin is exposed to the exterior, hinges will be peened, brazed, spot welded, or equipped with a hinge secure pin. For planning purposes, the preferred hinge assembly is a hinge assembly equipped with hinge protection as shown in figure 5-5. Studs extend from one hinge leaf to a hole in the corresponding

5 Jun 09

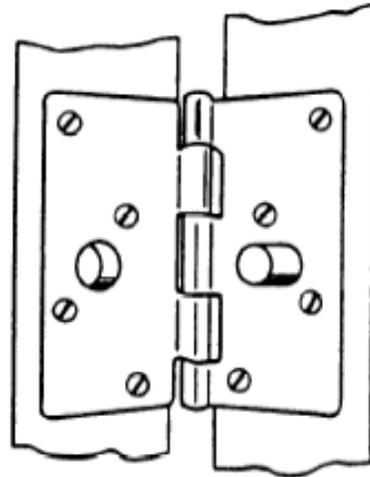
position on the opposite leaf. When the door is closed, the stud sits in the hole. If the hinge is removed, the door still cannot be taken off its hinges because the stud holds the door in place. Unless the width-to-height ratio of a window or opening eliminates the physical possibility of intruder entry, openings will be protected by securely fastened 9-gauge wire mesh, framed and permanently bolted to the structure. Openings are considered inaccessible when they are located 18 feet or more above ground level and 14 feet or more distant from buildings, structures, etc., outside the perimeter. Protective screens provide additional protection by preventing projectiles such as rocks, hand grenades, bombs, and incendiaries from being hurled through the windows from outside the perimeter.

5015. SEWERS, CULVERTS, AND OTHER UTILITY OPENINGS. Unless the width-to-height ratio absolutely eliminates the physical possibility of intruder entry (for example, 5 inches by 24 inches) all utility openings, which penetrate the perimeter or restricted area barriers will be protected against surreptitious entry. Protection of restricted area openings will 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, and storm drains 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.

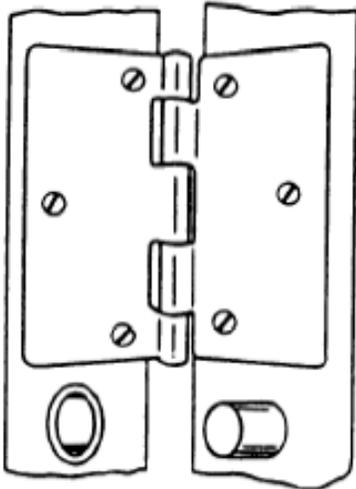
5016. UTILITY POLES, SIGNBOARDS, AND TREES. Utility poles, signboards, trees, etc., located outside of and within 15 feet of the perimeter barrier of the activity, present a possible assistance to entry. To reduce the vulnerability, the perimeter barrier will be staggered to increase the distance to more than 20 feet. Another alternative may be to raise the barrier to the extent necessary to prevent entry. In the event that it is not possible to move or raise the barrier, the hazard must be removed. Any utility poles, signboards, trees, etc., that obstruct the visibility of the guards, must be moved to at least 20 feet outside of the perimeter barrier.



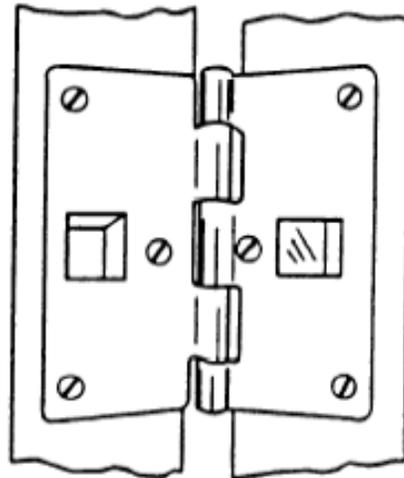
A) Metal lug and receptacle system.



B) Addition of a metal dowel-pin and socket to the existing hinge.



C) Installation of a metal dowel-pin in the door and reinforcing metal cup in the door frame.



D) Hinge with lug and matching socket formed into hinge at factory.

Note: Lugs, dowel-pins, etc., should be 1-inch-diameter (25.4mm) minimum.

Figure 5-5.--Example Hinge Protection

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 6

ELECTRONIC SECURITY SYSTEMS

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|---|------------------|-------------|
| INTRODUCTION | 6000 | 6-3 |
| GENERAL | 6001 | 6-3 |
| ESS DETERMINATION FACTORS | 6002 | 6-3 |
| 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 SYSTEMS | 6008 | 6-13 |
| AUTOMATED ACCESS CONTROL SYSTEMS (AACS) | 6009 | 6-22 |
| MASS NOTIFICATION SYSTEMS (MNS) | 6010 | 6-25 |
| MARINE FORCES RESERVE | 6011 | 6-27 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

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 components are designed to detect a predetermined anomaly, provide real-time assessment and timely notification to the MCESS Operator; however, it does not prevent actual or attempted penetrations. The design, implementation, and operation of ESS must contribute to the overall physical security posture and the attainment of security objectives.

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

1. Permit more economical and efficient use of security personnel by allowing MCESS Operators to control and direct the response of 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. 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 MCESS program was established to standardize ESS throughout the Marine Corps. Each Marine Corps installation has a standard ESS terminating at the installation PMO Dispatch Center. The purpose is to serve as the foundation for subsequent ESS procured by Security Division (PS) or coordinated by the installation/command. Prior to the advent of MCESS, individual installations 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, Security Division (PS) is the program manager for ESS and oversees system funding, procurement, installation, and maintenance. The MCESS is currently a suite of systems including IDS, Automated Access Control Systems (AACS), Mass Notification Systems (MNS), and Closed Circuit Television (CCTV) systems. These systems will not be modified in any way without prior Security Division (PS) approval. The focal point for the operation of these systems is the installation provost marshal.

3. Arms, Ammunition, and Explosives storage facilities and flight lines in the Marine Corps are serviced by a single alarm system. Security Division (PS) is responsible for funding MCESS installation for AA&E, flight line, and MNS applications. Security Division (PS) will attempt to obtain funding for all other ESS security projects through the normal Program Objective Memorandum (POM) process; however, activity/installation

commanders are still responsible for obtaining funding for projects in the absence of Security Division (PS) funding.

a. Any commercial alarm systems procured that will annunciate at, or be monitored by PMO will be compatible with the MCESS. This will eliminate proliferation of multiple alarm systems installed at PMO. Existing systems that annunciate at PMO will be compatible by 2012. Installations/commands may continue to use their current alarm system until 2012, at which time it will be replaced with a MCESS compatible system. No new non-MCESS compatible systems will be installed at PMO, or transferred/relocated to joint dispatch centers.

b. Installation of a MCESS compatible system for non Security Division (PS) funded facilities requires local installations/commands to obtain funding. The MCESS Technical Support Agency (TSA) or a local contractor (approved by the MCESS TSA) will perform all installations. Identified local contractors will provide an Installation Design Plan (IDP) to the MCESS TSA for approval. To maintain system integrity, compatibility must be certified (compatibility review costs will be borne by the installation), and final connectivity to the PMO Dispatch Center will be accomplished/supervised by MCESS TSA personnel.

c. Security Division (PS) will provide the final connection to the MCESS for all approved locally funded and installed ESS. Installations, commands, or responsible agencies may elect to use a local contractor to perform maintenance upon approval of the maintenance plan by the MCESS TSA. The MCESS TSA will be responsible for maintenance from the Remote Terminal Unit (RTU) back to the Dispatch Center.

d. Security Division (PS) will provide life cycle upgrades and maintenance support for installations, commands, or responsible agencies that procure local funding and utilize the MCESS TSA for installation.

e. Installations, commands, or responsible agencies will assume all repair costs, if it is determined to be negligence on the part of civilian, military, or contractor personnel acting on their behalf.

f. Dispatch centers will be monitored 24 hours a day. The system will provide an audible and visual alarm identifying the affected area. Dispatch centers will be designated as

restricted areas, in accordance with this Order and be properly protected, with controlled access. Where practical, alarm consoles and central dispatching will be consolidated. New construction will include ballistic protection.

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

(1) 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 3 minutes.

(3) AA&E storage facilities will be responded to within 10 minutes.

h. An electronic running 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. This electronic log can be a system log that requires no action on the part of the MCESS Operator; however, in the absence of a system generated electronic log the MCESS Operator will be required to maintain an alarm log. Alarm logs will be maintained for a period of three years and will be reviewed to identify and correct trends, reliability problems, and/or equipment failures.

i. A log-file and database backup will be made and stored in the physical security office on a monthly basis. Backups will be maintained for a period of three years.

j. The hard drives of each computer on the MCESS Domain will be imaged semi-annually. The three most recent images will be kept in the physical security office.

k. Security Division (PS) is not authorized to fund the procurement and installation of ESS in military/civilian housing. Funding for military/civilian housing ESS must be sought from the Housing Appropriation.

4. All alarm notifications aboard the installation, responded to by interior guard, military police, or MCCLEP personnel will annunciate at PMO. Existing ESS not compatible with the MCESS will not annunciate at PMO, but will annunciate at an off base

location staffed with personnel capable of notifying PMO of an alarm. These systems may be used until the end of life cycle, or 2012, at which time the system will be replaced with a new MCESS compatible system per paragraph 6003.3.a & b.

5. The provost marshal's physical security chief will manage all access codes for the MCESS. His/her level of access will be dependent on the capabilities of the MCESS; however, the physical security chief will always be assigned the highest level allowable, with all other persons being subordinate. Only the physical security chief will assign access levels for subordinate personnel.

6. 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.

5 Jun 09

(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 that requires documentation for tracking purposes.)

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 (USMC ESS)
- (6) Account, Line, RTU Address, and Zone numbers
- (7) Brief description of failure
- (8) Circumstances of failure

c. Response to a priority 1 and 2 trouble call (compensatory measures have been implemented) may be in the form of a phone call from the MCESS TSA within four hours of notification.

d. Response to a priority 3, 4, and 5 trouble call, may be in the form of a phone call from the MCESS TSA, and will be made 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.

7. The following requirements apply to all MCESS and non-MCESS systems aboard Marine Corps installations:

- a. Computerized ESS will be safeguarded against tampering.

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 emergency power to ensure continuous operation. Emergency power will be provided by an uninterrupted power source (UPS). At a minimum it will be a battery source with the capacity to maintain proper operation of the system under normal conditions for a minimum of four hours, except for AA&E sites which require a minimum of eight hours capacity. Critical areas may require an UPS supported by a generator to maintain emergency power requirements.

d. Keyswitches, controllers, or other mechanisms used to activate and deactivate the ESS and other components associated with an alarmed facility (sensors, transmitters, transponders, and control units) will be installed inside the protected area whenever possible. Components mounted on the exterior will be provided protection with a locking assembly or an anti-tamper device. Delay devices are installed to allow sufficient time for personnel to enter or exit the facility without transmitting an intrusion alarm.

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 ESS will have a primary and secondary (back-up) means of communication. Each line of communication will be separate and independent from the other (i.e. not physically located within the same fiber cable).

8. Security Division (PS) will fund the MCESS TSA to perform installation/command ESS cost estimates for MCESS requirements. All requests will be forwarded to Security Division (PS) via the installation PMO Physical Security Section.

a. Requests for cost estimates must contain the following information:

(1) Type of cost estimate requested (i.e., CCTV, AACS, IDS, MNS, etc.)

- (2) Location where equipment is to be installed
 - (a) Installation
 - (b) Type of facility (armory, flight line, etc.)
 - (c) Bldg number or Project number for MILCON
- (3) Requirement (i.e. applicable order)
- (4) Equipment Procurement and Installation Funding Source (Site or Headquarters Marine Corps (HQMC))
- (5) Date of requested installation
- (6) Any other amplifying information

b. Cost estimate request approvals, by Security Division (PS), are not an indication that funding is available for design, procurement or installation.

c. Cost estimate requests can be forwarded to Security Division (PS) via e-mail, naval correspondence, or the Electronic Security System Information Management System (ESSIMS).

6004. TYPES OF SYSTEMS

1. Local Alarm. Local alarms actuate a visible and/or audible alarm and are usually located on the exterior of the facility. Alarm transmission lines do not leave the facility. Response is generated from security forces in the immediate area or, in the absence of security forces, may only be generated upon notification from an individual passing through the area. Maintenance is conducted through a civilian agency. Local alarms must be connected to a central monitoring station.

2. Central Station. Central station system signals annunciate in an independent monitoring station that records activations and maintains the on site equipment. A civilian firm capable of providing a 24-hour armed response generally manages central stations. Connection to the station is primarily over leased telephone lines. Central station monitoring requires a contract that may include a lease/purchase clause with the civilian agency, and will address maintenance support.

3. Police Connection. Police connection systems annunciate in a local police 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. System maintenance 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 a Dispatch Center that is monitored 24 hours a day by military police and civilian employees. Military police or civilian law enforcement personnel are the primary response force. In some cases interior guard personnel may serve as the response force. Maintenance for the proprietary MCESS 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 will receive semi-annual preventive maintenance service. All performed maintenance will be recorded and records will be maintained for a period of three 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) semiannually, with the exception of AA&E storage areas, which will be tested quarterly to ensure systems and components are functional. Semi-annual preventive maintenance, performed by the MCESS TSA contracted maintenance technician(s), meets semi-annual testing requirements as long as all alarm points are tested, and test results (electronic or hard copy with signature) are maintained by physical security for three years. 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 years. For perimeter (flight line) ESS, randomly selected zones should be tested daily and include touching the fence, walking or running over protected ground, or passing through a sensor beam. All tests for ESS components will be coordinated with PMO prior to conduct of the test. Any component malfunction or other issue during testing will be provided to the physical security section.

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. Performing maintenance on non-MCESS equipment subject 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 certified.

1. Physical Security Specialist

a. Physical security specialists 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 specialists will be trained, tested, and certified by either the 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.

2. MCESS Operators

a. MCESS operators, synonymous with PMO Dispatcher, are required to be trained, tested, and certified in the operation of the MCESS. All certification records will be maintained on file for three years.

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.

4. Refresher training will be conducted for one of following reasons:

a. An update to the MCESS that impacts the responsibilities of the MCESS operator.

b. The MCESS operator hasn't performed operator duties within the last 90 days.

c. MCESS operators who transfer from one installation to another will be required to receive installation specific familiarization training.

6007. MCESS OPERATOR RESPONSIBILITIES. MCESS Operators are the first line of defense against unlawful entry into areas or against critical assets protected by the MCESS. They are 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 status.

c. Process alarms and dispatch 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. The role of Closed Circuit Television (CCTV) systems is progressively expanding in security and law enforcement applications. The roles can be

broadly categorized as detection, area surveillance, and post incident assessment and analysis. Furthermore 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 remain major factors in achieving quality video assessment systems. The following paragraphs address major areas of concern, and provide guidance for effective design, installation, and operation of a CCTV System.

1. POLICY

a. CCTV Systems will not be utilized to meet constant surveillance requirements, unless they are connected to an event driven IDS with immediate notification and recording capability.

b. Procurement of any commercial CCTV Systems monitored by PMO, to supplement or replace existing CCTV Systems, must be compatible with the MCESS 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.

c. Procurement, installation and maintenance for all CCTV Systems will meet standardization requirements as outlined in paragraph 6003.3.

d. MCESS TSA must approve design and performance parameters prior to the installation, integration, or connection to the MCESS. Systems failing to meet certification and performance parameters established by the MCESS TSA will not be connected to the MCESS.

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

f. Sustainment maintenance will be funded by Security Division (PS) on all CCTV Systems, including systems locally installed, as long as the MCESS TSA performs the installation.

g. The following requirements apply to all MCESS and non-MCESS CCTV Systems aboard Marine Corps installations:

(1) CCTV transmission will be point-to-point connectivity utilizing a fiber optic or coaxial transmission method. Wireless and networked CCTV systems are not authorized for security CCTV unless encrypted using a National Institute of Standards and Technology (NIST) approved algorithm with a key length no shorter than 128 bits. Additionally, MCESS TSA will approve wireless and networked CCTV security systems designs. Security CCTV will not be viewable or transmitted on non-MCESS networks or viewable on computers via the worldwide web.

(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) Locally installed wireless CCTV Systems not connected to the MCESS, will be encrypted to the NIST 128.0 bite standard.

(2) CCTV Systems used in conjunction with IDS will have emergency power to ensure continuous operation. Emergency power will be provided by an uninterrupted power source. At a minimum it will be a battery source with the capacity to maintain proper operation of the system under normal conditions for a minimum of four hours. Critical areas may require an UPS supported by a generator to maintain emergency power requirements.

(3) Security cameras used for forensic purposes or event driven incidents 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) Monitoring displays will be designed with the operator in mind. Monitors will be placed in such a manner that the operators attention is drawn to the monitor in the case of an event, but not be so consuming that the operator might miss something.

(a) Event driven CCTV is the preferred method of monitoring. The preferred location of event driven CCTV

monitors is in the peripheral vision, to the right and left, of the MCESS operator.

(b) Some applications require event driven CCTV monitoring. Event driven CCTV monitors may be installed in the direct view of duty or dispatch personnel.

(c) The MCESS operator will have the ability to pull up, on command, any CCTV connected to the MCESS; however, normally the MCESS operator will not be tasked with the continued viewing of event driven CCTV monitoring.

(5) CCTV monitoring and recording devices will not be located in gatehouses, with the exception of under-vehicle inspection system monitors, and monitors used in conjunction with AACS.

h. Security CCTV systems that provide monitoring of Marine Corps installations, assets, personnel, or procedures will not be transmitted off the installation or to outside agencies.

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, it must be noted 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) ensure cameras are equipped with environmentally sealed housings, 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 (as human eyes do), planners and designers must avoid placements in the path of the sun and moon. Bright objects cause the iris to narrow and reduce the amount of light allowed to reach the camera's sensing element. Dark places will appear darker and scene visibility can be reduced to zero.

(a) The same principles apply to man-made illumination and will be given the same consideration. Street lights, flood lighting, and headlights within the camera's field of view (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 must 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 will 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 analog and digital. 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, planners and designers need to examine camera qualities that meet their requirements and have a full understanding of their 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. 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

5 Jun 09

infrastructure costs rise significantly. 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. Digital images can 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.

(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 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 on the resolution requirements and the distance from the camera's position and the object(s) to be viewed.

(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 is required 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 is 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.

(4) 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. 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. A Local Area Network (LAN) is sometimes used to further reduce costs; however, the use of non-MCESS LAN viewable CCTV is not authorized aboard Marine Corps installations for security. 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.

(5) 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 liquid-crystal display (LCD) and plasma convert analog signals to digital, which means slower speeds than the conventional cathode-ray tube (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.

(6) 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 human operation considerations 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. The majority of detection cameras relate to motion and data is presented only when undesired activity occurs, drawing the operator's attention to a scene. It is important that information is presented to an operator only when his/her attention is required. Normal activity that triggers a sensor or prompts operator attention results in information overload (false alarms), and will tend to be ignored. Monitors should be located within the peripheral vision of the operator. Since many cameras may be assigned to this category, but only used when an event occurs, operator fatigue is not as critical a factor. Video motion detectors and event-driven switching matrices are key in this approach. Designers will pay strict attention to factors affecting false alarm rates so as not to overload an operator with meaningless data. If the camera is a Pan-Tilt-Zoom (PTZ), operators need to possess the skills and knowledge to rapidly manipulate the camera's view.

(b) Surveillance Cameras. Surveillance cameras are typically provided to an operator with a live connection for constant assessment capabilities. In this application, workload on the operator is significantly increased. The amount of video data being presented to an operator must be considered. When multiple cameras are used, additional manpower will be required

5 Jun 09

to adequately assigned areas. The use of "scroll-through" or "cycle" cameras (in a pre-determined order and rate) may be used. This application is not recommended because with each subsequent switch to a new camera, the operator must orient himself to the new scene and determine if there have been changes from the last time the scene was presented.

1. Using multiple monitors may alleviate some problems, but introduces others. If multiple monitors are assigned, a single operator is required to split his/her attention between the various monitors. Information can be easily missed because each monitor is presenting different scenes every one to three seconds. This activity can be mentally fatiguing and the amount of time an operator remains in this mode becomes critical. Statistically operator performance begins to degrade after approximately 30 minutes. The likelihood of an undesired event being seen can diminish to as little as 50% of the time.

2. Security officers need to be aware of these limitations and must review requirements for all applications. The number of camera applications will be limited to what is absolutely necessary to reduce manning requirements for monitoring.

(c) After-Action Assessment Cameras. This category requires little or no attention from the operator. Cameras often have their output directed to a video storage unit (i.e. Digital Video Recorder (DVR), hard drives, or tape). The challenge is to select video storage equipment capable of quickly retrieving useful information.

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

influences will reduce the effectiveness of the operator. Facility design and policies and procedures must be considered to increase proficiency.

2. Control room layout is 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 will be intuitive to an operator and not require complicated actions to bring an image to his/her attention. Pan, tilt, and zoom controls should also require no special dexterity for viewing areas of significance and be incorporated into a single control unit. Control room lighting will be selected to reduce glare.

3. To be effective, operators must be familiar with the areas they are assigned to view. Initial and on-going training programs will be developed to ensure that MCESS Operators are familiar with system design, principle landmarks, and/or special circumstances (e.g., construction projects). Operators should be aware of distances between the camera location and significant points within its field of view. Operators often 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. Per references (y) through (aa), the DOD Common Access Card (CAC) will be the principle access control token for buildings, facilities, installations, and controlled spaces. As such:

- a. All newly installed AACS will utilize the CAC.
- b. Existing systems will migrate to the CAC.
- c. AACS connected to the MCESS will be brought into compliance immediately.
- d. Activities with an AACS, that will not be compliant with paragraphs (a) through (c) above, will report non-compliance to Security Division (PS).

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

2. All AACS(s) will be DOD Personnel Identity Protection (PIP) Program compliant, per reference (z). PIP authenticates an individual's identity by:

a. Binding an identity to an identity protection system through the issuance of a DOD credential;

b. Linking the credential to an individual through use of a unique identifying characteristic and a personal identification number; and

c. Digitalizing the authentication of the identification credential link to the individual.

3. All AACS will be compliant with references (y) through (aa), and will use one of the following types of credentials:

a. DOD Common Access Card

b. Military ID Card (TESLIN) for dependants, retirees, and inactive reserve members

c. DOD approved "third" card installation access credential

d. Installation or Service specific card issued to service providers (e.g. contractors, vendors, who require routine access to the installation)

4. The magstripe technology on the CAC will be utilized for all Marine Corps AACS. The Marine Corps AACS will be upgraded as new technologies become available on future CAC designs and capabilities/technologies. Future systems must be Federal Information Processing Standard 201-1 (FIPS 201-1) compliant and include ISO 14443 contactless technology.

5. With the exception of billeting, all buildings, facilities, installations, and controlled spaces will adhere to the following:

a. The SEIWG 012 credential will be encoded on track two of the magstripe.

5 Jun 09

b. Encoding of the CAC magstripe will be performed by the local PMO for AACS connected to the MCESS, or the facility manager for those AACS not 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 Security Division (PS) MCESS TSA. AACS, other than those connected to the MCESS, must obtain a 4-digit system code by contacting HQMC, Security Division, Physical Security Chief at DSN 222-4333/4496.

6. 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.

7. Personnel requiring access that are not authorized the issuance of a CAC will be issued a DOD approved "third" card.

8. Supplemental badging systems (flash badges) considered necessary for an additional level of security not presently afforded by the CAC (e.g., entrance into 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. These badges will be solely used for further identification purposes of person(s) within the controlled space.

b. Supplemental badges will not contain a magstripe that can be encoded.

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.

9. Biometrics will only be used in conjunction with the CAC as an identity verifier and not as a primary access control token. PINs may be used in conjunction with the biometrics.

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 DOD components are required to provide mass notification capability. This Order defines requirements for implementation of MNS aboard Marine Corps installations.

1. Mass notification is required in all new inhabited buildings, including new primary gathering buildings and new billeting. Mass notification is required in existing inhabited and primary gathering buildings and existing billeting when implementing a project exceeding the replacement cost threshold specified in reference (i). Mass notification is required for leased buildings, building additions, and expeditionary and temporary structures as identified in reference (i).

2. MNS falls under the MCESS Program, for which Security Division (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 PM. This requirement does not apply to Marine Forces Reserve (MARFORRES).

5. Procurement and installation of a MNS for non Security Division (PS) funded facilities by an installation/command, requires local installations to obtain proper funding. The MCESS TSA or a local contractor (approved by the MCESS TSA) will perform all installations. Identified local contractors will provide an IDP to the MCESS TSA for approval. Final connectivity to the PMO Dispatch Center will be accomplished/supervised by MCESS TSA personnel.

6. Installations, commands, or responsible agencies that elect to utilize the MCESS TSA to install a MNS with funding obtained

locally, Security Division (PS) will provide the sustainment maintenance and life cycle upgrade.

7. General. Reference (j) contains additional and amplifying information on MNS.

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 or cell-phone by mobile security forces. A text message notification appliance may be used.

b. The base-wide control system will provide redundant (primary and backup) central control units. The Provost Marshal's Dispatch Center 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 of 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 Security Division (PS).

g. The provost marshal will conduct monthly base-wide tests of the MNS. Testing results will be recorded and maintained for 3 years in the physical security office. Additional testing requirements are identified in paragraph 6005.4.

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 Order cannot be strictly applied. Therefore, the Commander, Marine Forces Reserve will incorporate the policies of this Order where applicable. In all other cases, the spirit and intent of this Order will be adhered to wherever possible. For Marine Corps Reserve Centers, where there is no government response force available, the system may be a police connection or central monitoring station from which a response force can be dispatched. Telephone answering services will not be utilized. All requirements for clarification will be addressed to Security Division (PS).

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 7

CRITICAL ASSET PROTECTION

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|--|------------------|-------------|
| INTRODUCTION | 7000 | 7-3 |
| PRIORITIZATION OF ASSETS | 7001 | 7-3 |
| FLIGHT LINE SECURITY (FLS) | 7002 | 7-5 |
| SECURITY OF PETROLEUM ASSETS | 7003 | 7-9 |
| SECURITY OF COMMUNICATIONS FACILITIES . | 7004 | 7-11 |
| WATERSIDE SECURITY | 7005 | 7-12 |
| CLASSIFIED INFORMATION STORAGE AREAS . . | 7006 | 7-19 |
| SECURITY OF SELECTED SENSITIVE INVENTORY ITEMS, DRUGS, DRUG ABUSE ITEMS, AND PRECIOUS METALS | 7007 | 7-30 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 7

CRITICAL ASSET PROTECTION

7000. INTRODUCTION. A critical asset is defined as a DOD or non-DOD military related unit, organization, facility/ installation, system, resource, equipment, or instrument considered essential to DOD operations. They perform an essential service, function, or use in peace, crisis, and war. They must be included in military operational plans or in support of operational plans. Critical assets include traditional physical facilities and equipment (communication, power, water, and fuel), non-physical assets (software systems) and those distributive in nature (command and control networks, wide area networks or similar computer-based networks). Critical assets may fall under the cognizance of DOD or another government agency can be public or privately owned and/or operated by either a DOD or non-DOD entity, domestic or foreign. These assets warrant continued command attention in addition to measures and precautions to ensure continued efficient operation, protection from disruption, degradation, or destruction and timely restoration. Disruption to operation, or loss, of an asset would render the asset ineffective or otherwise seriously disrupt DOD or Service operations.

1. Assets must be identified and recognized at all levels; unit, organization, facility, or installation. 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, the Resource and Asset Prioritization Chart provides 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

| SECURITY SYSTEM LEVEL | ASSET DEFINITION | ASSET EXAMPLE |
|---|---|--|
| <p style="text-align: center;">A</p> <p>INTEGRATED ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, ACCESS DELAY AND DENIAL SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED IMMEDIATE RESPONSE FORCES</p> | <p style="text-align: center;">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 style="text-align: center;">B</p> <p>ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED RESPONSE FORCES</p> | <p style="text-align: center;">THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD BE EXPECTED 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 TEST ASSETS</p> |
| SECURITY SYSTEM LEVEL | ASSET DEFINITION | ASSET EXAMPLE |
| <p style="text-align: center;">C</p> <p>ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIERS, SECURITY PATROLS, DESIGNATED RESPONSE FORCES</p> | <p style="text-align: center;">THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD IMPACT UPON THE TACTICAL CAPABILITY OF THE UNITED STATES</p> | <p>NONALERT RESOURCES AND ASSETS</p> <p>PRECISION GUIDED MUNITIONS</p> <p>COMMAND, CONTROL AND COMMUNICATION FACILITIES AND SYSTEMS</p> <p>CATEGORY II ARMS, AMMUNITION, AND EXPLOSIVES</p> <p>PETROLEUM, OIL, LUBRICANT (POL)/ POWER/WATER/SUPPLY/STORAGE FACILITIES</p> |
| SECURITY SYSTEM LEVEL | ASSET DEFINITION | ASSET EXAMPLE |
| <p style="text-align: center;">D</p> <p>ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED RESPONSE FORCES</p> | <p style="text-align: center;">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>EXCHANGES 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.—Resource and Asset Prioritization Chart

requirements including, but not limited to, access control, personnel and vehicle inspections, and increased security requirements in accordance with FPCONS and contingencies.

2. In order to establish security priorities, commanders need to be aware of threats to installation resources and critical assets. Figure 7-2 provides a threat matrix for commanders to use 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, 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.

| Threat Type | Threat Description | Threat Example |
|---------------------|---|--|
| Maximum | Individual in organized and trained groups alone or with assistance from an insider; skilled, armed, and equipped with penetration aids | Terrorists 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; terrorists or paramilitary forces; foreign intelligence agents with access |
| Intermediate | Career criminal; individuals(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; some terrorist groups |
| 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

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

- a. Whether the installation is open or closed.
- b. If the installation has a defense in depth posture.
- c. Personnel and vehicular access to the flight line.
- d. If the flight line is adequately fenced, lighted, and posted.
- e. The use of ESS in conjunction with physical security barriers, devices, and procedures.
- f. Available manpower and equipment response capabilities.

2. Aircraft Parking Areas. Plans for establishing aircraft parking areas will address 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.

3. 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, flight lines, aircraft, aircraft parking areas, and hangars require surveillance. CCTV

5 Jun 09

surveillance used in conjunction with IDS is encouraged, however, in the absence of electronic surveillance equipment, security personnel will be assigned.

d. CCTV surveillance equipment used in conjunction with an IDS must annunciate at the security force dispatch center and include an event driven recording with assessment capabilities.

e. The use of CCTV surveillance equipment is not designed to reduce manpower, but to enhance the security force capability to perform its security mission.

4. Flight Line Restricted Access. Access control for the flight line is designed to prevent 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 ACPs and ECFs manned by security force personnel, or those controlled by an 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). Emergency vehicles will not be impeded, and security personnel will render assistance as directed.

c. Government vehicles authorized on the flight line will be clearly marked for easy recognition. 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.

5 Jun 09

g. Privately owned vehicles are prohibited from entering all flight lines, and all restricted areas within the flight line.

h. Flight line perimeter clear zones will be designed to ensure that the required standoff is provided and clear zones maintained. This includes POV parking areas.

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 Order.

7. Emergency Situations. A National Defense Area (NDA) will be established in any emergency involving an asset that has been forced to land, or has crashed, 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, for the purpose of safeguarding classified defense information or protecting government equipment and/or material. Establishing a NDA temporarily places non-federal lands under the effective control of the Department of Defense and can only be established as a result of 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 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 investigation.

8. Transient Aircraft. MCAS and MCAF commanders will ensure 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. 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 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 will be limited to those personnel authorized by the aircraft commander. Transient aircraft commanders are required to identify an significant security requirements or priorities to the host installation command staff and security personnel.

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.

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 AACS 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.

5 Jun 09

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

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 POL 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 include tactical and garrison motor pools where large amount of POL stocks are maintained.

a. Installation 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.

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 security device (credit card type device, coded keys, etc).

5 Jun 09

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.

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

3. Fuel Issue Points. Fuel issue points are those points on the installation that are used strictly to refuel government vehicles. This includes single and multiple pump fuel islands and/or stations.

a. Fuel issue points and individual pump islands will be provided security lighting during the hours of darkness.

b. Power switches will be secured to prevent tampering.

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

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

7004. SECURITY OF COMMUNICATION FACILITIES. Communication systems play a major role in the Marine Corps mission by providing essential communications in garrison and expeditionary environments. Security is required for communications facilities and systems to ensure continuity of operations for critical facilities and systems they support. 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 AACS 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 hours of darkness.

d. Key control will be established per paragraph 3005.

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.

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 limited waterside/waterway security zones and areas, cognizant agencies that assist in their establishment, and information for each Limited Waterway Area.

2. Waterside Assets. The following assets are common at installations with waterside/waterfront property(s):

- a. Passenger and cargo vessels
- 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 waterside facility and asset security by erecting perimeters and

| AREA | AGENCY | AUTHORITY | LIMITATION | 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 | Felony 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 6.01-5 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. | 50 USC 192 Felony - 10 years/ \$10, 000 | USCG only. Marine Corps may patrol under COTP authority. | Threat required. COTP control 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) |

Figure 7-3.--Limited Waterway Areas

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).

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

5 Jun 09

(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 (C&E) 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.

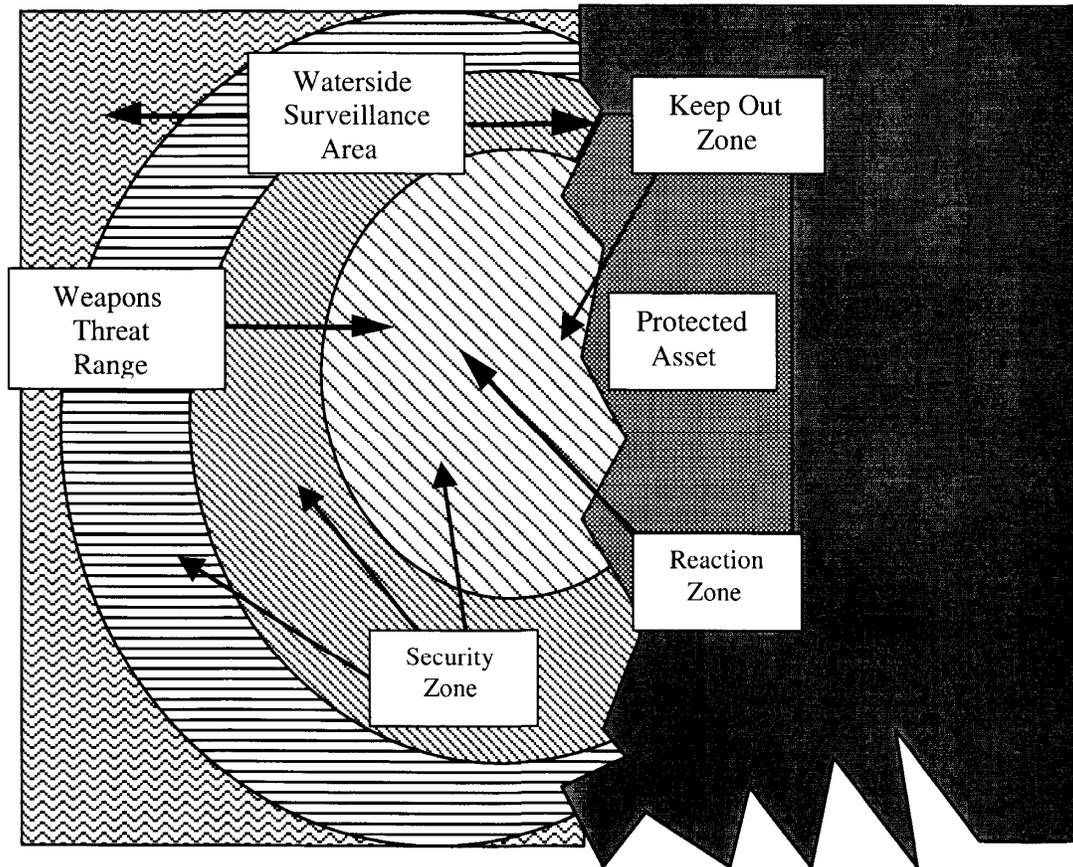


Figure 7-4.-Waterside Security Zones

(1) Several barriers can be used to slow or impede access to facilities by boats or swimmers. Nets are among the best for this purpose, however, well-marked partially submerged objects can also be used; there are legal implications regarding the emplacement of barriers that constitute a hazard to navigation. Prior to placement of these devices, commands will consult with the command SJA.

(2) 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.

5 Jun 09

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 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. 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 will 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 most cases boarding will take place outside the security zone at a secure location.

6. Patrol Tactics and Techniques. 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. Random patrolling is an effective defensive measure 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. Response and Use of Force Considerations. The first level of response in waterfront security is to notify transiting vessels of the security zone(s) and determine their intentions. Non-aggressors will simply be escorted out of the area. The utilization of tactics and techniques outlined in this section will provide a system for effectively responding to a wide range of threats. In an effort to ensure the safety and security of Marines assigned to waterfront security patrols, coordination is required with local, state, federal, and host nation law enforcement and legal organizations.

a. In a Continental United States (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, Rules of Engagement (ROE)/Rules for the Use of Force (RUF) will be promulgated to address the specific threat, and will be briefed to all Marines performing waterfront security duties.

8. 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 may not be 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.

9. Pier, Hull, and In-Water Structure Inspections. Pier, hull, and in-water structure inspections will be conducted on a periodic random basis. Other at risk structures such as navigation aids, bridges, utility cable towers, tunnels, etc. should also be inspected on a periodic, random basis. Frequency of inspections should be increased on the basis of increased FPCONS. Prior to a ship's arrival, 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 will inspect the pier area and ship's hull randomly.

7006. CLASSIFIED INFORMATION STORAGE AREAS. Physical security surveys for classified information storage areas (excluding SCIF(s)) will address structural and ESS requirements of reference (d). ESS will be addressed as they are the responsibility of the Provost Marshal's Office. Physical security surveys will identify the area (e.g. secure room, vault), and address structural and ESS requirements only. Installation information security managers will address further requirements of references (d) and (e). All matters concerning

5 Jun 09

classified information storage areas will be addressed to the Security Division (PS).

1. Commanding Officers must ensure that all classified information is stored in a manner that will deter or detect access by unauthorized persons. Classified information will be stored in accordance with reference (d) and this section. Classified information storage areas, under the personal observation of cleared and authorized persons, are still required to meet the construction requirements of reference (d). To the extent possible, these areas will be limited and current holdings reduced to the minimum required for mission accomplishment.

2. Weapons or sensitive items, such as money, jewels, precious metals, or narcotics will not be stored in the same security containers used to store classified information.

3. There will be no external markings revealing the classification level of information stored in a specific security container, vault, or secure room. Priorities for emergency evacuation and destruction will not be marked or posted on the security container. This does not preclude placing a mark or symbol on the security container for other purposes or applying decals or stickers required by the Director, Central Intelligence (DCI) for security containers used to store or process intelligence information.

4. Storage Requirements. Classified information not under the personal control or observation of an appropriately cleared person will be guarded or stored in a locked GSA-approved security container, vault, modular vault, or secure room (open storage area constructed per paragraph 7006 5b).

a. Store Top Secret information in the following method:

(1) In a GSA-approved security container equipped with a lock meeting Fed Spec FF-L-2740 and one of the following supplemental controls;

(a) The location housing the security container will be subject to continuous protection by cleared guard or duty personnel.

(b) An IDS with personnel responding to the alarm within 15 minutes of the alarm annunciation.

5 Jun 09

(2) In an open storage area (secure room or vault), equipped with an IDS, with a security response force capable of responding to the alarm within 15 minutes of the alarm annunciation.

b. Store Secret information by one of the following methods:

(1) In the same manner prescribed for Top Secret;

(a) In a GSA-approved security container equipped with a lock meeting Fed Spec FF-L-2740 in a modular vault or vault without supplemental controls; or

(b) In an open storage area (secure room) with one of the following supplemental controls;

1. The location housing the open storage area is subject to continuous protection by cleared guard or duty personnel;

2. Or an IDS with response time within 15 minutes of alarm annunciation.

(2) New lock-bar cabinets cannot be fabricated from either existing or new containers, nor will any existing lock-bar container, not previously used for the protection of classified information be put into use for that purpose.

c. Store Confidential information in the same manner prescribed for Top Secret or Secret except that supplemental controls are not required.

d. Under field conditions during military operations, the Commanding Officer may require or impose security measures deemed adequate to meet the storage requirements outlined in paragraphs a through c, commensurate to the level of classification.

e. Chapter 8 provides requirements for storing classified AA&E items too large to store in GSA-approved containers.

f. Storage areas for bulky material containing Secret or Confidential information may have access openings secured by GSA-approved combination padlocks (Fed Spec FF-P-110 Series), or high security key-operated padlocks (MIL-P-43607). If these

storage requirements cannot be met afloat or aboard aircraft, Secret or Confidential information may be stored in a locked container constructed of metal or wood (such as a foot locker or cruise box) secured by a GSA-approved padlock meeting Fed Spec FF-P-110. The area in which the container is stored will be locked when not manned by U.S. personnel and the security of the locked area checked once every 24 hours.

g. Entrances to vaults or secure rooms will be under visual control during duty hours to prevent entry by unauthorized personnel, or equipped with electric, mechanical, or electromechanical access control devices to limit access. Electrically actuated locks (e.g., cipher and magnetic strip card locks) do not afford the required degree of protection for classified information by themselves and will not be used as a substitute for the locks prescribed in this section.

h. Periodically examine existing areas and promptly repair correctable defects. Existing approved vaults and secure rooms do not require modification to meet current standards.

i. GSA-approved modular vaults meeting Fed Spec AAV-2737 may be used to store classified information as an alternative to vault requirements as described in paragraph 5a of this section.

j. Figure 7-5 is the priority list for replacing existing mechanical combination locks with locks meeting Fed Spec FF-L 2740. The mission and location of the command, the classification level and sensitivity of the information, and the overall security posture of the command determines the priority for replacement of existing combination locks. All system components and supplemental security measures including IDS, automated access control subsystems, video assessment subsystems, and level of operations shall be evaluated when determining the priority for replacement of security equipment. Priority I requires immediate replacement.

k. New purchases of combination locks shall conform to Fed Spec FF-L-2740. Existing mechanical combination locks will not be repaired. They will be replaced with locks meeting Fed Spec FF-L-2740.

| PRIORITY FOR LOCKS REPLACEMENT | | | | |
|--|--------|----|-------|-----|
| Priorities range from 1 to 4, with 1 being the highest and 4 the lowest. | | | | |
| LOCK REPLACEMENT PRIORITIES IN THE U.S. AND ITS TERRITORIES | | | | |
| ITEM | TS/SAP | TS | S/SAP | S-C |
| Vault Doors | 1 | 1 | 3 | 4 |
| Containers(A)* | 3 | 4 | 4 | 4 |
| Containers(B)** | 1 | 1 | 1 | 2 |
| Crypto | 1 | 1 | 2 | 2 |
| LOCK REPLACEMENT PRIORITIES OUTSIDE THE U.S. AND ITS TERRITORIES | | | | |
| ITEM | TS/SAP | TS | S/SAP | S-C |
| Vault Doors | 1 | 1 | 2 | 2 |
| Containers(A)* | 2 | 2 | 3 | 3 |
| Containers(B)** | 1 | 1 | 1 | 2 |
| Crypto | 1 | 1 | 2 | 2 |
| High Risk Areas | 1 | 1 | 1 | 1 |
| *A-Located in a controlled environment where the DoD has the authority to prevent unauthorized disclosure of classified information. The U.S. Government may control or deny access to the space, post guards, require identification, challenge presence, inspect packages, program elevators, or take other reasonable measures necessary to deny unauthorized access. | | | | |
| **B-Located in an uncontrolled area without perimeter security measures. | | | | |

Figure 7-5.—Combination Lock Replacement Priority

5. Vault and Secure Room (Open Storage Area) Construction Standards

a. Vault

(1) Floor and Walls. Eight inches of reinforced concrete to meet current structural standards. Walls will extend to the underside of the roof slab.

(2) Roof. Monolithic reinforced concrete slab, with the thickness determined by structural requirements, but no less than the floors and walls.

5 Jun 09

(3) Ceiling. The roof or ceiling will be reinforced concrete of a thickness to be determined by structural requirements, but not less than the floors end walls.

(4) Doors. Vault door and frame units will conform to Federal Specification AA-D-2757, Class 8 vault door, or Federal Specification AA-D-600, Class 5, vault door. Doors will be equipped with a built-in GSA-approved combination lock meeting Fed Spec FF-L-2740.

b. Secure Room

(1) Walls, Floor, and Roof. Walls, floor, and roof construction will be of permanent construction materials; plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls will extend to the true ceiling with permanent construction materials, wire mesh, or 18-gauge expanded steel screen.

(2) Ceiling. Ceilings will be constructed of plaster, gypsum, wallboard material, hardwood, or any other acceptable material.

(3) Doors. The access doors to the room will be substantially constructed of wood, metal, or other solid material and equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740. For open storage areas approved under previous standards, the lock may be a previously approved GSA combination lock until the door has been retrofitted with a lock meeting Fed Spec FF-L-2740. When double doors are used an astragal will be installed on the active leaf of the door. The hinge pins of the out-swinging doors will be peened, brazed, spot-welded, or equipped with a hinge secure pin to prevent removal. Doors other than access doors shall be secured from the interior (e.g., by a dead bolt lock, panic dead bolt lock, rigid wood or metal bar that extends across the width of the door, or by any other means that will prevent entry from the exterior). Key operated locks that can be accessed from the exterior side of the door are not authorized. A balanced magnetic switch meeting Underwriters Laboratory (UL) 634 standards will protect each perimeter door.

(4) Windows. All windows that might reasonably afford visual observation of classified activities within the facility will be made opaque or equipped with blinds, drapes, or other

coverings. Windows located less than 18 feet above the ground (measured from the bottom of the window), or that are easily accessible by means of objects directly beneath the windows will be constructed from, or covered with, materials which provide protection from forced entry. The windows will be protected with an IDS, either independently or with motion detection sensors in the space. Window protection does not need be stronger than the contiguous walls.

(5) Openings. Utility openings such as ducts and vents will be kept at less than man-passable (96 square inches) opening. Openings larger than 96 square inches will be hardened per reference (q).

6. Electronic Security Systems and Access Control Requirements. IDS will detect unauthorized or authorized penetration in the secure area. Existing ESS may continue to be used until upgraded or replaced.

a. Unless specified in this Order, the commanding officer is responsible for determining whether ESS is required for those areas that reasonably afford access to the container, or where classified data is stored. Prior to IDS installation, Commanding Officers will consider the threat, vulnerabilities, and in-depth security measures and perform a risk analysis.

b. Acceptability of Equipment. All ESS, including components, must be UL-listed (or equivalent) and approved.

c. Transmission Line Security. When the transmission line leaves the secured area and traverses an uncontrolled area, Class I or Class II line supervision will be used.

d. Internal Cabling. The cabling between the sensors and the Central Processing Unit (CPU) will be dedicated and must comply with national and local code standards.

e. Access Controls Systems. If an access control system is integrated into an IDS, reports from the AACS will be subordinate in priority to reports from intrusion alarms.

f. Maintenance Mode. When an alarm zone is placed in maintenance mode, this condition automatically signals the monitor station and the ESS cannot be secured while in the maintenance mode. The alarm or message must be continually visible at the monitor station throughout the maintenance

period. A standard operating procedure must be established to address appropriate actions when maintenance access is indicated. All maintenance periods will be archived in the system.

g. Annunciation of Shunting or Masking Condition. Shunting or masking of any internal zone or sensor must be appropriately logged and recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

h. Alarms Indications. Indications of alarm status will be revealed at the monitoring station and may be revealed within the confines of the secure area.

i. Power Supplies. Primary power for all ESS components will be commercial. In the event of commercial power failure at the protected area or monitor station, the equipment will change power sources without causing an alarm indication.

(1) Emergency power. Emergency power will consist of a protected independent backup power source that provides a minimum of 8-hours operating power battery and/or generator power. When batteries are used for emergency power, they must be maintained at full charge by automatic charging circuits. Manufacturer's periodic maintenance schedule will be followed and results documented.

(2) Power Source and Failure indication. An illuminated indication will exist at the Control Unit of the power source. Equipment at the monitor station will indicate a power failure, to include the location of the failure or change.

j. Component Tamper Protection. ESS components located inside or outside the secure area will be provided tamper protection.

7. Systems Requirements

a. Independent Requirement. When multiple areas are protected by one monitor station, secure room zones must be clearly distinguishable from the other zones to facilitate a priority response. All sensors will be installed within the protected area.

b. Access and/or Secure Switch and Control Unit. No capability will exist to allow changing the access status of the ESS from a location outside the protected area. All control units must be located inside the secure area and near the entrance. Assigned personnel will initiate all changes in access and secure status. Operation of the control unit may be restricted by use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space will cause an alarm to be transmitted to the monitor station.

c. Motion Detection Protection. Secure areas that reasonably afford access to an area or container or where classified information is stored will be protected with motion detection sensors (e.g., ultrasonic and passive infrared). Use of dual technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector must cause an immediate and continuous alarm condition.

d. Protection of Perimeter Doors. Each perimeter door will be protected by a balanced magnetic switch that meets UL 634 standards.

e. Windows. All readily accessible windows (within 18 feet of ground level) will be protected.

f. IDS Requirements for Continuous Operations Facility. A continuous operations facility may not require ESS. This type of secure area will be equipped with an alerting system if the occupants cannot observe all potential entrances into the room. Duress devices may be required.

g. False, and/or Nuisance Alarm. All alarms shall be investigated and the results documented. Maintenance programs will ensure false alarms incidents not exceed one incident in a period of 30 days per zone.

8. Installation, Maintenance, and Monitoring

a. Installation and Maintenance Personnel. U.S. citizens who have been subjected to a trustworthiness determination per reference (e) will accomplish alarm installation and maintenance.

b. Monitor Station Staffing. U.S. citizens who have been

subjected to a trustworthiness determination per reference (e) must supervise the monitor station continuously.

9. Access Control. Access to a facility will be accomplished by visual control or AACS (as prescribed below) at all times during working hours to prevent entry by unauthorized personnel. An employee workstation or guard may accomplish visual control. A cleared person who has been trained in facility security requirements must escort uncleared persons within the facility.

a. Automated Access Control Systems. An automated access control system may be used to control admittance during working hours instead of visual control, if it meets the AACS criteria stated in this paragraph and paragraph 9b of this section. AACS must identify an individual and authenticate the person's authority to enter the area through the use of an identification badge or card.

(1) Identification Badges or Key Cards. The identification badge or key card must use embedded sensors, integrated circuits, magnetic stripes, or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(2) Personal Identity Verification. Personal identity verification (Biometrics Devices) identifies the individual requesting access by unique personal characteristics, such as:

- (a) Fingerprinting
- (b) Hand Geometry
- (c) Handwriting
- (d) Retina scans
- (e) Voice recognition

A biometrics device may be required for access to the most sensitive information.

b. In conjunction with paragraph a(1) above, a Personal Identification Number (PIN) may be required. The PIN must be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the

5 Jun 09

individual. The PIN must be changed when it is believed to be compromised or subjected to compromise.

c. Authentication of the individual's authorization to enter the area must be accomplished within the system by inputs from the identification badge/card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer, or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than the required access level.

d. Protection must be established and maintained for all devices or equipment that constitutes the access control system. The level of protection may vary depending upon the type of device or equipment being protected.

(1) Locations where authorization data and personal identification or verification data is input, stored, or recorded must be protected.

(2) Card readers, keypads, communication or interface devices located outside the entrance to a controlled area will have tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels located within a controlled area require security protection sufficient to preclude unauthorized access to the mechanism.

(3) Keypad devices will be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

(4) Systems that use transmission lines to carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area will have line supervision.

(5) Electric strikes used in access control systems will be heavy duty, industrial grade.

e. Access to records and information concerning encoded identification data and PINs will be restricted. Access to identification or authorizing data, operating system software or any identifying data associated with the entry control system will be limited to the fewest number of personnel as possible.

Associated data or software will be kept secure when unattended.

f. Personnel entering or leaving an area are required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirmation of need-to-know and access.

g. Electric, Mechanical, or Electromechanical Access Control Devices. Electric, mechanical, or electromechanical devices which meet the criteria below may be used to control admittance to secure areas during duty hours if the entrance is under visual control. These devices are also acceptable to control access to compartmented areas within a secure area. Access control devices must be installed in the following manner:

(1) The electronic control panel containing the mechanical mechanism by which the combination is set is located inside the area. The control panel (located within the area) will require security designed to preclude unauthorized access to the mechanism.

(2) The control panel is installed in such a manner, or has a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination(s).

(3) The selection and setting of the combination is accomplished by an individual cleared at the same level as the highest level of classified information controlled within.

(4) Electrical components or mechanical links (cables, rods, etc.) are accessible only from inside the area, or, if they traverse an uncontrolled area they will be secured within protecting covering to preclude surreptitious manipulation of components.

7007. SECURITY OF SELECTED SENSITIVE INVENTORY ITEMS, DRUGS, DRUG ABUSE ITEMS, AND PRECIOUS METALS

1. The following definitions describe sensitive items:

a. 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.

b. Code "Q" Items. Drugs or other controlled substances designated as Schedule III, IV or V items, per 21 Code of Federal Regulations, Part 1308.

c. 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.

d. Precious Metals. Refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium in bar, ingot, granule, liquid, sponge or wire form.

2. Controlled Substances Inventory. Accountability, inventory and security of controlled substances shall be as prescribed in reference (ab).

3. Security Requirements for "R" Coded Items at Base/Installation Supply Level or Higher

a. "R" coded items maintained at base/installation level and higher will be stored in a vault or GSA approved security container weighing 750 pounds or greater in accordance with reference (ab). Smaller GSA approved security containers are authorized but must be securely anchored to the floor or wall. All security containers will be secured with built-in combination locks meeting Fed Spec FF-L-2740 (Mass Hamilton X-09 Series).

b. Vaults and security containers storing "R" Coded Items will have an IDS connected to a central monitoring station, with personnel on 24-hour duty who can provide a rapid armed response to an alarm signal.

c. Access to storage areas, including containers, will be kept to a minimum and all personnel authorized access will be assigned in writing. Access to the storage area will be maintained in an access control logbook. Completed logbooks will be maintained for a period of three years.

4. Security Requirements for "Q" Coded Items at Base/Installation Supply Level or Higher

a. The preferred storage for sensitive inventory items coded "Q" is in vaults or GSA approved security container weighing 750 pounds or greater.

b. Small quantities may be stored in security containers approved for items coded "R". Larger or bulk quantities may be stored in a Level Three Restricted Area as described in paragraph 3003. The storage area will have an IDS which is connected to a central monitoring station with personnel who can provide rapid armed response to an alarm signal.

c. Storage facilities and procedures for operation will be adequate to ensure the prevention of fire, explosion, accident, or overexposure of personnel using the areas.

d. Access to storage areas will be kept to a minimum and all personnel authorized access will be assigned in writing. Access to the storage area will be maintained in an access control logbook. Completed logbooks will be maintained for a period of three years.

5. Security Requirements for "R" and "Q" Coded Items for Small Units/Individuals

a. The preferred storage for sensitive inventory items coded "Q" is in vaults or GSA approved security container weighing 750 pounds or greater.

b. Small quantities may be stored in security containers approved for items coded "R". Larger or bulk quantities may be stored in a Level Three Restricted Area as described in paragraph 3003. The storage area will have an IDS connected to a central monitoring station with personnel who can provide rapid armed response to an alarm signal.

c. Storage facilities and procedures for operation shall be adequate to ensure the prevention of fire, explosion, accident, or overexposure of personnel using the areas.

d. In a field environment or in the absence of proper facilities, small units are authorized to maintain minimum required stock in a 750 pound or heavier GSA approved security container. As a last resort, smaller GSA approved security containers are authorized but must be securely anchored or provided continuous surveillance. These containers must be located within a continuously manned space or checked by security personnel twice per 12 hour shift.

e. Access to storage areas will be kept to a minimum and all personnel authorized access will be assigned in writing.

MCO 5530.14A
5 Jun 09

Access to the storage area will be maintained in an access control logbook. Completed logbooks will be maintained for a period of three years.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 8

SECURITY OF ARMS, AMMUNITION, & EXPLOSIVES (AA&E)

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|--|------------------|-------------|
| GENERAL | 8000 | 8-3 |
| PRIORITY | 8001 | 8-7 |
| PERSONNEL | 8002 | 8-7 |
| ACCOUNTABILITY AND INVENTORY | 8003 | 8-12 |
| AA&E STORAGE FACILITIES (SPECIAL REQUIREMENTS) | 8004 | 8-18 |
| SECURITY OF ARMS | 8005 | 8-21 |
| SECURITY OF AMMUNITION & EXPLOSIVES (A&E) | 8006 | 8-28 |
| FENCES | 8007 | 8-31 |
| AREA DESIGNATION AND ACCESS CONTROL . . . | 8008 | 8-31 |
| ELECTRONIC SECURITY SYSTEMS | 8009 | 8-32 |
| KEY SECURITY AND LOCK CONTROL | 8010 | 8-33 |
| SURVEILLANCE AND SECURITY CHECKS | 8011 | 8-35 |
| SECURITY LIGHTING | 8012 | 8-35 |
| COMMUNICATIONS | 8013 | 8-36 |
| PHYSICAL SECURITY SURVEYS | 8014 | 8-36 |
| PHYSICAL SECURITY PLAN | 8015 | 8-37 |
| READY FOR ISSUE (RFI) FACILITY | 8016 | 8-37 |
| RECRUIT TRAINING AND FORMAL SCHOOL ENVIRONMENTS | 8017 | 8-37 |

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|--|------------------|-------------|
| DISPOSITION AND DEMILITARIZATION | 8018 | 8-38 |
| ROTC/JROTC/GUN CLUB/RESERVE UNIT PROHIBITIONS | 8019 | 8-42 |
| CLASSIFIED AA&E | 8020 | 8-42 |
| MARINE CORPS COMMUNITY SERVICES (MCCS) RESALE AND EXCHANGE FACILITIES | 8021 | 8-43 |
| MARINE CORPS MUSEUMS AND UNIT DISPLAYS | 8022 | 8-48 |
| ORGANIC/UNIT AND STATION MOVEMENTS OF AA&E | 8023 | 8-49 |
| SECURITY STANDARDS FOR SECURE HOLDING AREAS FOR AA&E | 8024 | 8-55 |
| SPECIAL CONSIDERATIONS FOR SMALL QUANTITY SHIPMENTS | 8025 | 8-57 |
| REPORTING OF MISSING, LOST, STOLEN, AND RECOVERED AA&E | 8026 | 8-57 |
| SIMULATED WEAPONS SYSTEMS | 8027 | 8-57 |
| STORAGE OF EVIDENTIARY AA&E | 8028 | 8-58 |
| STORAGE AND SECURITY OF PERSONAL WEAPONS AND AMMUNITION | 8029 | 8-58 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 8

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

8000. GENERAL. This chapter prescribes standards that provide appropriate protection against loss or theft of AA&E at Marine Corps activities. It does not authorize methods, actions, or operations inconsistent with the explosive safety standards of references (ac) through (ae). AA&E Security Risk Categories are listed in Appendix H.

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, and exercises. For sites not specifically covered in this instruction and expeditionary environments, commands will establish procedures to protect AA&E consistent with the intent of this chapter.

2. 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 (af) and (ag).

a. This chapter covers:

(1) Arms: In addition to those arms listed in Appendix H, U.S. prototype arms, and comparable foreign arms are included.

(2) Ammunition: In addition to Appendix H, see stock list of Navy ammunition 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 Order does not discuss security requirements for:

(1) nuclear weapons;

(2) devices charged with chemical agents (unless specified in Appendix H);

5 Jun 09

(3) Procurement of commercially available AA&E while at a commercial production facility. However, once the items are placed in transit to a DOD activity, all pertinent requirements of this chapter and reference (ah) apply.

3. Commanders and individuals issued, or in possession of, AA&E are responsible for its security.

4. Installation physical security plans will address 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 the following: 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 control, access control, structurally secure storage buildings, personnel and vehicular access control, administrative inspections at entry/exit points, security training programs, ESS, and 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 immediately and capable of responding before AA&E can be compromised.

5. Non-compliance with standards of this Order requires immediate command attention and corrective action. In the event that corrective action requires funding not available to the command, compensatory measures must be emplaced and the affected organization is required to submit an exception or waiver as outlined in paragraph 1008. Exceptions or waivers do not relieve the command's responsibility to seek funding to correct the deficiency.

6. Marine activities will ensure that physical security requirements for Marine Corps AA&E stored at non-Marine facilities, whether by another branch of Service, foreign

nation, North Atlantic Treaty Organization (NATO), or other personnel, are delineated in MOUs/MOAs and all efforts will be made to maintain AA&E to a level equivalent to that required herein.

7. Security Division (PS) maintains cognizance over AA&E security policy, while CMC(LPC) is responsible for Ammunition and Explosives (A&E) transportation policy. Marine Corps Systems Command (MARCORSYSCOM) Program Manager Ammunition (PM AMMO) is the life cycle manager for Class V(W) (ammunition) and explosives. Aviation ordnance policy falls under the purview of CMC(ASL).

8. 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.

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

10. 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, inventory control, and to reduce theft vulnerability. AA&E will be protected according to the highest risk category stored within the facility.

11. Consolidated armories will be constructed with solid walls separating individual unit storage areas. This requirement ensures unit integrity is maintained.

12. Remove AA&E from secure storage areas for as short a time as necessary and only in required quantities.

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

14. 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 for military and civil/criminal action for civilian personnel.

5 Jun 09

15. Clearing Barrels. Clearing barrels provide personnel a safe and effective means to properly clear, load, and unload their assigned weapon(s). Commanders will ensure:

a. Clearing barrels are placed at or near AA&E facilities, guard facilities, RFI points, and ranges.

b. Clearing barrels will be positioned away from high traffic and populated areas to ensure safety of bystanders in the event of a negligent discharge.

c. Weapons clearing procedures for all weapons approved to be cleared at the designated point will be displayed prominently near the clearing barrel.

d. A designated noncommissioned officer, staff-noncommissioned officer, or commissioned officer will supervise all weapons clearing.

e. Further guidance concerning clearing barrel design is provided in reference (ae).

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 OCONUS will receive priority over CONUS sites.

2. Deviations from these priorities will be permitted only when Security Division (PS) has determined that an identified local threat dictates the deviations and compensatory measures have been addressed.

8002. PERSONNEL. Activities must be selective in assigning personnel to duties involving control of AA&E. Only personnel who are U.S. citizens, 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, distribution, or security responsibilities for AA&E, will be

5 Jun 09

subject to one of the following investigations as set forth in references (b) and (ai).

(1) Military Personnel: National Agency Check, with Local Agency Check, and Credit Check (NACLCL). (NOTE: Commanding officers may grant interim assignment to non-U.S. citizens, upon favorable completion of investigations identified in paragraph 1a(1) below, and proof of application for U.S. citizenship).

(2) DOD Civilian Personnel: National Agency Check with Written Inquires (NACI) and Credit.

(3) Contractor Personnel: NACLCL.

(4) Foreign Nationals: Foreign national personnel providing services as described in paragraph 1a above, in overseas locations, will receive an investigation according to the policy and procedures governing locally hired employees under SOFA, export licenses or laws of the host government. The DOD components assume responsibility for permitting access to DOD systems, information, material, and areas when an investigation conducted by the host country does not meet the investigative standards outlined in references (b) and (ai).

b. Marines assigned custody, maintenance, disposal, distribution, or security responsibilities for AA&E can continue to perform assigned duties while awaiting adjudication of the investigation outlined in paragraph 8002.1.a.(1) above, at the Commanding Officer's discretion only if all other screening requirements have been completed.

(1) Monthly inquires will be made as to the status of the pending adjudication, and status will be documented in the individuals screening package.

(2) Individuals whose investigation results reflect negative or unfavorable findings, per reference (ai), will no longer be allowed to performed duties involving the custody, maintenance, disposal, distribution, or security of AA&E.

(3) For Marines whose investigation reflects negative or unfavorable findings, and who possess the requisite MOS, the commanding officer must notify Marine Monitor Officer Assignments (MMOA) or Marine Monitor Enlisted Assignments (MMEA) to request reassignment.

5 Jun 09

c. Civilians who perform duties involving the custody, maintenance, disposal, distribution, or security of AA&E will have an adjudicated investigation, as outlined in paragraph 8002 1.a.(2) or 1.a.(3) above, prior to assumption of duties. Civilians whose investigation results reflect negative or unfavorable findings, per reference (ai), will not be allowed to performed duties involving the custody, maintenance, disposal, distribution, or security of AA&E.

d. In addition to the investigation requirements of paragraph a above, all personnel involved in the custody, maintenance, disposal, distribution, or security of 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, as outlined in reference (aj) is a further requirement of the A&E Program, but does not replace the annual AA&E screening requirement, as outlined in this Order and reference (ae).

(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 individual to ensure compliance with screening requirements. All personnel responsible for conducting the screening will examine the service records of the individual being screened and discuss the duties and responsibilities of the billet with the person. Persons assigned as a screening officer will be assigned in writing, and will be a commissioned officer, warrant officer, staff non-commissioned officer, or civilian equivalent. GS-9 or above.

(2) Screening will be conducted on an annual basis and an entry will be made in the Unit Diary to ensure that the screening is reflected in the Marine's Basic Training Record (BTR). The screening package will be retained in the individual's training record or Qualification/Certification record. Civilian personnel requiring screening must maintain a copy of the screening package in their personnel file and local training file maintained within the AA&E area.

(a) Maintain for at least 1 year after termination of the person's assignment (or 1 year after the final interview if the person is disqualified).

(b) Re-screen personnel when circumstances indicate a review would be prudent.

5 Jun 09

(3) At each screening read the following statement to the person being screened and have him/her sign a copy of the 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."

(4) Determination of disqualifying traits and actions is at the discretion of the commanding officer. Additional guidance can be obtained from Security Division (PS).

e. All screening will be conducted in accordance with this paragraph and those documents contained in Appendix I. All screening documentation will be marked FOR OFFICIAL USE ONLY when filled in and/or completed with personal information.

f. 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 (ak), and carrier-issued identification.

2. AA&E Officer. Commanding officers will designate in writing, an individual, military or civilian, as the AA&E Officer. The AA&E Officer designation letter will be maintained for 3 years from termination of assignment. AA&E Officer duties are further outlined in reference (al).

3. Training. Activities possessing AA&E will establish and conduct an annual AA&E training program for personnel with AA&E-related duties (including personnel responsible for custody, maintenance, disposal, distribution, and security of AA&E items). Training will be conducted to ensure that all personnel remain vigilant of their responsibilities for controlling and safeguarding AA&E. The program will include inventory and accountability procedures, 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, and instruction on use of deadly force, per references (s) through (u), as applicable. All training will be documented and maintained in the individual's training record or through the qualification certification program as outlined in reference (aj).

4. Arming of Security Personnel. Personnel whose duties require that they carry a weapon will participate in weapons qualification training in accordance with reference (v) and deadly force training as directed in references (s) through (u). Deadly force refresher training will be conducted at least annually and documented in the individual's training record.

a. Armory personnel will be armed upon the deactivation of the MCESS/IDS.

b. Deactivation of the MCESS for an ammunition storage area requires an armed guard response capability (may be area guard duty personnel).

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 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 maintained within (e.g. If a Category I and Category II storage area simultaneously alarm, response priority will be given to the Category I storage area).

b. During normal working hours, entry and exit points into an Ammunition Supply Point (ASP) or holding areas will be controlled by a guard, whose primary responsibility is access control. After normal working hours if ESS is not provided, surveillance and physical check requirements identified in paragraph 8011 will be adhered to. CCTV is not a substitute for guards or constant surveillance unless it is used as part of an intrusion detection system (i.e. video motion detection, intelligent video, video tracking, etc.) with event driven technology.

c. An armed security patrol will periodically check facilities and areas storing AA&E, as prescribed in paragraph 8011. Checks will be increased based on FPCONS or vulnerability. Increased patrols and checks at night, on weekends and holidays will be conducted 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.

e. Security force and interior guard orders and Standard Operating Procedures (SOP) must address the requirement for posting of unit interior guard personnel at AA&E facilities if the ESS is inoperable.

8003. ACCOUNTABILITY AND INVENTORY. Commanding Officers will establish procedures to appoint/relieve an A&E audit and verification officer/Staff Noncommissioned Officer (SNCO) in accordance with references (al and am). Appointment letters will outline primary duties, responsibilities, and turnover procedures. All appointment, acceptance, and revocation letters will be retained for 3 years from date of assignment/termination.

1. All activities will maintain complete records identifying accountability, shipment, receipt, storage, inventory, issue, expenditures, and demilitarization in accordance with references (b), (c), (ac) through (ah), and (al) through (ar). Further guidance on the demilitarization of AA&E can be found in paragraph 8018.

2. Losses of AA&E shall not be attributed to an accountability or inventory discrepancy unless determined through causative research that the loss was not the result of theft. All causative research packages including MLSR reports and investigation findings, will be retained in accordance with references (al and am).

3. Ammunition and Explosives.

a. Inventories. Class V(W) A&E accountability and inventories will be conducted in accordance with reference (al) for unit inventories and reference (am) for intermediate-level (ASP) inventories.

b. Inspections. A review of the inventory portion of the Explosive Safety Self Audits (ESSA) and Explosive Safety Inspection (ESI) will be conducted during the Physical Security Survey. All Corrective Action Plans (CAPs) will reviewed to ensure corrective action has been implemented.

4. Arms.

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 data (forwarded monthly from component registries) containing the most recent UII list of arms. The DoN registry is maintained by Crane Division, NSWC, Code JXNP.

(b) Marine Corps Logistics Command (MARCORLOGCOM) (PEI Management Branch, Supply Chain Management Center) serves as the Program Manager for the Marine Corps Serialized Control of Small Arms Systems per reference (ap). MARCORLOGCOM contracts Crane Division, NSWC, Code JXNP, to maintain the small arms 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 Crane Division, NSWC, Code JXNP, which ensures that:

1. Such losses, thefts, or recoveries are, or have been, reported and investigated as outlined in Chapter 10.

2. Marine Corps arms recovered by police or investigative agencies are 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 and CMC, Historical Division (HD).

(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 (a).

(b) National or DoN-assigned UIIs will be used by Crane Division, NSWC, Code JXNP, 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 a National Stock Number (NSN) or UII missing, illegible or obliterated, will be reported by message or letter in the following format to the DOD Central Registry by Crane Division, NSWC, Code JXNP, for assignment of an NSN and management control UII:

1. NSN (NSN or "None")
2. UII (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) Crane Division, NSWC, Code JXNP, 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.

(h) Refer questions concerning daily operations to the Navy Registry, Navy Small Arms Management:

Commander
Naval Surface Warfare Center (NSWC)
Crane Division
Code JXNP
Building 3422
300 Highway 361
Crane, IN 47522-5001

5 Jun 09

b. Physical Inventories of Arms. In addition to physical inventories required by paragraph 8005.4, 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 the commanding officer determines there is any evidence of tampering.

(4) A unit level monthly inventory of all arms by UII conducted by a disinterested third party not in the inventory chain of command and not having access to the items being inventoried. The inventory will be conducted using an extract of the most currently signed and validated Consolidated Memorandum Receipt (CMR). The disinterested third party must be a commissioned officer, warrant officer, SNCO, or civilian equivalent, GS-9 or above. Persons conducting the inventory will be assigned in writing by the commanding officer. Inventory results will be provided to the commanding officer and will include the following:

(a) Verified seal numbers for all Level A packed arms.

(b) Documentation for all arms not on hand (e.g., receipt copy of Equipment Repair Order (ERO) or NAVMC 10520).

(c) Inventory officer appointment letter, including any instructions or guidance.

(d) Current signed and validated CMR extract utilized for inventory.

(e) A memorandum from the supply officer outlining action to be taken to correct identified discrepancies, and a final report once all discrepancies are corrected.

(5) All arms not Level A packed, boxed, banded, and secured with a tamper proof seal will be physically "sight"

5 Jun 09

counted and recorded on a daily sight count (inventory) form upon initial opening and final closing of any armory.

(6) Records of all sight counts and inventories (including the signed CMR, inventory assignment letter, letter of discrepancy from inventorying officer, supply officer endorsement, commanding officers endorsement, and copies of supporting documentation) will be retained for a period of three year. Crane reports will be maintained for 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 references (al) through (ap). Additionally, activities will establish procedures for AA&E Officers to ensure the adequacy of requisition verification of Category II-IV arms. Procedures will include positive steps for rejecting excess and unauthorized requisitions.

(2) Inventories. Physical inventories will be conducted as indicated below:

(a) Unit Level: 100 percent monthly count. 100 percent quarterly inventory by UII.

(b) Installation: 100 percent semiannual inventory by UII.

(c) Logistic Base (Depot Level): 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 NAVMC forms 10520 and 10576 listing serial number and type of item(s) received.

(1) Persons issued or in possession of arms are responsible for its security and may be required to provide armed security in accordance with this Order. The individual may check out a security weapon and related ammunition as required and authorized.

(2) Individuals being issued small arms will be weapons qualified, in accordance with reference (v), and trained in the use of force in accordance with references (s) through (u) as required.

(3) The quantity of arms removed from secure storage areas will be kept to a minimum as operational needs dictate. In order to maintain adequate security, arms will be returned to storage upon mission completion.

8004. AA&E STORAGE FACILITIES (SPECIAL REQUIREMENTS). AA&E will be stored in facilities as prescribed in paragraphs 8005 and 8006. This paragraph addresses requirements for facilities that do not meet standards of 8005 and 8006.

1. Existing Facilities Located On Military Installations. Existing facilities may continue to be used as long as they provide 10 minutes of forced entry delay and meet the requirements contained within this Order 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 (q) provides both design and retrofit guidelines and requirements. Substandard facilities must have an approved exception/waiver.

2. Facilities Located Off Military Installations. Facilities may continue to be used but they must provide 10 minutes of forced entry delay; reference (q) 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 GSA approved 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, 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.

c. Organizations will ensure that an approved secondary wireless means of communications is maintained for both communication and monitoring purposes.

5 Jun 09

3. Arms Storage Facilities in an Expeditionary/Field Environment. When operationally feasible, and as directed by the commanding officer, arms will be stored in a prepared shelter (e.g. quadcons, ISO Containers, Amphibious Assault Vehicles (AAVs), tents, pre-existing buildings, etc.), as such, it will provide security personnel with the reasonable means to secure and protect the 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.

a. A barrier will be maintained for the shelter perimeter (may be triple strands of concertina wire). Maintain clear zones of 30 feet on the interior and 20 feet on the exterior of the wire. Access through the wire limited to one ingress/egress point. Access to the storage facility will be limited to the minimum number of personnel necessary for operations. Area designation and access control will be established in accordance with paragraph 8008.

b. Weapons will be secured in storage racks. When racks are unavailable, secure weapons in available containers in an effort to provide security commensurate with this Order. In the absence of racks or containers, connect weapons together by running a steel cable through the receivers and secure the ends of the cables with a low security padlock to prevent weapons removal.

c. Major weapons parts (i.e. barrels, receivers, and major subassemblies, 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. Unit physical security plans will address the protection of AA&E to include maintaining two separate and distinct forms of communication. 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. When a field armory is established a serialized

5 Jun 09

inventory must be conducted. Each time the facility is opened, closed, or if there is a change of responsible personnel, a sight count will be conducted. When the armory is disbanded a serialized inventory must be conducted. Commanders will establish a tracking system (e.g. logbook, spreadsheet, temporary 10520) to ensure accountability of weapons.

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 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 8011.

5. Personal Protection/Duty Weapons/Ammunition. Weapons and ammunition issued to general/flag officers for personal protection, *as directed*, and to accredited criminal investigators, *if compliance impedes mission performance*, are exempt from requirements of this Order, except for inventory and loss reporting. During non-duty hours, weapons and ammunition will be stored in commercial weapons containers/safes within the affected residence. All weapons will be fitted with a trigger lock. Commercial weapons containers will be constructed of metal and provided with a three-digit combination. The container will be stored in a closed space that restricts access to the container by unauthorized persons.

6. Competition Rifle/Pistol Team Weapons and Ammunition. Weapons and small arms ammunition issued to members of Marine Corps Shooting Teams will be maintained in accordance with this Order. During matches held off-installation, weapons and ammunition will be provided security commensurate with requirements outlined in this Order. Accountability, storage, and inventory requirements during matches will be addressed in battalion/team orders. The Commanding Officer, Weapons Training Battalion (WTBN) Marine Corps Base, Quantico, VA, in conjunction with the Officer in Charge (OIC) of the Reserve Shooting Team will ensure that all requirements of Chapter 10 of reference (as) have been addressed with Reserve Shooting Team personnel. Additionally, the CO, WTBN and the OIC of the Reserve Shooting Team will ensure that all Reserve Marines assigned to the team are screened in accordance with paragraph 8002. Use of POV for transportation of weapons and small arms ammunition may be

5 Jun 09

authorized by the installation commanding officer in writing. When a POV is used, the arms and ammunition must be securely stowed and protected from view. Weapons and ammunition will be stored in commercial weapons containers/safes. Commercial weapons containers will be constructed of metal and provided with a three-digit combination. The container will be maintained in a space that restricts access to the container by unauthorized persons. The arms and ammunition must be under constant surveillance during stops en-route to destination.

7. Security of Small Amounts of Arms. On military installations, small numbers of arms (less than 15) 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 (Fed Spec AA-F-363 (latest series)). The container must be under constant surveillance or protected by an IDS. The facility will be checked by a security patrol at least once every 24 hours. Containers weighing less than 500 pounds will be secured to the structure.

8. Security seals will be attached to both doors on all AA&E shipments moving in MILVANS and ISO Shipping Containers designed with a door retention plate. Both seal numbers will be recorded on the Bill of Lading.

9. MARCORSYSCOM (PG-132) is the only authorized small arms RDT&E facility within the Marine Corps. Weapons and ammunition maintained used within this facility will be maintained in accordance with this Order. During travel for events within the areas of Research and Development, field operations, fielding of new weapons systems, weapons exchanges, or demonstrations (on and off military installations), weapons and ammunition will be stored in commercial weapons containers/safes. Commercial weapons containers will be constructed of metal and provided with a three-digit combination. The container will be maintained in a space that restricts access to the container by unauthorized persons. The arms and ammunition must be under constant surveillance during stops en-route to destination. MARCORSYSCOM (PG-132) will ensure that all personnel assigned to the program are screened in accordance with paragraph 8002, and trained in the use of force requirements of references (s) through (u) and weapons qualifications of reference (v).

8005. SECURITY OF ARMS. This paragraph prescribes security standards and requirements for the storage and protection of conventional Category II through IV arms. Construction

requirements for Category I through IV AA&E facilities are summarized in Table 1 of Appendix J. Construction requirements for Category I through IV Arms and non-earth covered magazines are identified in Table 2 of Appendix J.

1. Arms Storage Facilities. Arms will be stored in fixed structures built as prescribed in references (b) and (q) and in accordance with specifications of reference (ac).

a. Walls. Walls will be constructed in one of the following methods as indicated below:

(1) 8-inch (200 mm) concrete reinforced with No. 4 (12.7 mm) reinforcing bars, 9 inches (225 mm) on center, in each direction and staggered on each face to form a grid approximately 4-1/2 inches (114 mm) square.

(2) 8-inch (200 mm) concrete block (or concrete masonry unit) with No. 4 (12.7 mm) bars threaded through block cavities filled with mortar or concrete and with horizontal joint reinforcement at every course.

(3) 8-inch (200 mm) of brick interlocked between inner and outer courses.

b. Floors. Floors will be constructed of 6-inch (150 mm) concrete construction reinforced with 6-inch by 6-inch (150 mm by 150 mm) W4 by W4 mesh or equivalent bars. Any arms storage area constructed on a second deck, or having a floor that serves as a roof/ceiling for a space beneath, will be constructed of 8-inch (200 mm) concrete reinforced with two grids of Number 4 (12.7 mm) rebar on 9-inch (225 mm) centers.

NOTE: All reinforcing bar spacing will form a grid using No. 4 (12.7 mm) bars or larger so that the area of any opening does not exceed 96 square inches (0.6 square meters).

c. Roof/Ceilings. Roofs and ceilings will be constructed in one of the following methods as indicated below:

(1) 8-inch (200 mm) concrete reinforced with Number 4 (12.7 mm) reinforcing bars, 9-inches (225 mm) on center.

(2) If the roof or ceiling is of concrete pan-joint construction, the thinnest may not be less than 6-inches (150

mm) and the clear space between joists may not exceed 20 inches (500 mm).

NOTE: All reinforcing bar spacing will form a grid using No. 4 (12.7 mm) bars or larger so that the area of any opening does not exceed 96 square inches (0.6 square meters).

d. Exterior Doors

(1) Class 5 Vault Doors. For all new armory construction, exterior doors will be a GSA Class 5 vault door or equivalent meeting Fed Spec AA-D-00600D. Class 5 vault doors provide a forced-entry penetration delay time of 10 minutes.

(2) Class 8 Vault Doors. For all new armory construction, a Class 8 vault door meeting Fed Spec AA-D-2757 may be used. However, in a designated high-severity threat level area, a GSA Class 8 vault door will be used. Class 8 vault doors provide a forced-entry penetration delay time of 15 minutes.

(3) Pre-existing Exterior Armory Doors. The following two paragraphs provide requirements for approved pre-existing armory perimeter doors (new construction requirements are noted above). These doors will be constructed in one of the following methods as indicated in paragraphs (a) and (b) below:

(a) Constructed of 1 3/4-inch (44 mm) thick solid or laminated wood, with a 12-gauge (2.7 mm) steel plate on the exterior face.

(b) Standard 1 3/4-inch thick (44 mm), hollow metal, industrial-type construction with minimum 14-gauge (1.9 mm) skin plate thickness, internally reinforced vertically with continuous steel stiffeners spaced 6-inches (150 mm) maximum on center.

NOTE: Facilities designated for upgrades including structural modifications will ensure that a Class 5 or Class 8 vault door is incorporated in the project for the exterior door.

(4) Day gates. Day gates are typically used to separate restricted arms storage areas from common spaces during normal operating hours. Figure 8-1 provides an example of a typical armory day gate. Day gates are generally constructed on the interior of the main entry point to an armory; however day gates

may be used to separately secure individual unit storage areas within an armory. Construction of the gate will be, at a minimum:

(a) 9-gauge diamond metal mesh, with a continuous weld through each point, welded to a 1/4-inch angle iron frame. Frame joints will be welded with a continuous weld. Hinges will be located on the interior and welded to the supporting wall and angle iron.

(b) Secured with a spring-bolt lock equipped with an exterior key point and interior thumb throw latch release. The latch release will be located at a point accessible only from the inside. Day gates should be self-closing.

(c) Day gates may also be secured with a chain and padlock. Chains will be heavy-duty hardened steel or welded, straight link, galvanized steel, of at least 5/16-inch thickness, or equivalent.

(d) Issue points, windows, and other openings are discussed in paragraph (f) below.

(5) Support Hardware. 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 the door frame. Frames and locks for doors will be designed and installed to prevent removal of the frame facing or built-in locking mechanism to allow disengagement of the lock bolt from outside.

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

(b) 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, security hinge type or equivalent.

(c) 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. Paragraph 5014 provides an example of hinge protection. Such devices must be of sufficient positive engagement and resistance to shearing force to prevent opening the door from the hinge side.



Figure 8-1.--Armory Day Gate

e. Vehicle or Large Bay Doors. Vehicle or large bay doors will be constructed as prescribed in reference (q). Medium-threat severity level doors will be, at a minimum, 4-inch (100 mm) thick sliding doors, 14-gauge (1.9 mm) hollow metal, or solid or laminated wood with a 3/8-inch (9 mm) gauge steel plate on the outside. There are no low-threat severity level doors.

f. Windows and Miscellaneous Openings. Windows, ducts, vents, or any AA&E opening of 96 square inches (0.06 square meters) or more with the least dimension greater than 6-inches (150 mm) will be protected by:

(1) Minimum 3/8 inch (9.5 mm) hardened steel rods with maximum 4-inch (100 mm) spacing with horizontal bars so that openings do not exceed 32 square inches (0.02 square meters); or

(2) Riveted steel grating (weight of 13.2 pounds per square foot (64.5 kilograms per square meter) or welded steel grating (weight of 8.1 pounds per square foot (39.6 kilograms per square meter) with 1 by 3/16 inch (25.4 mm by 4.7 mm) bearing bars. Weapon issue points (including those in doors, day-gates, etc.) will not exceed 190 square inches when opened and when not in use, will be secured. Additional guidance can be obtained in reference (q).

g. Locks and Hasps. GSA approved vault doors will be secured with a built-in three-position dial combination lock meeting Group 1, Underwriter Laboratory Standard 768. Other doors will be secured with a high security hasp meeting Military Detail (MIL-DTL) 29181C, 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/lock installation are required in order to store arms.

(d) Further information concerning procurement of the portable explosive magazine is available by contacting the Commanding Officer, Crane Division, Naval Surface Warfare Center (NSWC) Code GXQS, Building 3395, 300 Highway 361, Crane, IN, 47522-5001.

i. Arms Racks, Storage Containers, and Safes. Arms will be stored in original containers, banded, and sealed to reflect the integrity of the contents. Containers will be fastened together in groups totaling at least 500 pounds total weight.

(1) Arms in an armory will be stored in banded crates, standard or locally fabricated metal arms racks or Class 5 GSA approved weapon containers/safes. Locally made arms racks must be constructed to prevent removal of a weapon by disassembly and provide the same degree of protection as a standard manufactured weapons rack or container.

(2) Arms racks will be locked with low security padlocks meeting Military Specification (MIL SPEC) Mil-P-17802 or Commercial Item Description (CID) A-A-1927.

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

(4) 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. All racks or containers will be secured with chains equipped with low security padlocks or bolted together to prevent removal. Racks secured solely with bolts must be spot welded, peened, or otherwise secured to prevent removal. Racks secured with chains may be bolted together for stability and do not require bolt heads to be spot-welded or peened. Chains will be heavy-duty hardened steel or welded, straight link, galvanized steel, of at least 5/16-inch thickness, or equivalent. Weapons containers, (when locked) that secure and encase weapons and prevent access to nuts/bolts that fasten one container to another, do not require the nuts/bolts to be spot-welded or peened. However, these nuts and bolts must be adequately tightened to prevent movement.

(5) Ready for issue point storage requirements are addressed in Paragraph 8016.

2. Arms Parts. Major arms parts such as barrels and major subassemblies will be protected to the same degree as Category IV arms (secured in racks or containers to prevent easy removal). The frame or receiver of an arm constitutes a weapon and these parts must be safeguarded according to the appropriate category (for example, the receiver of a .30 caliber machine gun must be safeguarded as a Category II arm).

3. Multiple Unit Arms Storage Facilities. Two or more units may share the same storage facility; however, arms will be identified and separated by unit. Unit inventories will not be stored in the same container.

a. Each unit arms storage area will be physically separated from the other unit storage areas within the facility.

b. Each unit storage facility will be provided an Intrusion Detection System and separately zoned.

5 Jun 09

c. Walls will be constructed of 1/4-inch wire mesh or galvanized chain-link fencing material covered by material (e.g. plywood, drywall, etc.) that prevents;

(1) Passing or removal of arms from one unit storage area to another; and

(2) ESS sensor devices from penetrating adjacent unit storage areas;

d. Walls may also be of permanent construction materials (plaster, metal panels, hardboard, wood, plywood, or other materials) offering resistance to, and evidence of unauthorized entry into the area.

e. Doors will be installed on each unit storage area.

f. One unit will be responsible for security of the entire storage facility. This unit will be designated in writing and a copy of the designation letter will be provided to all units within the facility.

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 Explosive Storage Facilities.

a. Intermediate Level (Ammunition Supply Points)

(1) A&E will be stored in fixed structures as prescribed in references (b), (q), and (ac) through (ae). Magazines will be sited and constructed to the requirements, outlined herein, in accordance with specifications of reference (ae).

(2) The installation Explosive Safety Officer (ESO) will be consulted prior to construction or procurement of facilities used to store A&E, to include Portable Explosive Magazines.

(3) Locks. All exterior doors will be equipped with an ILD. High security locks/hasps, Universal Security System (USS), and Anti-Intrusion Barriers (AIB) may continue to be used until replaced.

b. Unit Level (Security Ammunition) Quantities. Limited quantities of A&E may be stored in accordance with reference (ae).

(1) Approved Storage Facilities. Arms rooms constructed in accordance with reference (q), armories, portable explosive magazines, 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, 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 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.

(4) Aircraft A&E. Category IV Cartridge Actuated Devices (CADs) and Pen Flares will be stored in original containers banded and sealed to reflect the integrity of the contents. The original containers will be maintained in approved explosive security container or magazines until operational necessity requires deployment.

(a) CADs will be secured in one of the following methods listed below:

1. Ready Service Locker (RSL). Key control, access, inventory requirements, and security checks as noted in Appendix K.

2. In operational aircraft within a Level II restricted area. Security checks are required as noted in Appendix K.

3. For temporary storage in a Seat Shop or re-work shop, the following security requirements will be met:

a. The storage space or room will be constructed of at least 3/4-inch metal, 4-inch poured concrete or reinforced concrete masonry unit, or similar, hardened, solid construction materials.

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

c. Windows will be kept to a minimum and all windows will require 1-3/4-inch metal or rebar secured to prevent removal, with no opening greater than 96 square inches.

d. The container or room will be secured with a mortise lock and deadbolt, at a minimum.

e. Access control and key control to the space must be established.

(b) Pen flares will be secured in one of the following methods listed below:

1. Ready Service Locker. Key control, access, inventory requirements, and security checks as noted in Appendix K.

2. In the custody of the individual the pen flare is issued.

3. In a flight equipment room, the following security requirement will be met:

a. In a metal container allowing for separation between each flare and vest.

b. In an approved explosive safety container.

c. Access control to the space must be established.

8007. FENCES. All Category I through III A&E storage facilities 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. Personnel and vehicular access control will be established for areas storing AA&E. Unaccompanied access to ammunition and explosive storage facilities will be limited to the minimum number of required personnel assigned to the facility to maintain safe, essential operation. These persons are required to be screened in accordance to paragraph 8002.1 prior to access being granted. Additionally, these personnel must be designated in writing by the Commanding Officer and kept current. 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 provide guidance concerning visitor access in AA&E storage spaces. All visitors must be escorted by authorized personnel and their ingress and egress logged. Visitor control logs will be maintained for 3 years.

b. Vehicles and personnel are subject to random searches and inspections upon entry and exit from AA&E areas.

c. Privately-owned vehicles are prohibited from entering AA&E storage areas.

d. Physical security personnel when acting within the scope of their duties will be granted access to restricted areas and must be escorted by authorized personnel.

e. 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.

f. Personnel having access to AA&E accountability records will not be granted key control access nor will they be allowed unescorted entry to an AA&E facility.

8009. ELECTRONIC SECURITY SYSTEMS. All AA&E storage facilities located aboard Marine Corps installations will be protected by the MCESS. Approval of all ESS protecting Marine Corps AA&E will be approved by Security Division (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 provided surveillance as directed in Appendix K.
2. MCESS/ESS will include point sensors on all doors, other human-passable openings, duress buttons, and interior motion (volumetric) or vibration sensors.
3. Intrinsically safe equipment will be utilized for all A&E facilities.
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. Coordination, by physical security personnel, will be made with the unit commanding officer prior to conducting periodic unannounced openings; however, timing and inconvenience will not prevent testing requirements from being met. At a minimum, one drill will be performed semiannually. The date, time, and results of security force drills, including deficiencies and corrective action taken will be recorded 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 and facility personnel.
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 one unit within the same

storage facility cannot activate/deactivate another unit's storage area ESS.

6. AA&E Facilities are constructed to withstand at least 10 minutes of forced entry delay. In an attempt to enhance security measures at AA&E facilities, commands may install a fence protection system and a CCTV assessment or event driven video motion detection with CCTV capability on the facility perimeter, or fence that will provide an assessment capability to the responding security force.

7. AA&E storage facilities located outside Marine Corps installations, under Marine Corps control, will be equipped with a commercial ESS 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. Approved secondary communications requirements, testing and maintenance must be addressed.

8010. KEY SECURITY AND LOCK CONTROL. All persons authorized access to AA&E keys will be designated in writing by the commanding officer, and a current roster will be maintained and kept from public view. In addition to the Key Security and Lock Control requirements of chapter 3, the following paragraphs of this section also apply:

1. Access control custodians will not be assigned unaccompanied access to the facility, nor will they be assigned a PIN. Access control custodians for AA&E facilities will be responsible for:

a. Preparing MCESS PIN requests for signature and submission to the provost marshal's office physical security section.

b. Maintaining and securing all spare keys for the facility, including active, spares, and replacement core keys.

c. Semi-annual key inventories.

d. Ensuring all safe combinations are changed annually or upon personnel rotation and appropriate records of the changes are maintained. Commanders will ensure that SF 700s are maintained for all containers.

2. Keys to AA&E facilities will be maintained separately from all other racks, containers, and miscellaneous keys. They will

be accessible only to individuals whose official duties require access to them and who have been authorized in writing by the commanding officer.

3. Keys to AA&E facilities will be provided protection commensurate with the material that the keys allow access. Keys will be provided security during their transport to and from non-working hour storage containers. Security will be accomplished as follows, per the commanding officer's direction as dictated in the company/battalion/base order.

a. Transportation

(1) Keys will be transported to and from storage non-working hours storage areas/containers by armed personnel equipped with a communications device from which a response force may be summoned.

(2) Keys will be transported to and from non-working hours storage storage areas/containers using the two-man rule (as defined in Appendix A) equipped with a communications device from which a response force may be summoned.

b. Storage

(1) When not attended or in use, operational keys to Category I and II 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.

(2) Keys to Category III and IV AA&E will be stored in containers of at least 12-gauge steel or equivalent. The container will be secured with a GSA approved built-in three-digit changeable combination lock, built-in three-digit combination lock meeting UL Standard 768 or a GSA approved key operated security padlock.

5. Master keying of AA&E locks is prohibited. The use of keyed alike locks, to minimize the number of keys to racks and containers, is authorized; however, keyed alike lock levels will be maintained at a maximum ratio of 15:1 (e.g. 15 locks can be opened with one key).

6. AA&E Keys will not be taken off the installation or removed from a Marine Corps-controlled space. In the event that a compromise does occur, an inventory will be conducted and all locks/cylinders changed.

7. 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. These persons will sign for a container secured with a GSA approved changeable combination padlock (Fed Spec FF-P-110-G) and will not have direct access to AA&E keys.

a. A logbook will be maintained to identify issue and recovery of the container. Logbooks will be maintained for three years.

b. During non-working hours, staff duty officers or designated personnel will provide constant surveillance for security containers storing AA&E keys.

c. Spare keys, including maintenance keys for AA&E facilities will not be maintained in the AA&E facility and will be turned over to the access control custodian for proper safekeeping.

d. Intermediate level storage facilities (ASPs) will ensure that all spare keys, including maintenance keys will be maintained in a separate storage container. The container use will be limited to storage of the spare keys. Spare locks/cylinders may be stored in the container at the discretion of the commanding officer.

8011. SURVEILLANCE AND SECURITY CHECKS. Constant surveillance is the continuous visibility of an item(s) or area, or of all means of access to the item(s) or area. Constant surveillance is further defined in Appendix A. Surveillance and security check requirements for AA&E storage are identified in Appendix K.

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.

1. Security lighting, designed to provide complete perimeter coverage will be accomplished by using pole or building mounted fixtures.

2. Switches for exterior lighting will be installed in 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 in order to summon a security force. The ESS duress button is recognized as a form of communication. The additional form of communication will be either a two-way radio, phone, or cell-phone. The communication system will be tested on a monthly 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 A&E storage facilities will meet Hazards of Electro-magnetic Radiation to Ordnance (HERO) standards of reference (at).

8014. PHYSICAL SECURITY SURVEYS. Physical security surveys of AA&E facilities (including AA&E RDT&E facilities, Ammunition Supply Points, Production Buildings, and Ready Service Magazines and Lockers) will be conducted as prescribed in paragraph 3001.

1. A random sampling of AA&E screening records, daily sight counts, monthly serialized inventory results, and key and lock control records will be reviewed.

2. Review status of any corrective action taken on security deficiencies noted during previous surveys, assistance visits, or command inspections.

3. Ensuring exception and waivers for AA&E security have been requested where appropriate, copies of approved current exceptions and waivers are on file, and compensatory measures are being enforced.

4. All MLSR reports will be provided for review.

5. A review of the inventory portion of the Explosive Safety Self Audits (ESSA) and Explosive Safety Inspection (ESI) will be conducted during the Physical Security Survey. All Corrective Action Plans (CAPs) will reviewed to ensure corrective action has been implemented.

8015. PHYSICAL SECURITY PLAN. Unit and installation physical security plans will address the protection of AA&E.

8016. READY FOR ISSUE (RFI) FACILITY. Units may store arms and ammunition together in the same area for security force personnel only. Arms and ammunition may be secured in the same containers when not being issued or received, as operationally necessary. Contingency weapons and ammunition in a RFI will be maintained in separate containers. A&E (security ammunition) maintained in RFI rooms will be stored in a container weighing 500 pounds or greater. 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 Order 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 duties (Sergeant of the Guard (SOG), Corporal of the Guard (COG), Desk Sergeant, Dispatcher, etc.) must not interfere with constant surveillance;
3. RFIs are inventoried at each change of watch; and
4. The area is designated and posted as a restricted area and access control is established and restricted.
5. RFIs must have command approval per reference (ae).
6. All security force personnel are trained in the use of deadly force in accordance with references (s) through (u).
7. All security force personnel are qualified with their assigned weapons in accordance with reference (v).

8017. RECRUIT TRAINING AND FORMAL SCHOOL ENVIRONMENTS. Security of weapons presents a unique challenge to Commanders in recruit training and formal school environments. There are inherent risks commanders at recruit depots and formal schools assume when balancing the requirement for security against training schedules. This paragraph assists commanders in meeting their security requirements while taking into consideration the unique challenges faced in the training environment.

1. The security provisions for the storage of functional AA&E remains the same. ESS provisions are still applicable whether the storage area/facility houses functional or non-functional AA&E. Unit armorers are not required to be armed, once the ESS is deactivated, if the armory stores only non-functional/demilitarized (DEMIL) AA&E.

a. Dummy weapons are authorized for drill, training and display and do not require security. Dummy weapons are defined as rubber, wood, plastic, or metal, cast in the form of an actual weapon. These weapons lack functioning parts and operations of actual firearms and are incapable of discharging a projectile.

b. Weapons at recruit depots and formal schools must be capable of functionally performing inspection arms. If a DEMIL weapon is used for training purposes, a DEMIL certificate must be maintained for the weapon. The certificate must identify that the weapon has been demilitarized per reference (ar), or the authorizing authority for demilitarization for the Marine Corps.

2. A two-man rule applies to recruits providing constant surveillance of arms during stack arms and when secured in arms racks. Recruit training commands must establish policy and procedures, in writing, that clearly provide watch standers directions on protection of arms and how to summon a response force. A period of instruction will be provided to all watch standers prior to assumption of duties.

8018. DISPOSITION AND DEMILITARIZATION. Disposition of AA&E (e.g., Foreign Military Sales, transfer to law enforcement agencies, disposal, etc.) is governed by references (c) and (ar). DEMIL of AA&E must be accomplished under references (c) and (ar). AA&E must be transported and stored in accordance with this chapter until accountability is transferred or demilitarization is complete. The term DEMIL is the act of destroying the military offensive or defensive advantages inherent in certain types of equipment or material, and does not necessarily require total destruction of the equipment or material. Demilitarization is further defined in Appendix A.

1. As authorized by 10 U.S.C. 2572, 10 U.S.C. 7545, 10 U.S.C. 4683, or other similar statutes, specific condemned or obsolete combat material may be donated to specified authorized recipients for ceremonial use and training (e.g.; veterans'

organizations for color guards and rendering funeral honors, Reserve Officer Training Corps (ROTC), Junior Reserve Officer Training Corps (JROTC), etc.) or display purposes (accredited museums, veterans' organizations, municipalities, etc.). Arms used for ceremonial purposes must be sufficiently operational to fire blanks and those used for training must be capable of functioning for close order drill and inspection arms. Only limited or minimum DEMIL of such items will be accomplished to render the items unserviceable in the interest of public safety, but will preserve the intrinsic, historical or display value of the property. The authority for these donations is DC I&L (LPC-2) and History Division (HD) for accredited museum recipients and captured property per reference (au).

2. Class V(W) ammunition items, to include civilian ammunition found on a Marine Corps installation requires a request for disposition to be sent to the Marine Corps Designated Disposition Authority (DDA) MARCORSSYSCOM (PM AMMO) per reference (ae).

3. DEMIL Moratorium. The annual Defense Appropriation Acts continue the prohibition on the use of DOD funds to demilitarize or dispose of certain small arms. The Act states: "None of the funds available to the Department of Defense may be used to demilitarize or dispose of M-1 Carbines, M-1 Garand rifles, M-14 rifles, .22 caliber rifles, .30 caliber rifles, or M-1911 pistols". The moratorium imposed by the Office of the Secretary of Defense remains in effect unless otherwise notified. This moratorium includes receiver assemblies and non-repairable small arms. The moratorium does not apply to the components of the cited small arms when turned-in for disposal as components. However, the cited small arms shall not be disassembled prior to turn-in for disposal.

a. This moratorium does not apply when the cited small arms are transferred or donated to legally authorized recipients where specific statutory authority exists such as:

(1) State and local law enforcement activities and other federal agencies [10 U.S.C. 371-382, 2576 and 2576a]. The DOD Law Enforcement Support Office at DLA has authoritative cognizance.

(2) Service Educational Activities and veterans groups where DOD funds are not used to perform limited demilitarization [10 U.S.C. 2572, 4683, 7545 and 18 U.S.C. Section 922(d)(9)].

b. During the moratorium, the cited small arms must be stored and secured. In order to minimize associated costs, impacted organizations are encouraged to pursue storage arrangements within DOD that would be most advantageous to the Department of the Navy.

4. Demilitarization of Foreign/Captured Weapons

a. Possession is subject to the, National Firearms Act [Title 26, United States Code 5801-5872], Gun Control Act of 1968 [Title 18 U.S.C. Chapter 44, Sect 921] and Lautenberg Amendment to the Gun Control Act of 1968 [18 USC Section 922(d)(9)].

b. Unless the technical directive, maintenance instruction, or drawings are captured with the war trophies those documents are generally not readily available. The instructions and precautions cited in reference (ar), as guidance and handling or supervision by appropriately trained, qualified, and experienced personnel with the proper MOS are absolutely necessary.

c. A team approach involving appropriate MOS personnel including explosives ordnance disposal, hazardous material specialists, and safety specialists should be utilized to supervise, handle, or provide counsel during the DEMIL process. All potential hazards will be identified in writing with the location(s) physically marked on the piece to undergo DEMIL or illustrated to approximate scale. All precautions observed will be taken and weapons will be considered as loaded, armed, or otherwise dangerous. If the weapon is part of the historical inventory, authority for destructive DEMIL will be sought from HD with a copy to DC I&L (LPC-2).

d. If properly trained, qualified and experienced personnel are not readily available:

(1) wait until those personnel become available, or

(2) if additional DEMIL instructions are required for a particular weapon system, address the chain of command for that information and expertise, or

(3) request guidance from the Marine Corps Intelligence Activity (MCIA), Quantico, VA, with a copy to DC I&L (LPC-2).

e. The point of contact for requesting translated directives on post-World War II foreign weapons is the Marine Corps Intelligence Activity, Marine Corps Base Quantico, VA, (703) 784-6167 or DSN 278-6167 or the Technical Reference Library, National Ground Intelligence Center, Charlottesville, VA. Some of this information may be sensitive, and the Historical Division does not have any declassification authority or handle classified material. This method is recommended in order to prevent accidents or fatalities resulting from improperly conducted DEMIL operations.

5. DEMIL Certification. Certificates of destructive or limited/minimum DEMIL for arms must be signed by a technically qualified U.S. government representative before AA&E is displayed, used for authorized ceremonial/training purposes, or DEMIL residue released for disposal.

6. Limited or Minimum DEMIL. Small arms altered to make them incapable of firing may be used for drill purposes, with marksmanship training systems, or for display purposes in offices, museums, or other areas, only if accompanied by a properly completed legibly authorized and signed demilitarization certificate, located nearby and produced for examination upon request. Limited DEMIL includes, at a minimum, a 2-point deactivation of the small arm by placing a bead of weld in the chamber (not to allow a cartridge to be inserted) and welding the barrel to the receiver. Additional DEMIL may involve:

- a. bolt assembly welding
- b. grinding and welding drill rod into chamber and barrel,
- c. grinding and welding gas cylinder components, or
- d. welding and end milling of operating rod disassembly mechanism on the receiver.

7. Unit Displays

a. All museums, offices spaces, and other areas desiring to display demilitarized AA&E, must request permission from the installation commander.

b. Per reference (au), unit display AA&E shall be documented by either a conditional loan agreement with HD or an HD letter authorizing the command to maintain historic property.

c. The Small Arms Program Manager at HD must approve the limited/minimum DEMIL of arms for displays. Small arms allowance approval is required and must be reported under the Small Arms Serialization Program to the Navy and Marine Corps Registry, Crane Division, (NSWC) Code JXNP.

d. A log will be maintained of all displayed munitions that contains the nomenclature, item, owning organization, location, and certification label number. This information will be submitted to the installation Explosive Safety Officer (ESO) annually.

8. Security of DEMIL AA&E. Perpetrators have been known to obtain pieces and parts of destructive DEMIL residue from a variety of different locations to assemble seemingly serviceable AA&E. Perpetrators have also stolen weapons, subjected to limited/minimum DEMIL, and used them in the commission of crimes and other fraudulent activities. In the interest of homeland security and to preclude potential third party liability claims against the government, Commanders/commanding officers will provide security measures for demilitarized AA&E to prevent loss or theft.

8019. ROTC/JROTC/GUN CLUB/RESERVE UNIT PROHIBITIONS.

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.

8020. CLASSIFIED AA&E. Classified AA&E must be protected as directed by this chapter and reference (d).

1. Entry points to structures housing classified AA&E will be secured with a GSA approved Class 5 or Class 8 vault door as described in paragraph 8005.1.d.

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).

8021. MARINE CORPS COMMUNITY SERVICES (MCCS) RESALE AND EXCHANGE FACILITIES. The following security standards apply to all Marine Corps Community Services Resale and Exchange Facilities approved to sell weapons and ammunition.

1. Weapons and ammunition will be stored per this section and current Bureau of Alcohol, Tobacco, and Firearms (BATF) guidelines.
2. All ammunition will be stored in an approved security container until a sale is conducted. Empty ammunition boxes will be used for display purposes.
3. During hours of operation, maintain arms in display racks and cases and provide constant visual surveillance of the weapons and ammunition. Racks and cases must be locked with low security locking devices at all times, unless the weapon is being shown to a customer. All weapons displayed will be provided with a trigger lock. Only one model of each type of weapon will be displayed. MCCS employees are allowed to present one weapon to one customer at any time. Weapons transactions will be conducted behind a physical barrier (counter) and access to the weapons and weapons transaction space(s) will be limited to authorized MCCS employees.
4. Exchange personnel will comply with this Order, federal legislation, state laws, and local ordinances. Prominently display state laws and local ordinances adjacent to where sales take place.
5. A 100 percent sight count will be conducted daily and a 100 percent inventory by serial number monthly. All records will be maintained for a minimum of 3 years. These requirements are outside of inventory requirements directed by federal, state, and local guidelines.
6. The storage area housing the weapons and ammunition will be monitored by an intrusion detection system equipped with point sensors on all doors and volumetric sensors covering the storage area. A duress button will be provided in both the weapons storage area and at the weapons display/sales counter.
7. After normal operating hours, move all arms from sales areas to an armory or secure storage area. Weapons storage area

construction requirements are provided in paragraphs a. and b. below.

a. New facilities. Weapons storage areas for new resale facilities and Marine Corps Exchanges will not be constructed on exterior walls. These areas will be constructed within the inner walls of the facility, as a stand-alone space. Weapons storage areas will be constructed as indicated below:

(1) Walls. Walls will be constructed of 8-inch (200 mm) concrete masonry unit filled with mortar. Walls will be built from true floor to true ceiling, or minimum nine-gauge diamond metal mesh, constructed to a height of eight feet, with a continuous weld through all joints. The walls will be joined to the floor with a minimum 1/4-inch angle iron frame. The angle iron will be bolted to the floor with 1/4-inch bolts with bolt heads welded to prevent removal. Wall joints will be further framed with a 1/4-inch angle iron welded to both floor and ceiling angle iron framing. The entire weapons storage area may be framed in gypsum board.

(2) Floors. Floors will be constructed of 6-inch (150 mm) concrete.

(3) Roof/Ceiling. False or drop ceilings are prohibited within weapon storage areas. Weapons storage area ceilings will be constructed of 6-inch (150 mm) concrete with reinforcing bars or stiffeners, or minimum nine-gauge diamond metal mesh with a continuous weld through all joints. The ceiling will be further framed with 1/4-inch angle iron with continuous welds at all joints.

(4) Doors. Doors will be constructed in one of the following methods as indicated below:

(a) Constructed of 1 3/4-inch (44 mm) thick solid or laminated wood, with a 12-gauge (2.7 mm) steel plate on the outside face.

(b) Standard 1 3/4-inch thick (44 mm), hollow metal, industrial-type construction with 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 Jun 09

(5) Support Hardware. 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 the door frame. Frames and locks for doors will be designed and installed to prevent removal of the frame facing or built-in locking mechanism to allow disengagement of the lock bolt from outside.

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

(b) 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, security hinge type or equivalent.

(c) 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. Paragraph 5014 provides an example of hinge protection. Such devices must be of sufficient positive engagement and resistance to shearing force to prevent opening the door from the hinge side.

(6) Windows and Other Openings. Interior weapons storage areas/armories will be constructed without windows. All other windows, ducts, vents, or any opening of 96 square inches (0.06 square meters) or more with the least dimension greater than 6-inches (150 mm) will be protected by:

(a) Minimum 3/8 inch (9.5 mm) hardened steel rods with maximum 4-inch (100 mm) spacing with horizontal bars so that openings do not exceed 32 square inches (0.02 square meters); or

(b) Riveted steel grating (weight of 13.2 pounds per square foot (64.5 kilograms per square meter) or welded steel grating (weight of 8.1 pounds per square foot (39.6 kilograms per square meter) with 1 by 3/16 inch (25.4 mm by 4.7 mm) bearing bars.

(7) Locks and Hasps. Doors will be secured with a TUFLOC security lock or equivalent. An example lock is provided in figure 8-2.



Figure 8-2.--TUFLOC Door Lock

(8) Storage Containers. Weapons will be stored in accordance with this Order, federal, state, and local laws. Where allowed, weapons may be stored in the original box/container within the weapons storage area. Weapons and ammunition required to be stored in containers must be stored in a GSA approved Class 5 Weapons Containers/Safes or commercial weapons container.

b. Existing Facilities. Weapons storage areas for existing resale facilities and Marine Corps Exchanges will be constructed as indicated in paragraph (a) above, or as noted below. Facilities designated for upgrades or structural modifications will ensure requirements outlined in paragraph a. above (New Facilities) are incorporated.

(1) Walls. Existing walls will be reinforced with a minimum of nine-gauge diamond metal mesh. An option to retrofitting existing facilities is to construct a diamond metal mesh cage within the existing storage area with a continuous weld through all joints. The walls will be joined to the floor with a 1/4-inch angle iron frame. The angle iron will be bolted to the floor with 1/4-inch bolts with bolt heads welded to prevent removal. Wall joints will be further framed with 1/4-inch angle iron welded to both floor and ceiling angle iron framing.

(2) Floors. Floors will be constructed of concrete.

(3) Roof/Ceiling. False or drop ceilings are prohibited within weapon storage areas. Weapons storage area ceilings will be reinforced with a minimum of nine-gauge diamond metal mesh, unless the current ceiling is constructed of 6-inch concrete. An option to retrofitting existing facilities is to construct a diamond metal mesh cage within the existing storage area, with a continuous weld through all joints. The walls will be jointed

to the floor with a 1/4-inch angle iron frame. The angle iron will be bolted to the floor with 1/4-inch bolts with bolt head welded to prevent removal. Wall joints will be further framed with 1/4-inch angle iron welded to both floor and ceiling angle iron framing.

(4) Doors. Doors will be constructed in one of the following methods as indicated below:

(a) Constructed of 1 3/4-inch (44 mm) thick solid or laminated wood, with a 12-gauge (2.7 mm) steel plate on the outside face.

(b) Standard 1 3/4-inch thick (44 mm), hollow metal, industrial-type construction with minimum 14-gauge (1.9 mm) skin plate thickness, internally reinforced vertically with continuous steel stiffeners spaced 6-inches (150 mm) maximum on center.

(c) Metal mesh cage doors, within a secured area, will be constructed with the same material as the cage walls.

(5) Support Hardware. 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 the door frame. Frames and locks for doors will be designed and installed to prevent removal of the frame facing or built-in locking mechanism to allow disengagement of the lock bolt from outside.

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

(b) 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, security hinge type or equivalent.

(c) 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. Paragraph 5014 provides an example of hinge protection. Such devices must be of sufficient positive engagement and resistance to shearing force to prevent opening the door from the hinge side.

(6) Windows and Other Openings. Interior weapons storage areas/armories will be constructed without windows. All other windows, ducts, vents, or any opening of 96 square inches (0.06 square meters) or more with the least dimension greater than 6-inches (150 mm) will be protected by:

(a) Metal mesh secured to the walls, with all bolt heads peened or welded to prevent removal.

(b) Minimum 3/8 inch (9.5 mm) hardened steel rods with maximum 4-inch (100 mm) spacing with horizontal bars so that openings do not exceed 32 square inches (0.02 square meters).

(c) Riveted steel grating (weight of 13.2 pounds per square foot (64.5 kilograms per square meter) or welded steel grating (weight of 8.1 pounds per square foot (39.6 kilograms per square meter) with 1 by 3/16 inch (25.4 mm by 4.7 mm) bearing bars.

(7) Locks and Hasps. Doors will be secured with a TUFLOC security lock or equivalent. An example lock is provided in figure 8-2.

(8) Storage Containers. Weapons will be stored in accordance with this Order, federal, state, and local laws. Where allowed, weapons may be stored in the original box/container within the weapons storage area. Weapons and ammunition, required to be stored in containers, must be stored in a GSA approved Class 5 Weapons Container/Safe or commercial weapons container.

8022. MARINE CORPS MUSEUMS AND UNIT DISPLAYS. AA&E will be safeguarded per this instruction. 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 Historical Division.

1. Storage. Secure arms in an armory or appropriate container as prescribed in paragraph 8005.

2. Display. AA&E items will not be displayed if functional. Arms will only be displayed if they are modified to render them 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 when certified by Explosive Ordnance Disposal (EOD) unit personnel.

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 on all doors and volumetric sensors covering weapons display areas and man-passable openings greater than 96 square inches.

c. For items exhibited in static outdoor displays, remove minor caliber weapons (up to 25mm) from vehicles and mounts (weapons 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, unless provided with an ESS. The structure will be checked every 8 hours after non-duty hours, unless provided with an ESS.

3. Inventory arms by sight count every month, and by serial number every quarter. Inventory records will be maintained for 3 years.

4. Certificates of destructive or limited/minimum DEMIL for arms must be signed by a technically qualified U.S. government representative before AA&E is displayed, used for authorized ceremonial/training purposes, or DEMIL residue released for disposal. All DEMIL certificates will be maintained on site.

5. Certificates of destructive or limited/minimum DEMIL for ammunition must be signed by a technically qualified U.S. government representative, (EOD personnel) before displayed and/or used for authorized ceremonial/training purposes. All DEMIL certificates will be maintained on site.

8023. ORGANIC/UNIT AND STATION MOVEMENTS OF AA&E

1. Organic/Unit Movements. Commanding officers are required to 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. All movements must be conducted in accordance with reference (ae). An armed guard is required for the movement of any amount of AA&E greater than individual issue. Any changes will be reported to DC I&L(LPC) for evaluation of standards and modifications as necessary. Commanding Officers are directed to assess current FPCONS to evaluate the need for increased security of shipments during increased FPCONS.

2. Special Considerations for Category I items.

a. Shipments of Category I material by all modes require a continuous audit trail from shipper to consignee with advance certification of serial numbers of individual items or certified item. Two-man certification is required; that is, each container must be checked by two responsible agents of the shipper, and sealed and locked in their presence before delivery to the carrier. This rule applies at transshipment points and terminals whenever the original shipment loses its original identity; for example, when two or more shipments are consolidated into another container for further movement or if repacking is required.

b. For unit or organization movements, Category I material will be placed in the custody of a commissioned or warrant officer, staff-noncommissioned officer, or government service employee GS-9 or above.

c. When item design and manufacture specifications for personnel portable Category I ordnance indicate separate packaging for main body sections, launchers, and guidance/control components, these sections/components will be transported separately in separate freight containers (MILVAN/ISO) and/or separate motor vehicles. The Stinger Weapon round Category I, and the Stinger Gripstock, Category III, will be shipped on separate containers and/or vehicles. Movements aboard Military Prepositioned Ships (MPS) are excepted.

d. At overseas commands, local nationals may accompany U.S. personnel when SOFA prohibit arming of U.S. personnel.

3. On Station Movements. Guidance for on station movements is provided in references (av) and (aw). Additional guidance is contained within this paragraph. Movements via organic and commercial vehicles will adhere to all security requirements

with the exception that Satellite Motor Surveillance (SNS) is not required. AA&E contained in organic and commercial vehicles outside of restricted areas will be under constant surveillance. Organic movements of A&E require 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 AA&E.

c. Accountability for ammunition and explosives manufactured and renovated on station involving bulk explosives, propellants, and illuminants, will begin when the items become finished products.

d. AA&E contained in vehicles, vans, and railcars must be parked in designated restricted areas. AA&E will be under constant surveillance or each vehicle, van, and railcar will be physically inspected by a security patrol every hour. A numbered seal meeting specification FF-S-2738, "Seals Anti-Pilferage" Type 11 or 12 (latest revision) will be secured to each vehicle, van, or railcar door. Numbered seals and seal inventory records for movements and shipments will be provided security at all times to prevent theft or alteration.

4. Off-Station Movements. Movements will adhere to standards set forth in references (ae) and (ah), chapter 205, except that SNS is not required. The level of physical security protection will be applied based on the higher FPCON from origin to the destination. One explosive driver and one assistant driver is required for all A&E movements off-station, and the assistant driver will be armed. For AA&E off-station movements, the

drivers must possess a means to communicate with the originating installation, the destination installation, and municipal law enforcement and emergency response officials along the planned route. CAT I and CAT II off-station movements require a Security Escort Vehicle (SEV) under all FPCONs.

a. Off-station transport of small quantities of explosives and training aids by EOD and MWD personnel is authorized as directed by the installation commander. Personnel transporting explosives will be armed. The explosives will remain in constant surveillance of EOD or MWD personnel or be stored in an approved explosive container permanently secured to a Government Owned Vehicle (GOV).

b. Commanding officers may authorize transportation of small quantities (15 or fewer) of arms and associated ammunition to facilities on or near a military installation for marksmanship training, competition, testing, evaluation, and demonstrations, or other requirement on a case-by-case basis. Weapons and ammunition must be in the custody of a designated individual. Use of POV for transportation may be authorized by the commanding officer in writing. When POVs are used, the arms and ammunition must be securely stowed and protected from view.

5. Shipping and transportation. All shipments of AA&E, categorized in Appendix H will be protected against loss, theft, or damage. Protective Service requirements are provided in reference (ah), while safety, security, and traffic management guidelines during transportation of AA&E are addressed in references (av) and (aw). All classified AA&E will be stored and transported in accordance with this Order and reference (d). With the exception of inventory and daily checks, Military Preposition Ships (MPS) are exempt from AA&E requirements of this chapter. 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 commensurate with the requirements of this Order.

a. DC I&L (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. DC (I&L) will:

5 Jun 09

(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 FPCCON measures as provided in reference (av).

b. AA&E security at military and commercial terminals will conform to standards outlined in this chapter. 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 commanders will notify DC I&L and Security Division (PS) and compensatory measures will be established to lessen the threat.

(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

5 Jun 09

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 K. Receiving commercial and military activities must be capable of securing and protecting AA&E during normal working hours and 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 Constant Surveillance and Custody Service (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.

6. 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, all Category AA&E require constant surveillance until off-loaded.

7. 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.

8. OCONUS installations are required to coordinate with commands to arrange in-country security for delivery only to the nearest U.S. controlled port facility.

8024. SECURITY STANDARDS FOR SECURE HOLDING AREAS FOR AA&E.

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 identified in reference (av), outlined herein, will comply with references (ac) and (ad).

1. Security standards for the secure holding areas are as follows:

a. General. Secure holding areas for Category I and II AA&E must be under constant surveillance as outlined in this Order. Secure holding areas will have access control and be within an area surrounded by a perimeter fence to limit access. For situations in which the guard does not have direct unobstructed view of the entire secure holding area, it will have an IDS to provide added security.

b. Restricted Area Signs. Restricted area sign posting will be per paragraphs 3003 and 3004.

c. Access Control. The facility director will establish strict personnel and vehicle access measures for the secure holding area.

d. Fencing. Secure holding area fencing will be constructed in accordance with chapter 5.

e. Lighting. Protective lighting will be provided in accordance with chapter 3. Security lighting will be automatically timed to provide illumination from dusk until dawn. 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 ensure a lighting survey is conducted for each secure holding area to ensure that adequate lighting is provided in accordance with chapter 3 and this paragraph.

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. It will be periodically tested under load to ensure effectiveness, and located within a controlled area for additional security. All electrical cabling and telephone lines will be buried or those 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 be provided to alert local law enforcement and/or response forces to the presence of intruders. One form of communications may be a duress system.

i. 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. Security force requirements are addressed in chapter 4.

j. 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.

k. Coordination will be made with local, county or state law enforcement to provide additional security, including back-up forces, during higher FPCONs, as required.

2. The installation physical security plan, per paragraph 2002, will address the protection of secure holding areas.

3. 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.

8025. SPECIAL CONSIDERATIONS FOR SMALL QUANTITY SHIPMENTS. Small quantity shipments are individual shipments of 15 or fewer small arms (Category II through IV and M-16 rifles), or 200 pounds or less of sensitive CAT IV ammunition may be sent by commercial carrier providing DOD CIS (as the only required transportation protective service) when placed in a locked container, and the size, weight, and safety factors meet the carrier requirement. An acceptable alternative to DOD CSS for arms is the use of registered mail (return receipt requested) when size and weight meet USPS requirements. Small arms and missile components (excluding ammunition and explosives) may be sent by registered mail (return receipt requested) when the size and weight meet USPS requirements. Whether arms are shipped or mailed, all Security Risk Category II weapons will have their bolt removed, tagged with the weapon serial number, and sent in a separate box or container.

8026. REPORTING OF MISSING, LOST, STOLEN, AND RECOVERED 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.

8027. 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 will provide ISMT weapons the same level of storage as 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 will be provided the same level of security as high

dollar items. Weapons associated with SESAMS will be secured per paragraph 8005.

8028. STORAGE OF EVIDENTIARY AA&E. Arms and small arms ammunition may be stored together in the same area for evidentiary purposes in evidence rooms meeting requirements outlined in this paragraph and reference (w). Ammunition other than small arms, to include explosives, will not be stored in evidence rooms, but in an approved magazine. Evidence rooms are not required to meet the construction standards of paragraph 8005 and 8006 provided the following conditions are met:

1. Arms and ammunition are secured in approved but separate containers.
2. The evidence room is equipped with an ESS, including point sensors on openings and a volumetric sensor covering interior spaces, as identified in chapter 3.
3. If the security container storing the arms or ammunition is accessed, container contents will be inventoried upon opening and closing.

8029. STORAGE AND SECURITY OF PERSONAL WEAPONS AND AMMUNITION. Storage of personal weapons and ammunition in Marine Corps armories must be authorized, in writing, by the commanding officer. One copy of the authorization letter will be maintained in the affected armory, while the owner will maintain the original copy. Personal weapons or ammunition will not be stored in a magazine. Personal weapons will be provided security commensurate with that of government weapons.

1. Commanders authorizing storage of personal weapons and ammunition in armories will develop and maintain an order or SOP providing guidance to Marines wishing to store the weapon and to armory personnel. Policy/guidance will address check-out procedures for Marines to ensure that personal weapons and ammunition are removed from the armory and not left behind when checking out of a unit.
2. Requirements outlined in this Order and federal, state, and local statutes will be adhered to concerning possession of private arms and ammunition, including licensing and records requirements. All weapons stored in an armory will be registered on base with the Provost Marshal's Office.

5 Jun 09

3. 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.
4. Personal ammunition will be stored in a box/container, but never in the same box/container as government AA&E. The individual ammunition box/container is required to identify the owner, shell or casing count, and other identifying characteristics in order to maintain accountability.
5. Inventory of personal weapons and ammunition maintained in an armory will be conducted concurrently with unit level inventories. Personal weapons and ammunition will be listed, by serial number on a separate document from government weapons. Caliber or other distinguishing characteristics will be listed on the personal weapons and ammunition inventory checklist. Personal weapons and ammunition may be stored in private cases within containers. These cases may be sealed (with ball end, or similar seal) after an inventory is completed by the owner and armorer/custodian, and requires a logbook entry. For the purposes of daily sight counts, sealed cases can reflect the integrity of the container, similar to the inventory requirement for banded and sealed weapons crates and boxes. Monthly, serialized inventories will reflect the case seal number.
6. A logbook will be maintained for personal weapons and ammunition stored in the armory. All issue and receipt transactions will be recorded in a single event format. Logbooks will be opened and closed on an annual basis and will be retained for at least three years.
7. Withdrawal of ammunition or weapon(s) requires the owner(s) to provide a copy of the storage authorization letter to the armorer/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.
8. Loss or theft of personal weapons or ammunition will be reported immediately to the installation PMO.
9. In the event a personal weapon(s) or ammunition is abandoned in an armory, every attempt will be made to locate the owner(s) in accordance with reference (c) and Title 10 U.S. Code, 2575. Once the requirements of reference (c) and Title 10 U.S. Code, 2575 have been satisfied, and the owner(s) not located,

5 Jun 09

commanders will ensure that the weapon(s) and/or ammunition is destroyed in accordance with reference (ar). Additional information concerning lost and found property and abandoned property handling is provided in chapter 9, paragraph 9007.

10. Waiver and exception provisions do not apply to personal weapons and ammunition storage.

11. Storage of any ammunition greater than small arms ammunition, to include explosives, in government owned quarters is prohibited.

12. Storage of weapons and ammunition in BEQ (NCO & below) is strictly prohibited. Personal weapons storage within BOQ and Staff Non-Commissioned Officer (SNCO) BEQ is at the discretion of the installation commander. All weapons and ammunition will be stored in approved containers. Weapons containers must be capable of being locked. All weapons will be fitted with a trigger lock. Installation commanders will publish directives pursuant to this Order, federal, state and local statutes.

13. Personal weapons may be maintained in government family quarters pursuant to the installation commander's guidance. All weapons and ammunition will be stored in approved containers. Weapons containers must be capable of being locked. All weapons will be fitted with a trigger lock. Installation commanders will publish directives pursuant to this Order, federal, state and local statutes.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 9

CRIME PREVENTION

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|--|------------------|-------------|
| GENERAL | 9000 | 9-3 |
| PROGRAM ELEMENTS | 9001 | 9-3 |
| PROGRAM OBJECTIVE | 9002 | 9-3 |
| CRIME FACTORS | 9003 | 9-4 |
| RESPONSIBILITIES | 9004 | 9-4 |
| SCOPE | 9005 | 9-5 |
| COMMUNITY RELATIONS/CRIME PREVENTION EDUCATION AND AWARENESS PROGRAMS | 9006 | 9-8 |
| LOST, FOUND, AND ABANDONED PROPERTY | 9007 | 9-10 |
| MARINE CORPS COMMUNITY SERVICES RESALE AND EXCHANGE FACILITIES CRIME AND LOSS PREVENTION | 9008 | 9-17 |
| SECURITY OF FUNDS | 9009 | 9-22 |
| SECURITY OF GOVERNMENT PROPERTY | 9010 | 9-22 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 9

CRIME PREVENTION

9000. GENERAL. Crime prevention is any measure taken to reduce the opportunity for crime by improving community safety through measures to include increased awareness and confidence, improved planning and design, and committing to strategies and programs that address risk factors. Crime prevention is key to quality of life issues in an effort to minimize hazards and threats within our communities that result from criminal and anti-social behavior. Installation commanders will support crime prevention in an effort to protect Marines, Sailors, family members and civilian employees 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 employees. 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. 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 (LAN), dedicated websites), and crime prevention material (pamphlets, handouts, etc).

b. Prevention focuses on reducing conditions conducive to criminals committing crimes against the persons and property, such as maintenance of lights, demolition of old, abandoned buildings, and removal of abandoned vehicles. 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. 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 employees 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 installation population, 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 employees. 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 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. Commanders are encouraged to develop, support, and maintain those programs outlined in

paragraph 9006. The following paragraphs delineate mandatory requirements of the Crime Prevention Program.

a. The provost marshal will ensure that a crime prevention brief is conducted as a part of the monthly command Welcome Aboard Brief.

b. Crime prevention awareness/education information will be presented on a monthly basis to the base population via available news media.

c. The Physical Security Office is responsible for maintaining a record detailing all Crime Prevention Program activity. Entries should detail the date, type of program, requesting command/unit/ activity, and attendance, at a minimum.

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; personnel officer; base inspector; chaplain; comptroller; Substance Abuse Counseling Officer (SACO); public affairs officer; facilities officer; Marine Corps Community Services; Navy/Marine Corps Relief Society.

2. Media Use. Installation commanders must 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 LAN announcements are excellent media platforms. Banners, handouts, and bumper stickers are excellent vehicles for promoting the program. Commanders at the company level and higher will ensure command bulletin boards contain Crime Prevention materials that reinforce issues such as securing valuables and wall lockers. Commanders will further 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. Surveys recommend

corrective action to a commander to reduce the opportunity for crime.

a. Physical security specialists assigned to the PMO will conduct the surveys.

b. 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. Surveys will be completed using the NAVMC Form 11121 or an equivalent electronic copy. A guide for preparation, completion, and distribution of surveys is provided in Appendix F.

d. 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 (cash, checks, etc).
- (4) Facilities designated by the installation commander.
- (5) Facilities requested by unit commanders, at the discretion of the Provost Marshal.
- (6) Tenant organizations such as banks, credit unions, concessionaires as noted in the installation/organization MOA.

4. Armed Forces Disciplinary Control Board. Installation Commanders will establish and maintain an installation Armed Forces Disciplinary Control Board (AFDCB) in accordance with reference (ax). The board will meet on a quarterly basis to identify establishments/areas in local communities that are detrimental to the well being of Marines. The board will maintain contact with other Service installations in the area to coordinate and exchange information. Board results will be published and disseminated to ensure all Marines kept informed. Unit commanders are required to brief their Marines and post the AFDCB findings in conspicuous locations.

5 Jun 09

5. Crime Analysis. Crime analysis is a systematic, analytical process that provides information regarding crime trends and patterns aboard the installation. An effective crime prevention program requires a systematic approach and crime analysis identifies target areas for increased crime prevention efforts.

a. Types of Crime Analysis

(1) Tactical Crime Analysis. An analytical process that provides information used to assist operations personnel (patrol and investigative officers) in identifying specific and immediate crime trends, patterns, series, sprees, and hotspots, providing investigative leads, and clearing cases. Analysis includes associating criminal activity by method of the crime, time, date, location, suspect, vehicle, and other types of information.

(2) Strategic. Concerned with long-range problems and projections of long-term increases or decreases in crime (crime trends). Strategic analysis also includes the preparation of crime statistical summaries, resource acquisition, and allocation studies.

(3) Administrative. Focuses on provision of economics, geographic, or social information to administration.

b. The most commonly used process for supporting and maintaining crime analysis is crime mapping. Crime mapping involves the use of color-coded pins to identifying a specific crime. The crime is plotted on an installation map at the location of the crime. To produce accurate and effective crime analysis using crime mapping, there are three factors to consider: the purpose of the map, the audience of the map, and types of data to include in the map.

c. The goal of crime mapping is to identify problem areas on the installation that require increased crime prevention efforts. These efforts may include additional Military Police patrols, increased education, or command attention. Crime mapping provides a visual media that isolates problem areas and may be included in the plan of action to reduce criminal activity in the area. Crime mapping must be maintained in order to be effective.

d. There are automated software applications available that maintain crime mapping to automate this process. Some of the

systems may be used in conjunction with a Global Positioning System (GPS).

6. Crime Prevention Funding. Funding crime prevention programs is the responsibility of the installation Commander. Provost marshals will seek funding annually from the installation comptroller in support of programs outlined in paragraph 9006. There are several other Marine Corps programs (drug and alcohol control counselors, family advocacy, Marine Corps Community Services, etc) that receive funding annually to support crime prevention programs unique to their areas of interest. Other sources of support include Enlisted and Officers Wives Clubs. Commanders and provost marshals must work with such interest groups in a joint effort to promote crime prevention aboard the installation.

9006. COMMUNITY RELATIONS/CRIME PREVENTION EDUCATION AND AWARENESS PROGRAMS. There are a number of Crime Prevention Program options available to commanders. National, state, and local programs (National Crime Prevention Council, state crime prevention offices, etc) offer further guidance and information. Commanders are encouraged to use all available assets to supplement the program including installation specific designs. Installation commanders and provost marshals need to design their education and awareness programs around the specific needs of their military community. Proven programs include:

1. 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.

2. 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 personnel.

3. Officer Friendly. Designed to familiarize children and adults with the roles and responsibilities of military police personnel, and enhance community relations.

4. 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 crime trends and can target specific event crime prevention tips (Halloween, Christmas, etc.). Common Marine Corps target areas are ideal for command emphasis and education. Target areas include, but are not limited to:

- 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. Underage alcohol consumption.
- f. Drinking and driving.
- g. Installation and state, county, and city rules, regulations and ordinances.
- h. Identity theft.

5. Child and Spouse Abuse. Designed to increase community awareness of signs of abuse and available services and support. Local police departments, abuse counseling centers, and the installation Family Service Center should be invited to attend as part of a community education effort.

NOTE: Physical abuse of a child or spouse is punishable under the Uniformed Code of Military Justice (UCMJ), federal, and state statutes. Actual or suspected abuse discovered by medical, school, daycare, or other persons will be immediately reported to the PMO for investigation and further reporting requirements.

6. Crime Prevention Month. Using all available media, this effort is directed at increasing community awareness of the crime(s) affecting the community, what people can do in the community, and what resources are available to deter and reduce crime.

7. Lady Beware. An informational program developed with the goal of increasing public awareness of rape and sexual assault. Emphasis is placed on high-risk situation avoidance. Local police departments, Rape Crisis Centers, and the installation

5 Jun 09

Family Service Center should be invited to attend as part of a community education effort.

8. National Night Out. The National Night Out Campaign involves citizens, law enforcement agencies, civic groups, businesses, and local officials. National Night Out has proven to be an effective, inexpensive and enjoyable way to promote neighborhood spirit and police-community partnerships. Along with traditional tactical equipment displays, block parties, and other activities, turning on outdoor and porch lights is symbolic of the community's effort to fight crime and support local law enforcement.

9007. LOST, FOUND, AND ABANDONED PROPERTY. Lost, found, and 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. Found or abandoned property will be turned over to the military police. All found or abandoned property will be handled in accordance with references (c) and (ar). The provost marshal will publish instructions for the receipt, handling, and disposal of found or abandoned property.

b. All government property designated as found or abandoned will be initially treated as lost and found property, and processed in accordance with this Section. 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 Investigation 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 designated in writing on an

5 Jun 09

unaccompanied access roster. The access roster will be maintained inside the main entry point.

f. A container, designated and marked as the Temporary Lost and Found Locker, will be provided for short-term storage after normal working hours. Access to the container will be restricted to the primary and alternate lost and found custodian. The container will be maintained within a non-public, controlled area.

2. Property Receipt and Storage

a. Military police personnel 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 mark the property with a Department of the Navy Evidence Tag (OPNAV 5527/17B).

b. The PMO Desk Sergeant will 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 temporary lost and found locker, the lost and found custodian will secure property in the lost and found secure storage area.

d. All property will be immediately entered in a lost and found property logbook or binder. Lost and found property logbooks/binders 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 (e.g. 001-06, 002-06, etc.). Each entry will identify, at a minimum: the Case Control Number (CCN), the date of receipt, a brief item description, final item disposition, date of final disposition, and the initials of the custodian responsible for the 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 item(s) were published for public information as required by federal law. The case folder will also contain the original Property Custody Receipt once the

5 Jun 09

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 special instructions. In events not covered, lost and found custodians will obtain further guidance from the provost marshal.

a. Firearms

(1) Definition. For the purposes of this chapter, firearms are defined as a weapon and all components thereof, not over .50 caliber that is designed to, or may be readily converted to expel a projectile. 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, the CID will be notified. The on-duty CID agent will be responsible for assuming custody, or determining further disposition. Any weapons assumed by CID as evidence will remain in CID custody until final disposition.

(3) Destruction. Firearms not claimed by the owner will be destroyed. A certified armorer will accomplish destruction in accordance with the reference (ar). The CID Evidence 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 (ammunition, explosives, etc.) will be reported immediately to the CID and the installation EOD Unit. All ordnance will be turned over immediately to the EOD Unit for disposition. Disposition of ordnance having evidentiary value will be coordinated with the CID and EOD unit. All Marines will be instructed to treat ordnance as unstable and ensure that only authorized, trained personnel handle the ordnance. In the event that an installation does not maintain an EOD presence, the closest military installation with an EOD unit will be contacted.

c. Alcoholic Beverages/Perishable Goods. All alcoholic beverages and perishable goods will be disposed of by emptying the contents in an approved location. The provost marshal will

provide disposal instructions. 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 negotiable instruments, not claimed will be turned over to the installation Disbursing/Finance Office. For those installations without a Disbursing/Finance Office, lost and found custodians will turn in the item(s) to the closest Disbursing/Finance office, regardless of Service. Responsible financial institutions will be contacted in the event of found checks and credit cards, to establish contact with the owner. In the event the owner is not located, the provost marshal will direct disposition (destruction/mailing to the responsible company) of the items.

e. Department of Defense Identification Cards and Badges. Department of Defense U.S. Government Identification cards will be turned in to the installation Centralized Identification Center/Defense Enrollment Eligibility Reporting System (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 may include, 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. Military police personnel and lost and found custodians are required to check with the CID to ensure items have no evidentiary value. Once determined that the item(s) has no evidentiary value, the property will be destroyed immediately. The lost and found custodian and one other witness will conduct/witness destruction of the contraband 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 immediately. Disposition will be noted on the Property Custody Receipt.

h. Vehicles. Reference (p) provides further instructions for disposition of abandoned vehicles, motorcycles, mopeds, other motorized vehicles, to include trailers, aboard the

installation.

i. Watercraft. Handling, storage, and disposition of boats and other watercrafts, to include trailers, will be conducted in the same manner as identified in reference (p).

j. Lost and found property stock will be inventoried on a quarterly basis by an officer, SNCO, or civilian GS-9 or above, not directly involved in the supervision of the lost and found custodians.

k. In any case not covered by this instruction the provost marshal will provide guidance.

4. Public Notice

1. The lost and found custodian will advertise lost items in the installation newspaper, television station, and LAN, at least twice a month. The media article will provide a brief description of an item, the lost and found custodian's name and contact number, and instructions for reclamation of the property during normal business hours. A note of the date of the advertisement will be made in the appropriate lost and found case file for each item mentioned.

2. With the exception of contraband and dangerous items, the lost and found custodian will take all necessary steps to locate the owner(s) of 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 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 distinguishing an owner, check base and worldwide locators, local telephone books, and/or LAN/email databases for a possible lead to the owner.

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 (c) and (ar). 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 owner's 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.

5 Jun 09

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, of this section, must be presented to a lost and found disposal board for final disposition instructions as required in references (c) and (ar). 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 at least two SNCOs, or civilian equivalent (GS-9 or above), assigned in writing by the provost marshal will convene the board. 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 final 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 will require a copy of the disposal board findings and a DD Form 1348-6 (DOD Single Line Item Requisition System Document).

5 Jun 09

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. All records will be disposed of in accordance with installation requirements.

9008. MARINE CORPS COMMUNITY SERVICES RESALE AND EXCHANGE FACILITIES CRIME AND LOSS PREVENTION. Marine Corps Community Services Resale and Exchange facilities, to include Convenience/7-Day Stores will maintain a vigorous Crime and Loss Prevention program. Marine Corps Exchange (MCX) facilities will meet all requirements of this Order to include requirements outlined in this paragraph. MCX facilities will meet all construction requirements outlined in reference (i) and (j). Further guidance concerning merchandise loss prevention requirements are provided in reference (ay). Requirements for the storage of weapons and ammunition sold in MCX facilities are addressed in paragraph 8021.

1. Facility Requirements

a. Entry/exit doors will be kept to a minimum allowed for safety. 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 and high value storage area doors will be constructed of solid metal and 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 will be equipped

5 Jun 09

with a peephole to enable employees to identify person(s) outside prior to opening door. Security glass may be used in cash cages, but will not allow a view to the interior.

f. Warehouse Doors. Doors to warehouses will be secured with mortise locks and deadbolt assemblies. Overhead doors will be metal, rollup doors, secured on the inside with padlocks and chains. When roll-up doors are in the up position during normal working hours, a gate will be provided on the interior of the roll-up door to prohibit unauthorized persons from entering the warehouse. The gate will be constructed as a double gate to a minimum height of five feet with nine gauge metal mesh and welded or bolted to the doorframe to prevent removal. It will be provided with a 1/2-inch rod on each gate that can be anchored in a hole on the floor to further secure the gate. As an added security measure the gate may be secured with a 5/16-inch chain and a padlock during non-working hours. The interior gate provides additional protection during non-working hours when used in conjunction with the regular doors.

2. Accessible Openings. All windows will be equipped with locking devices. Windows located within 18 feet of the ground that provide entry into cash handling, high value 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. Any opening of 96 square inches or more and man-passable, will be protected by hardened steel rods or security grating.

3. Lighting. Facility lighting will meet requirements outlined in paragraph 3011.

4. Electronic Security Systems. In accordance with chapter 6, any commercial alarm systems procured that will annunciate at, or be monitored by PMO will be compatible with the MCESS. This will eliminate proliferation of multiple alarm systems installed at PMO. Commands may continue to use their current alarm system until 2012, at which time it will be replaced with a MCESS compatible system. Additional requirements for MCESS are provided in chapter 6. MCX Cash cages, registers, exterior doors, windows, and accessible openings must be equipped with electronic security. MCX Managers will coordinate installation, maintenance and testing with the installation PMO. 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 allows clean-up and stock crews to work in a portion of a facility without compromising security in cash offices, warehouses, stock rooms, etc. Systems, including duress alarms will be tested semi-annually. 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. Security can be maintained only if keys to exchange spaces are properly safeguarded and if access is controlled. Key and lock control will be established in accordance with paragraph 3005. 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 panic bar and alarm. The exchange manager or a designee, authorized in writing, will be responsible for key control. Keys will be marked with an identity number so that personnel can readily identify the location the key allows access. Duplicate or spare keys will be kept in a locked cabinet in a secure area, accessible only to the key custodian. Lock cores must be changed whenever the system is compromised through theft or loss of keys, or through employee termination. Records must be continually updated to reflect these changes.

6. Opening and Closing Procedures. When an activity is opened, an inspection will be immediately conducted to include, but not limited to safes, doors, security room windows, weapons storage facilities, and stockroom merchandise. Any evidence of burglary or attempted burglary will be reported to PMO immediately. Nothing will be touched or disturbed until military police have completed a preliminary investigation. A supervisor and at least one other employee will be responsible for the daily opening and closing of an activity. An opening and closing checklist will be used. During closing, personnel will conduct an inspection of the premises. The inspection will ensure that all safes, doors, windows, etc., have been secured, and that no person(s) is hiding in bathrooms, stockrooms, warehouse, or any area of the exchange. Upon completion of the inspection, the alarm will be set and personnel will exit the premises.

7. Cash Handling. The exchange manager or designee will establish written procedures for handling and safeguarding cash instruments and ensure familiarity with those procedures by all

employees. Procedures will address maintaining minimum cash on hand for cashiers.

8. Cash Handling Spaces. Cash cages and check cashing offices require additional security measures.

(1) Cage Construction. Cash 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 security glass view panel (no larger than 6-inches by 6-inches) or peephole to allow cashiers to identify persons requesting entry. Teller 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 manager. Security or supervisory personnel will escort unauthorized persons requiring entry. Cash office doors will be posted to identify the area as a restricted area and entry is prohibited by unauthorized personnel.

(3) Cash cages will be equipped with magnetic door contacts, a volumetric sensor, and a duress alarm zoned separately from the facility IDS. This will allow the cash cage to remain activated while the facility alarm system is deactivated.

(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 will remain locked at all times with the combination dial engaged unless opened for withdrawals or deposits. Staging locks is prohibited.

9. Cash Storage Containers. A GSA approved safe will be provided for the storage of all funds. Each individual responsible for a major account will be provided a safe. Exceptions will be cashiers and salesclerks who have custody of the funds only for daily purposes. Safes weighing less than 750 pounds will be secured to the structure to prevent removal.

5 Jun 09

a. Safes will be located in a secure area, where access is restricted. The room will be provided with a volumetric sensor.

b. When opening a safe, the dial will be shielded to prevent compromise of the combination. Safes will not be left in a day-lock position with the dial turned slightly off last combination letter for convenience. Unless opened for withdrawals or deposits, safes will be locked at all times with the combination dial spun.

c. The exchange manager 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 and securely sealed in such manner that it cannot be opened without mutilating the envelope or seal. The envelope will be delivered to the exchange manager, for safekeeping, who will issue a receipt for the envelope. Sealed envelopes, containing safe combinations will be secured in a safe under the exchange manager's direct control. The safe containing the envelopes will be opened, only in an emergency situation, by the exchange manager and in the presence of at least one witness.

d. Combinations changes to safes will be conducted in accordance with paragraph 3005.11. 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.

e. Numbers used for safe combinations should be randomly selected rather than based on birthdays, telephone numbers, or addresses, etc., of persons having the combination.

10. 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. The determination of adequate physical security for warehouses is a management decision taking into consideration location, structural integrity of the building and the value of assets stored.

11. Employee Guidance

a. Employees will be provided with an area where personal gear may be secured. Lockers should be constructed to allow supervisory personnel the opportunity to view what is stored inside individual lockers.

5 Jun 09

b. Employees will be provided with a parking area, away from exchange and warehouse entrances and exits. Guidelines regarding lockers, packages, and parking will be conspicuously displayed in employee break areas.

c. Employees will be instructed to use a single point upon entering and exiting the facility. The Exchange Officer will designate the entrance/exit and the policy will be strictly enforced. Employees will not be allowed to exit and enter through fire doors, back doors, warehouse loading docks, etc., based on convenience.

12. Service Station Operation

a. Managers or designees will retain keys to fuel pumps and storage tanks.

b. Cash Control. All cash register controls discussed in this chapter apply to registers in service stations.

(1) Each cashier will be assigned their own drawer and access to the drawer will be limited to that individual only.

(2) The service station manager will verify, record, and reconcile the total fuel pump and cash register readings.

(3) A minimum amount of cash will be retained in the cash register at all times.

(4) Managers will periodically inspect trash removal areas to ensure merchandise is not being disposed of. Cartons will be broken down and folded flat.

9009. SECURITY OF FUNDS. Physical security requirements for funds under control of a Disbursing/Finance Officer or stored within a Disbursing/Finance Office are contained in reference (az).

9010. SECURITY OF GOVERNMENT PROPERTY

1. All U.S. Government computers, typewriters, and similar office equipment will be marked in some fashion to identify the item as U.S. Government property. During non-duty hours, office doors will be secured and access controlled.

2. Video recorders, televisions, film projectors, and similar

5 Jun 09

items used for mission-related audio-visual purposes will be stored in spaces where access is controlled during normal duty hours. These items will also be marked with identification tags identifying them as U.S. Government property.

3. Government owned televisions and other audio-visual equipment within clubs, lounges, and transient and permanent personnel housing will be secured to prevent theft. These items will also be marked with identification tags identifying them as U.S. Government property. A recommended method is to secure the item in place with commercially available anchor pads or similar securing devices.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 10

REPORTING REQUIREMENTS

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|---|------------------|-------------|
| GENERAL | 10000 | 10-3 |
| MISSING, LOST, STOLEN, AND RECOVERED (MLSR) REPORTING | 10001 | 10-3 |
| DEPARTMENT OF DEFENSE AA&E ANNUAL REPORT | 10002 | 10-10 |
| OTHER AA&E REPORTING REQUIREMENTS | 10003 | 10-11 |
| LAW ENFORCEMENT AND PHYSICAL SECURITY ACTIVITIES REPORT (LEPSAR) | 10004 | 10-11 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 10

REPORTING REQUIREMENTS

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 property under his or her jurisdiction. Property issued to individuals does not become private property by act of issuance or possession, but remains government property that 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 Marine Corps to centrally track material losses and to identify trends and areas where security enhancements may be required.

1. Unit commanders and military police agencies will promptly receive all pertinent information concerning losses of government property. Physical security deficiencies and operating practices that contributed to such losses must be investigated and corrective action taken.
2. MLSR reporting assists the provost marshal in determining the adequacy of command loss prevention and physical security programs, and enables Marine Corps-wide statistics on all formal account adjustments to be accumulated by CMC(LPC-2).
3. MLSR reports do not waive the accountability requirements for loss/gain reports prescribed by other Marine Corps directives, nor for causative research and vouchering requirements prescribed by references (a) through (an).
4. MLSR reports are required only if actual gains or losses have occurred.
5. MLSR reports will be generated as soon as possible but not later than 48 hours after the occurrence. Report Control Number DD-5530-01 is assigned to this reporting requirement. 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 an MLSR was submitted and further research revealed an administrative error, then an additional MLSR is required to be submitted to correct the reported error.

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; however missing, lost, or stolen privately owned weapons will be reported to PMO. Found or recovered privately owned weapons will be turned over to PMO.

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 L.

b. All Navy funded aviation ordnance items in possession of Marine Corps units.

c. All Marine Corps Ground Equipment Resource Reporting (MCGERR) reportable equipment as published in the Marine Corps Bulletin (3000 series), regardless of dollar value.

d. Precious metals valued over \$100 and presentation or commemorative silver. Precious metals include, but are not limited to; refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium in bar, ingot, granule, liquid, sponge, or wire form.

e. Losses of controlled substances (e.g., narcotics, barbiturates, amphetamines, etc.) are not included under the MLSR program and shall be reported as prescribed in chapter 21 of reference (ab). For losses aboard Marine Corps

installations, also submit a copy of Drug Enforcement Administration (DEA) Form 106 to PMO.

f. Classified printed material losses are not included under the MLSR program and will be reported as prescribed in reference (d). 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 all Marine Corps activities will submit reports of all MLSR to CMC (PS/LPC) with copies to the chain of command, NAVSURFWARCENDIV Crane, Code JXNP, 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 aboard an installation will promptly submit appropriate information relating to theft or suspected theft of AA&E to the local PMO. Commands required to release a MLSR report will ensure that a copy of the MLSR has been provided to the installation PMO Physical Security Section. Commands not aboard Marine Corps installations will refer MLSR incidents to the nearest NCIS office for investigation or further referral to outside agencies.

c. Activities 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 M. 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 (a1).

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.

From: COMMANDER MCB QUANTICO VA
Sent: Wednesday, June 04, 2004, 2:48
To: CMC WASHINGTON DC PPO PS (uc)
CMC WASHINGTON DC L LPC (uc)
NAVSURFWARCENDIV CRANE IN (uc)
COMMARCORSYCOM AM-IMS (uc)
COMMARCORLOGCOM ALBANY GA (uc)
Subj: R 041718Z JUN 04 MLSR SENSITIVE MATERIAL REPORT

Importance: Low

MSGID/GENADMIN//
SUBJ/MLSR SENSITIVE MATERIAL REPORT
(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

9. Notification to Law Enforcement Activities. Timely notification of all reportable losses and recoveries, as well as losses which are not reportable under this Order will enable 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.

5 Jun 09

a. For thefts observed while in progress or immediately afterwards, telephonic reports will be made immediately to the military (or civilian) authorities with descriptions of suspects, vehicles, and property involved.

b. All commands having an installation PMO will immediately make telephonic notification to the PMO upon discovery of an MLSR reportable incident. This notification is independent of the MLSR reporting process and will 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 authorities.

(1) When NCIS declines to investigate missing AA&E, they will immediately notify the command security officer and provost marshal of the accountable or host command, who will conduct 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 five years.

10. Notification to DOD, Director of Security. Security Division (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. Security Division (PS) will review all MLSR message reports involving AA&E and other sensitive government property

losses for physical security deficiencies. When required, Security Division (PS) will assist activities to correct problems, which necessitated the MLSR submission. Security Division (PS) will maintain statistics on MLSR reporting of losses and recoveries and when required, report all related information to concerned DOD activities. Security Division (PS) will conduct an analysis to determine whether losses were a result of criminal acts.

b. CMC(LPC-2) will review all MLSR message reports involving AA&E. CMC(LPC-2) 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. Commander, Marine Corps Logistics Command (COMMARCORLOGCOM), upon receipt of all MLSR messages, will coordinate with NSWC, Crane, to ensure an enterprise wide search is executed and respond to all addressees with findings. COMMARCORLOGCOM will also coordinate with NSWC Crane, CMC I&L (LPC), and Security Division (PS), to provide an automated central repository for all automated MLSR messages. The central repository will provide capability to search MLSR messages for specific serial numbers in conduct of causative research and for historical research. A quarterly report will be provided to CMC I&L(LPC) of all MLSR messages broken down by both category (missing, lost, stolen, recovered) and by major subordinate command.

(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 Appendix M for familiarization with the requirement.

d. Commander, Marine Corps Systems Command (COMMARCORSYSCOM) (PM Ammo) will review all MLSR message reports involving ammunition and explosives (A&E). PM Ammo will conduct trend analysis of A&E losses to identify trends and areas where A&E management procedures might be enhanced. Additionally, PM Ammo will provide amplifying instructions for contingency operations if not covered within this order.

5 Jun 09

e. Commander, NSWC, Crane, IN, Code JXNP is responsible for managing a registry of DoN arms and day-to-day management of the MLSR process.

f. COMMARFORS will ensure that in addition to basic Commander's responsibilities to safeguard all government property in the unit's charge, all Commanders at all levels within their AOR will:

(1) Report MLSR reportable items to SECURITY DIVISION (PS) and (LPC-2) in the MLSR format as prescribed in Appendix M. This report will be made 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 five days prevented prompt submission of the report). Final MLSR reports will be submitted within 45 days of the initial report. If unable to finalize the MLSR report, a status update will be due at that time and subsequent updates will be made at 90, 150, 180, and every 30 days thereafter or until the final MLSR report is released referencing the initial report by report number, date time group (DTG) or correspondence identification.

(2) Report MLSR reportable items to the nearest law enforcement agency to include the PMO aboard Marine Corps installations, the nearest NCIS resident agency or to the local law enforcement agency when the unit is not located aboard a Marine Corps installation.

g. All personnel have the legal and moral responsibility to report missing, lost, stolen, or recovered government property and must do so immediately upon discovery, to the command responsible officer accountable for the MLSR reportable government property.

10002. DEPARTMENT OF DEFENSE 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 per reference (b). 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 (BATF), 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.

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 Security Division (PS) as follows:

1. Installation Crime Statistics for the period of 1 January to 31 December of any given calendar year will be submitted not later than 1 February of the following calendar year. This reporting requirement is exempt from reports control per reference (ba), Part IV, paragraph 7.g. This report will be cumulative in nature.

2. Installation provost marshals will maintain statistics to be available to the Security Division (PS) upon request. All criminal offenses brought to the attention of Marine Corps commands aboard Marine Corps installations will be reported to the provost marshal for appropriate action.

3. Installation annual crime statistics will be submitted using NAVMC 11197 (LEPSAR Report), an example form is provided in Appendix N. An electronic copy may be obtained at <http://www.marines.mil/units/hqmc/Pages/default.aspx> by linking to the forms library through News, Publications, then Marine Corps Forms. Instructions on completing the NAVMC 11197, paper or electronic form, are discussed in Appendix N.

4. All LEPSAR Reports will be retained by Security Division (PS) and the installation provost marshal for a period of 3 years after the date of submission, and thereafter destroyed.

MCO 5530.14A

5 Jun 09

5. Security Division (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 Security Division (PS) initiatives can be implemented that will assist installation commanders in reducing the crime.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 11

EXPEDITIONARY PHYSICAL SECURITY

| | <u>PARAGRAPH</u> | <u>PAGE</u> |
|---|------------------|-------------|
| GENERAL | 11000 | 11-3 |
| CHALLENGES AND THREATS | 11001 | 11-3 |
| EXPEDITIONARY PHYSICAL SECURITY SUPPORT . | 11002 | 11-4 |
| SITE SURVEY | 11003 | 11-5 |
| PROTECTIVE MEASURES | 11004 | 11-6 |
| SYSTEMS APPROACH | 11005 | 11-8 |
| DEFENSE IN DEPTH | 10006 | 11-13 |
| EXPEDITIONARY AIRFIELD (EAF) SECURITY . . | 11007 | 11-14 |
| AA&E STORAGE SITE SECURITY | 11008 | 11-15 |
| CRITICAL INFRASTRUCTURE PROTECTION . . . | 11009 | 11-16 |
| PORT AND WATERSIDE SECURITY | 11010 | 11-16 |
| PHYSICAL SECURITY PLAN | 11011 | 11-19 |
| PHYSICAL SECURITY SURVEYS | 11012 | 11-19 |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

CHAPTER 11

EXPEDITIONARY PHYSICAL SECURITY

11000. GENERAL. During combat or tactical operations and Military Operations Other Than War (MOOTW), Marines operate in environments where inhabitant emotions range from passive and tolerant to those openly and continuously hostile. Commanders must address a number of security and force protection concerns as they assume an inherent security mission that includes protecting personnel, equipment, and facilities; protecting lines of communications; preventing or minimizing disruption of command and control and support operations; and neutralizing, defeating, or containing rear area threats.

1. Physical security is paramount to mission accomplishment and must be included in all planning. It is seamlessly integrated into operations conducted at Forward Operating Bases (FOBs), Forward Arming and Refueling Points (FARPs), fixed sites, and temporary sites.

2. Physical security equipment and practices deter persons from attempted entry, detect penetration, and delay or deny access to an asset. Physical security strengthens the overall site FP and AT posture.

11001. CHALLENGES AND THREATS. Maintaining combat operations and operational tempo are two of the most significant challenges for commanders. Establishing and maintaining security at one site or a number of sites is another.

1. Host nations present a number of security concerns with regard to agreements involving use of force, personnel in security and support positions, use of security technology and communications, and inadequate infrastructure.

2. Restricted space availability, encroachment, and urban proximity limit a commander's options in security and defense.

3. Marines face a number of traditional and non-traditional threats and tactics from enemy personnel, terrorists, and criminals. Aggressor's objectives include inflicting injury or death, destroying and/or damaging facilities, property, equipment, and resources, stealing equipment, material and information. Objectives are attempted, and in some cases completed with weapons, tactics, and tools that form the basis

for threats to Marines and the mission. Threats result in the loss of life, disruption to the mission, compromise of sensitive information, and damage, loss, and destruction of property.

4. The impact of these threats, tactics, and challenges can be minimized through proactive measures and random changes to the site and area security posture.

11002. EXPEDITIONARY PHYSICAL SECURITY SUPPORT. Provost marshals provide commanders with military police subject matter expertise, including physical security, which is outside of the scope of ATOs. Physical security specialists apply directives and learned skills to establish a sound security posture. The application includes general requirements and comprehensive initiatives for protecting specific resources including Expeditionary Airfields (EAFs), ports, AA&E, and critical infrastructure.

1. Physical security specialists, under the purview of the provost marshal:

a. Assess threats, identify hazards, and recommend the employment of defensive measures.

b. Employ procedural and physical protective measures to safeguard personnel, prevent unauthorized access to equipment, material, and documents, and defend against espionage, sabotage, damage, and theft. Application of these measures mitigates and in some cases, prevents threats.

c. Conduct physical security surveys of those sites outlined in paragraph 11012 and as directed.

d. Assist in the design and employment of physical security equipment at ECFs and ACPs.

e. Identify critical infrastructure.

f. Research and develop physical security plans.

g. Assess the security and force protection posture of a facilities construction.

h. Provide loss prevention support.

i. Provide technical equipment support.

5 Jun 09

j. Provide operation training for security equipment.

2. Pre-deployment coordination and planning between military police, planning (G3), and logistics (G4) personnel is essential. A host of security support equipment (barriers, sensor suites, portable lighting, generators, etc.) is available to Commanders. Coordination and planning allows physical security personnel to identify logistics requirements for equipment and logistics personnel to identify space availability. It also provides intelligence regarding the availability of security equipment available from units in country or host nations.

3. Coordination and planning continue once an operational site(s) has been identified. Determining, shaping, and finalizing physical security requirements begin immediately.

4. All security initiatives must be coordinated with the Marine Rear Area Operations Center (MRAOC), Antiterrorism Officer, Air Combat Elements (ACE), and Ground Combat Elements (GCE) on site.

11003. SITE SURVEY. A comprehensive site survey is the first step in determining physical security and force protection requirements. The survey is intended to identify, uncover, and isolate security deficiencies and vulnerabilities both inside and outside of the perimeter.

1. In order to support an integrated and comprehensive security plan the following information must be compiled prior to conducting the survey.

a. A complete and current threat assessment. This provides the basis for determining enemy, terrorist, and/or criminal activities that pose the greatest threat.

b. The commander's identification and prioritization of assets (personnel, equipment, facilities, etc.) essential to mission accomplishment.

c. An orientation map that includes locations, dimensions and descriptions of structures, roads, terrain and landscaping. The map must identify property perimeter boundaries and existing security features, including static posts, defensive positions, and unit positions.

d. A brief on existing security measures, procedures, and security equipment on hand and in use.

2. This information is critical to physical security personnel assessing the current security posture. Upon completion, results are provided to the commander. Results identify required actions and/or recommendations to establish or complement the security, force protection, and antiterrorism posture. Once approved, planned initiatives and modifications must be coordinated and conducted with the ATO, GCE, MP, and unit(s)/organization(s) representatives responsible for security. Coordination ensures proposed enhancements supplement in-place security and there is no duplication of effort.

3. Physical security personnel will annotate all equipment deployment on a map. This map is the source document for all equipment placement and will be maintained in the MRAOC. Physical security personnel will assist engineers in moving and staging security equipment to ensure the equipment is properly deployed.

4. Comprehensive protection is achieved through the use of manpower, equipment, procedures, and other security components and options. Perimeter sensors, lights, and closed circuit television can be used to detect vehicles attempting to covertly penetrate the perimeter, while MWDs and trace explosive detection equipment can be used to detect explosives hidden in vehicles entering a facility. A wide range of potential threats can be detected early using unobstructed clear zones and standoff distance.

11004. PROTECTIVE MEASURES. Protective measures are established through a process focused on an integrated systems approach. Development procedures are researched and addressed, and supporting elements are applied. The focus is intended to identify specific assets for well-defined threats.

1. Full systems integration is dependent on development procedures and supporting elements.

a. Development procedures incorporate:

- (1) Asset(s) to be protected.
- (2) Threat(s) to the assets.

- (3) Risk levels.
- (4) Additional vulnerabilities, based on the threat(s).
- (5) Regulatory requirements.
- (6) Asset protection levels against identified threats.
- (7) Available resources.

b. Supporting elements encompass:

- (1) Physical measures such as hardening, barriers, lighting, and electronic security systems.
- (2) Procedural measures hinge foremost on the commander's intent and guidance. Procedural measures include applicable DOD and Marine Corps regulatory guidance, general and special orders, standard operating procedures, guard orders (including singular post orders).
- (3) Terrorism counteraction measures including self-protection measures (personal protection equipment), self-protection training, and unique protective equipment (armor-plated vehicles) and mass notification systems.
- (4) Passive security measures such as camouflage, dispersion, natural cover, and dummy positions.

2. Protective measures can be divided into five elements, Site-work, building, detection, notification, and procedural.

a. Site-work elements include the area surrounding an asset, facility, FOB, FARP, or other expeditionary site. These elements are associated with exterior points and include landforms, standoff distances and barriers, both natural and man-made.

b. Building elements are directly associated with a facilities construction and includes the structure's present posture. Included are walls, doors, roof/ceiling, and windows.

c. Detection elements detect or assess intrusion. Detection elements include ESS, CCTV, metal detectors, and CBRNE detection equipment.

5 Jun 09

d. Notification elements signal personnel of an emergency situation(s) or may notify alert forces of attempted or actual penetration of an area(s). Notification elements include mass notification systems, electronic security systems and communications gear.

e. Procedural elements are DOD and Marine Corps orders and directives addressing physical security, force protection, and antiterrorism. Procedural elements also include Battalion Orders, Standard Operating Procedures, and Post Orders.

11005. SYSTEMS APPROACH. Physical security personnel utilize the results of the protective measures process to support design and deployment of security measures in a systems approach. The systems approach is intended to provide the three basic functions of a system design; detect, delay, and deny. Defense is organized in depth and contains mutually supporting elements and procedures that prevent gaps or overlaps in responsibilities and performance. The systems approach allows commanders to make informed decisions concerning personnel and equipment deployment tradeoffs. Where threats are frequent and the threat level increased, the ability to increase the guard force, vacate particularly vulnerable locations or buildings for a brief period, or change day-to-day operations may be far more effective than a high cost project.

1. The systems approach includes a number of security applications that will be addressed:

a. Personnel and vehicle access and control

(1) Entry Control Facility. Construct independent Marine and friendly forces ECFs with as large a degree of separation as possible from civilian ECFs to reduce/remove a number of threats including Vehicle Borne Improvised Explosive Devices (VBIED). Each ECF needs to be provided with a high-speed bypass to allow response forces an immediate, uncontested response to exterior points. The primary mission of a civilian vehicle ECF is contraband and explosives inspection. The ECF must be provided maximum standoff from the site perimeter, and will contain a substantial barrier pattern. Signage, in English, and the native language, is paramount to identify entry requirements, to include search, seizure and use of force. The site should also have a speaker system with the capability to project commands and instructions to a number of personnel in and around the ECF. ECFs must be constructed to support

inspection for contraband and explosive detection (to include MWDs and other equipment (as provided)) and identification, registration, and rejection/egress. The site should also have a means to project voice commands and instructions to all persons in and around the ECF. Each point must be provided with supporting over watch positions with a substantial defense capability of addressing weapons and VBIED threats. Final denial barriers must be included in design of every ECF.

(2) Access Control Point. Construct independent Marine and friendly forces ACPs with as large a degree of separation from civilian personnel ACPs as possible to reduce/remove a number of threats including suicide bombers. Identification controls, including technology assets, are recommended at ACPs to reduce manpower requirements, increase rapid process and movement of personnel, and lessen the vulnerability to Marines. The primary mission of a civilian ACP is contraband and explosive inspection. Civilian ACPs should be located close to civilian ECFs in order to provide a combined point that reduces threats, restricts movement and reduces operating forces manpower requirements associated with multiple locations. ACPs must be constructed to support identification, registration, and rejection/egress of personnel. The ACP should also have a means to project voice commands and instructions to all persons in and around the ACP. Each point must be provided with supporting over watch positions with a substantial defense capability of addressing personnel, vehicle, and weapons threats. ACPs must be constructed to support inspection for contraband and explosive detection (to include MWDs and other equipment (as provided)) and identification, registration, and rejection/egress.

(3) Circulation Control. Strict control of personnel and vehicle movement within a site (FARP, FOB, and fixed sites) is essential. Circulation control lessens vulnerabilities against personnel, critical assets, and facilities. Personal identification is required for all individuals approved for entry that are not Marines. Personal identification issued at perimeter ACPs is essential in order to establish a visible indicator of personnel authorized inside the perimeter fence line. ESS, electronic locks, and other technologies may be used to prohibit access and control circulation in and around facilities. Use of CCTV at some facilities may reduce manpower requirements, however, CCTV does not preclude constant surveillance requirements where directed by regulatory guidance. Fences, barriers, and signage are required to identify

restricted access areas and control movement in and around critical assets. Actual access to interior spaces can be further restricted through ESS technology (access control devices).

(4) Personal Identification Control. Positive identification of personnel authorized entry to FOBs, FARPs, EAFs, and other sites are essential. Personal identification for visitors must be addressed, processed and completed at the perimeter ECF/ACP. This includes identification control and specific area access control. Photo identification badges with biometrics capabilities and the CAC provide a greater level of security. Exchange badge systems and/or badges with magnetic stripes or barcodes that query a database provide a greater level of security for identification into spaces containing critical assets. Personal Identification Numbers (PINs) are an option that can be used with card systems.

b. Barriers and barrier systems. Included are natural barriers (rivers, streams, woods) and man-made (fixed, portable, active, and passive).

(1) Natural barriers. Does the barrier support an offensive or defensive position for the site? Does the barrier present a vulnerability to fixed positions by providing cover or concealment for aggressor personnel? Coordination with engineer personnel supports changing, shaping, and strengthening natural barriers.

(2) Man-made barriers. Fixed and portable barriers both active (requires some action), and passive (no moving parts) provide commanders options.

(a) Fixed barriers may be permanently installed, but included in this group are those barriers that require heavy equipment to move or dismantle. Fixed barriers are used to fortify vulnerable points, establish and maintain boundaries and stand-off, prohibit entry, and channel traffic. Fixed passive barriers generally require heavy equipment support, however, continued maintenance is generally not required. Passive barriers absorb greater energy and transmit the energy to the foundation.

(b) Portable barriers provide commanders a readily deployable asset that can be used to respond to emerging threats; however, portable barriers are likely to impose greater maintenance and heavy vehicle support requirements. Portable

5 Jun 09

barriers allow commanders an option for random deployment in force protection, safety, and access. Portable barriers generally require some action by personnel, equipment, or both, to permit ingress/egress.

(3) Considerations. There are a number of considerations that commanders must address prior to selecting barriers and barrier systems. Included are threat type(s), direction of the threat or attack, operating protocols, supporting infrastructure, operating conditions such as weather and environmental changes, maintenance support, and support equipment required to stage the barriers.

c. Access delay and denial systems. ECFs and ACPs provide initial perimeter access delay and denial points. Additional systems will generally be used at interior points in support of manpower requirements. Access control systems utilizing current badge reading technology may be used to activate locks, turnstiles, and barriers in support of access control. CCTV systems may be included as examples of access delay and denial systems, when arranged in such a way where an individual is recognized prior to allowing admittance. However, CCTV will include an additional physical access control device and will not be depended upon as a sole source of denial.

d. Notification Systems. Expeditionary ESS provides security force and response force personnel instant notification of actual or attempted intrusion into a protected area. MNS serve as a capability to provide real-time information to all building occupants, or personnel in the immediate vicinity of a building, during emergency situations. Commanders must address operating protocols, supporting infrastructure, operating conditions and maintenance support during the selection process.

e. Physical Security Aids. Physical security aids such as lighting, fencing, key and lock control, and current technologies (metal detectors, personal x-ray scanners, CBRNE detection equipment), contribute significantly in site physical security.

(1) Lighting requirements must be balanced. Lighting enhances force protection by discouraging unauthorized entry while permitting an enhanced visual assessment capability during darkness. However, lighting must not expose security personnel and posts, or draw attention to a critical area or asset. Visual assessment capability reduces the advantage of

concealment and surprise and facilitates increased detection of intruders. There are a number of portable lighting systems that provide flexibility in security requirements at ECFs and ACPs and other areas where permanent lighting is not practical or possible. Lighting may also be used in conjunction with detection equipment to support perimeter defense; however, security positions must remain in comparative darkness.

(2) Fencing serves to channel persons at ACPs, create buffer zones for critical areas, and preclude visual compromise by unauthorized persons. Fencing may be used in a number of situations; however, it should primarily be used a boundary indicator based on the fact that there are a limited number of fences that provide substantial protection and delay. Perimeter fencing should also be reinforced on the interior with barriers lines or random barrier patterns in an effort to support force protection efforts. Fencing is vulnerable to compromise, and when used, commanders must ensure that an inspection process is in place. When fencing a large area, vehicle and personnel entrances must be kept to the minimum required for safe and efficient operations. In some cases fencing may be used to serve as a screen to protect against and possibly defeat both hand thrown and stand off weapons.

(3) Locks, and lock and key control are fundamental element of security, widely used for protecting and security facilities, materials, and property. Rotation and maintenance of locks while maintaining strict key control lessens the vulnerability of compromise.

(4) Current technologies provide commanders options to detect and address threats with a long range and short-range capability. Vehicle and pedestrian traffic present an ever present, in-close CBRNE threat. Commanders are encouraged to support efforts to broaden force protection and physical security capabilities through the use of current technologies.

f. Communications Systems. A number of units and designated forces within a given site require primary and secondary communications. Perimeter defense and rapid response forces, interior guard personnel, and MP personnel require adequate communications systems to respond to threats and a number of support tasks. Communications requirements must be addressed as a part of pre-deployment planning with the communications platoon personnel in order to address secure, dedicated, and shared frequency requirements.

g. Security forces. All sites, especially fixed sites, require commanders to maintain of a number of personnel designated as security forces. Security forces include perimeter defense, rapid response forces, MP (to include mobile and foot patrols), and interior guard forces. Security force personnel must be aware of physical security applications including operation and maintenance requirements, as they may be required to perform sustainment operation and maintenance functions.

h. Emergency Power Sources. As noted in paragraph 11009, commanders have an indisputable interest in ensuring that critical infrastructure is protected. Protection of utilities (power, water, waste, oil & gas lines) ensures no, or little, interruption of resources required for continued operations. Physical security equipment (barriers, lighting, access control equipment and ESS) relies on electricity. Physical security personnel must address generator, uninterruptible power source, additional battery, and portable lighting system requirements during pre-deployment planning with logistics and engineer personnel.

11006. DEFENSE IN DEPTH. Defense in depth with echelon approaches provides a layered methodology, with overarching and complementing security measures.

1. First echelon measures involve security patrols outside of the perimeter as directed by the commander. The patrols conduct random and aggressive reconnaissance in an effort to detect enemy movement and positions, maintain open roadways, and discourage loitering in and around the perimeter. Patrols must be in constant communications with the MRAOC in order to call for mutual support and fire support missions as necessary. Expansive use of technologies such as deployable ESS, night vision devices, and electronic sensors serves to provide enhanced detection capabilities. These areas require coordinated, on-call fire support, and support from adjacent GCEs.

2. Second echelon defense focuses on the true identified perimeter of FOBs, FARPs, and established sites. Defense measures in these areas require the greatest amount of coordination with GCE and MP security personnel. Defense along the perimeter is aggressive and includes static and mobile patrols. Physical security efforts are directed towards consecutive barriers, obstacles, sensors and other devices that

detect, delay and support denying any attempt to penetrate the site perimeter.

3. Third echelon presents heightened physical security measures that provide a heavy barrier presence directly adjacent to critical assets. Barrier presence serves as a boundary and identifies access points. Measures focus on increased access control and security management of facilities and support equipment located directly inside and outside of the assets. Heavy technology use is encouraged in support of surveillance, detection and notification, and access control requirements. Physical security personnel must ensure engineer heavy equipment support is coordinated as requirements may dictate the need for movement and placement of barriers and other physical security and force protection equipment.

4. Fourth echelon allows commanders to maintain an interior defense that places security personnel in close proximity of the assets. This echelon provides for constant surveillance and protection of invaluable and critical assets such as hot aircraft, AA&E, and support equipment.

11007. EXPEDITIONARY AIRFIELD (EAF) SECURITY. Aircraft are most vulnerable in avenues while in flight routes on approach and take off. Air Base Ground Defense (ABGD) security plans must address aggressive random foot and mobile patrols by security force personnel in these areas to detect and prevent the threats to aircraft during takeoff and landing. Patrols will be suited for mobility and firepower in order to commit immediate maximum firepower to disrupt and destroy enemy operations. Defense in depth allows for maintaining a security presence adjacent to air assets while supporting strong defensive positions along the perimeter.

1. Operation tempo normally requires aircraft to be staged with a full complement of support equipment. Hot aircraft, fuel, ammunition, equipment, and supporting facilities and are prime enemy targets. Indirect fires present the greatest threat to these assets. Defensive measures must include a defense in depth that will defeat or delay enemy forces.

2. Defense in depth with echelon approaches provides a layered methodology, with overarching and complementing security measures. It allows for maintaining a security presence adjacent to air assets while supporting strong defensive positions along the perimeter.

11008. AA&E STORAGE SITE SECURITY. Paragraph 8004.3 provides additional guidance for Arms Storage facilities in an expeditionary/field environment. AA&E storage sites, along with EAFs, are one of the primary targets for infiltration and indirect and harassing fire. Security for AA&E must be weighed against accessibility, proximity to personnel and other critical assets, storage compatibility issues, and environmental concerns. Additionally, commanders must weigh the requirements for fixed storage structures against expeditionary mobile structures.

1. Facilities storing arms must be provided with a capability for securing weapons and major subassemblies in locked racks or containers. The requirement includes spare weapons and casualty weapons. Access control will be strictly enforced and limited to military personnel assigned duties within the facility that have been authorized in writing by the commander. Entry points and racks contained within the facility will be provided with locking devices. Racks and containers weighing less than 500 pounds will be chained together to prevent removal. In the absence of an ESS, the facility will be under constant surveillance by armed personnel. Exterior security concerns include a perimeter boundary that provides standoff, and includes a channeling access point. The boundary may consist of fencing, barriers, or concertina wire. Lighting should be used sparingly in an effort to not draw attention to the facility. Lighting should be provided, at a minimum, over the entry point of the facility. Restricted area signage is required.

2. Facilities storing ammunition and explosives will be protected against indirect fire. Commanders are encouraged to make full use of concealment for all ammunition and explosives sites. In-ground facilities are recommended and require coordination with engineer personnel to expedite placement and construction. Roofs and walls must be protected against small arms and high explosive rounds and fragment penetration that may lead to interior ammunition or explosives "cooking off". The use of pre-detonation screens is highly recommended. Access points will be located at a point that provides no line of sight to assets. Extensive use of barriers provides standoff and concertina wire should be used for the perimeter boundary. Concertina wire provides an additional layer of access control and must include an access point. Lighting should be used in accordance with the tactical situation in order to not draw attention to the facility. Lighting should be provided, at a minimum, over the entry point of the facility. Restricted area

and safety signage is required. In the absence of ESS, the facility will be guarded 24 hours a day by armed personnel.

11009. CRITICAL INFRASTRUCTURE PROTECTION. Commanders have an indisputable interest in ensuring that critical infrastructure is protected. It is imperative that commanders identify critical infrastructure and address security requirements without delay. Fresh water, fuel, power sources, and communications links are examples of critical infrastructure essential to sustain operational readiness for fixed and temporary sites. In an effort to lessen manpower requirements, maximum use of barriers, standoff (where available), sensors, and hardening materials are encouraged. Protection measures outlined in this chapter and throughout this Order may be applied to critical infrastructure facilities. Coordination with Host Nation personnel is necessary in order to identify any redundant facilities, which may present another issue. Redundancy is intensive and expensive, however, it may ensure no loss of service in the event a primary site(s) fall victim to an attack, terrorist activity, or act of sabotage. Another option may be establishing deceptive measures such as mock facilities.

11010. PORT AND WATERSIDE SECURITY. Operational Maneuver from the Sea (OMFTS) is monumental to the Marine Corps continued forward presence and war fighting capability. A crucial element of OMFTS is the capability to provide logistical support to components ashore. Naval, Maritime Pre-positioning Ship, and Military Sealift Command ship's cargoes are vital to the movement of personnel, vehicles, and aircraft. Critical cargoes are at great risk to sabotage, diversion, and/or theft during loading, transporting, and storing phases of port operations. Waterside, particularly port security in an expeditionary environment presents a tremendous challenge. Secure port facilities with a strong, sound, antiterrorism and physical security posture serve to ensure logistics are moving forward from the port to connecting Main Supply Routes (MSRs). An integral part of maritime pre-positioning force arrival and assembly operations, strict port operations and security measures must be established to offer protection of critical assets during ship loading and offloading. Supply corridors to and from the port may include inland waterways, railways, pipelines, and airfields. Additional port and waterside guidance is provided in paragraph 7005.

1. Generally, the HN or port authority identifies port security requirements. In cases where facilities are shared with allied

5 Jun 09

forces, their own forces must provide security. Host nations may request U.S. assistance for security. Once U.S. assistance is requested ensure that security personnel (PM/MP) conduct liaison with other agencies (HN police and military, port security, Coast Guard) to address areas of responsibility, support and additional requirements.

2. There are a number of waterborne threats (mines, swimmers, small boats with armed personnel, small boats laden with explosives) that must be addressed.

3. Aggressive land and sea patrols of the port and supply corridors are required to detect, report, and combat the threat. Additionally, ensure:

a. Rules of engagement for waterborne vessels are addressed and have been reviewed by the cognizant Staff Judge Advocate.

b. Land and waterborne access control requirements are addressed.

c. Restricted areas are identified.

d. Likely avenues of approach (land and waterborne) are provided constant surveillance and random patrols.

e. Barriers (land and waterborne) are emplaced.

f. MSR's and alternate routes are identified to and from the port area.

g. Static posts and roving patrols are established.

4. Enforcement Zones. Enforcement zones must be established to enforce waterside security and serve as an action position for security forces. Enforcement zones require coordination between naval forces, the Coast Guard, HN naval and shore personnel. Signage and constant communications in native language(s), and at times, in a host of languages, are required.

a. Security zones are established from the average high water mark to a point at the range of anticipated waterborne threats. In this zone, security forces make the first notification to uncleared vessels that they are entering restricted waters, stop and search vessels if necessary, and may use force, depending on rules of engagement.

b. Reaction zones range from the high water mark to a distance beyond the maximum range of anticipated waterborne threats. Security forces stop and board all un-cleared vessels using force to stop potential threats depending on rules of engagement.

c. Keep out zones are closest to critical vessels and assets and located from the asset to the maximum range of anticipated threats and weapons. Security forces will prevent entry of hostile craft or vessels into this zone and shore defenses will engage hostile vessels entering this zone.

5. Boundaries. Boundaries will be established in order to identify restricted access areas and can provide areas of operation for waterborne security patrols. Several devices can be used to establish boundaries:

- a. Buoys or floats
- b. Nets
- c. Anchored or pile mounted channel markers
- d. Signaling devices
- e. Log Booms
- f. Barges
- g. Workboats, whalers, and other small boats at anchor

6. Barriers. Water barriers establish boundaries, isolate activity, and can be used to restrict waterside access and impede passage. Floating nets of wire mesh anchored to the ocean floor can be used to deny access to a number of surface and submerged vehicles. Barges may be used to 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.

7. Surveillance/Intrusion Detection Systems. A variety of surveillance systems may be used for waterside security. During darkness, a reduction in surface activity occurs. As a

5 Jun 09

result, nighttime surveillance of waterside activity must rely on active measures such as radar in locating, and partially identifying potential problems. Commanders are encouraged to provide security personnel with night vision capabilities.

8. Lighting. In an expeditionary environment, security lighting may not be available, or may be subject to loss of power. Commanders are encouraged to assess lighting requirements and provide additional security lighting as necessary. Lighting should be used in order to not draw attention to a specific area(s) and as tactical situations may dictate. Commanders are encouraged to utilize controlled and standby lighting as addressed in paragraph 3011.

9. Inspections. Pier inspections will be conducted on a random, continuous basis. 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 Units, if available, may be used for this mission. While a ship is in port, landside personnel and Coast Guard waterside patrols will inspect the pier area and ship's hull randomly. Other at risk structures such as navigation aids, bridges, utility cable towers, tunnels, etc. will also be inspected on a random basis. Pier inspection and security requirements should be coordinated with Coast Guard and NCIS personnel when available to assist.

11011. PHYSICAL SECURITY PLAN. The physical security plan in Appendix D will be utilized in support of operating forces and is to be included in the Force Antiterrorism Plan.

11012. PHYSICAL SECURITY SURVEYS. Physical security personnel provide the commander continuous assessments of facilities to ensure regulatory instructions are being utilized and followed. They also identify violations of and vulnerabilities to threats. In an effort to maintain a strong secure physical security posture, commanders will ensure surveys are conducted on:

- a. Arms, ammunition and explosive storage sites
- b. Expeditionary airfields including flight lines, and other aviation assets in support of the ACE
- c. Piers, wharfs, port facilities, preposition and waterfront areas used in logistics support

- d. Petroleum, oil, and lubricant facilities
- e. Command, control, communications, and computer facilities
- f. Entry control facilities and access control points
- g. Critical infrastructure
- h. Motor pools

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX A

DEFINITIONS

For the purpose of this manual, the following definitions apply:

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.

Airborne Contamination. Contamination of a facility air system by introducing chemical, biological, or radiological agents into the Heating Ventilation Air Conditioning (HVAC) system.

Ammunition. An end item, complete round, or materiel component charged with explosives, propellants, pyrotechnics, or initiating composition for use in connection with defense or offense (including demolitions) as well as ammunition used for training, ceremonial, or non-operational purposes. This includes inert devices that replicate live ammunition, commonly referred to as dummy ammo, which contain no explosive materials.

Antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

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 references (s) and (t) and qualified with the firearm in accordance with reference (u).

Arms. A weapon which will, or is designated to, expel a projectile or flame by the action of an explosive, in the frame or receiver or metal parts of any such weapon from which a complete weapon could be constructed.

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.

5 Jun 09

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.

Classified Material Storage Area. An approved security container, vault, modular vault, or secure room used to store and safeguard classified information and items not in the personal control of authorized personnel.

Code "Q" Items. Drugs or other controlled substances designated as Schedule III, IV or V items, per 21 Code of Federal Regulations, Part 1308.

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.

Command Driven CCTV. A CCTV system that presents the MCESS operator with a view of an area when the operator calls up a specific camera.

Commanding Officer. The term commanding officer used throughout this Order refers to those officers assigned charge of an installation, battalion/squadron, or company.

COMSEC Equipment. Equipment designed to provide security to telecommunications by encrypting data for transmission and decrypting data for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process.

COMSEC Facility. Space employed primarily for the purpose of generating, storing, repairing, or using COMSEC material.

COMSEC Material. Material used to protect U.S. Government transmissions, communications, and the processing of classified or sensitive unclassified information related to national security from unauthorized persons and that material used to ensure the authenticity of such communications. (NOTE: COMSEC material includes, but is not limited to, key, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.)

Communication Security (COMSEC). Protective measures taken to

deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications. (NOTE: COMSEC includes crypto-security, emission security, transmission security, and physical security of COMSEC material and COMSEC information.)

Constant Surveillance. Maintaining continuous visibility of an item(s) or area, or of all means of access to the item(s) or area, directly by personnel. To accomplish constant surveillance indirectly through use of Closed Circuit Television (CCTV), an intrusion detection system (i.e. video motion detection, intelligent video, video tracking, etc.) will be used in coordination with event driven technology.

Controlled Cryptographic Items (CCI). CCI material is unclassified, accountable in the communications security (COMSEC) material system, and is authorized to move through the supply system.

Corrective Measures. Actions taken to rectify deficiencies in a command security posture.

Counter-terrorism. Offensive measures taken to prevent, deter, and respond to terrorism.

Covert Entry. Entry into a facility using stealth or false credentials.

Crime. An act or an omission, defined in law, and made punishable by constituted authority through a judicial proceeding for the protection of society.

Crime Analysis. A set of systematic, analytical processes directed at providing timely and pertinent information relative to crime patterns and trend correlations to assist the operational and administrative personnel in planning the deployment of resources for the prevention and suppression of criminal activities, aiding the investigative process, and increasing apprehensions and the clearance of cases.

Crime Control. The detection and investigation of crimes and offenses, and the apprehension and prosecution of offenders.

Crime Prevention. The application of measures necessary to minimize or eliminate the opportunity or desire to commit or

engage in criminal activities.

Crime Prevention Program. A program for planning, coordinating, executing and reviewing courses of action designed to prevent crimes and offenses.

Critical. Those facility or infrastructures that have been designated as crucial to mission accomplishment and essential to the continuity of installation operations.

DEMILITARIZATION. The act of destroying the military offensive or defensive advantages inherent in certain types of equipment or material. The term comprehends mutilation, dumping at sea, cutting, crushing, scrapping, melting, burning, or alteration designed to prevent the further use of this equipment and material for its originally intended military or lethal purpose and applies equally to material in unserviceable or serviceable condition, that has been screened through the Inventory Control Point (ICP) and declared surplus or foreign excess.

Egress. A 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.

Espionage. Acts directed toward the acquisition of information through clandestine operations.

Event Driven CCTV. A CCTV system used in conjunction with an IDS that presents the MCESS operator with an immediate view of the alarmed area once the sensor is tripped.

Exception. A written, approved long-term (36 months or longer) deviation from a specific provision of this manual.

Explosives. A chemical compound mixture or device, the primary or common purpose of which is to function by explosion. The term includes, but is not limited to, individual landmines, demolition charges, and blocks of explosives (dynamite, TNT, C-4, and other high explosives).

Exterior Attack. An attack against a facility, asset, or position, at close range.

First Echelon Maintenance. As it applies to the Marine Corps Electronic Security System, first echelon maintenance applies to Physical Security personnel who have completed MCESS

5 Jun 09

Administrator Training. First echelon maintenance includes troubleshooting, minor system software configuration changes, and limited replacement of hardware components.

Forced Entry. Unauthorized entry into a facility using hand, power, or thermal tools to create a man passable opening for the purpose of gaining access to contents within.

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.

High-Risk Billet. Authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary, or symbolic value may make Personnel filling them an especially attractive or accessible terrorist target.

High-Risk Personnel. U.S. personnel and their family members whose assignment or symbolic value may make them especially attractive or accessible terrorists target.

High-Risk Target. U.S. material resources and facilities, because of mission sensitivity, ease of access, isolation, and symbolic value, may be an especially attractive accessible terrorist targets.

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.

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 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.

Insider Compromise. Persons authorized access, compromise, or attempt to compromise, a facility or asset by taking advantage of their access.

Loss Analysis. Actions taken to compile facts, develop loss trends and patterns and other data manipulation concerning gains, losses, and theft of government property.

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.

Lost item. Item(s) that cannot be accounted for.

Mail-bomb delivery. Bombs or incendiary devices placed in letters, packages, or parcels and delivered through the mail by the postal system.

Missing. Item(s) that are not in their proper place and cannot readily be accounted for.

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.

Negotiable Instruments. A transferable, signed document that promises to pay the bearer a sum of money at a future date or on demand. Examples include checks, bills, bills of exchange and promissory notes.

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.

Physical Security Program. Part of the overall security posture at an activity including policy and resources 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.

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 an annual physical security survey. Commanding officers will establish local physical security inspection programs for their subordinate commands.

Physical Security Survey. A specific on-site examination of a facility, area, or activity conducted by a trained physical security specialist (MOS 5814), or civilian equivalent) to identify security weaknesses and recommend corrective measures.

Pilferage. Continuing theft of small quantities or amounts of property that is often difficult to detect.

Precious Metals. Refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium in bar, ingot, granule, liquid, sponge, or wire form.

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.

Recovered. An item of material that is found, gained by inventory, or recovered after previously being reported as missing, lost, or stolen.

Responsible Officer. That person or commander, having custodial or signature accountability for government property.

Sabotage. An act or acts with intent to injure, interfere with, or obstruct 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.

Security Violations. Any breach of security regulations, requirements, procedures or guidelines, whether or not a compromise results.

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.

Sensitive Government Property. Arms, ammunition, explosives, precious metals, MARES reportable items, or classified equipment/repair parts.

Serialized Government Property. Any item of government property which has an individual serial number affixed by the manufacturer or assigned for control purposes by an inventory control point of an item manager.

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.

Standoff Weapons. Military weapons or improvised military weapons that can be fired against a facility, asset, or position from long range.

Stolen. An item that is either missing or lost under circumstances indicating the possibility of criminal activity.

Suicide Bombers. A terrorist who blows himself up in order to kill or injure other people.

Supply bomb delivery. Bombs or incendiary devices concealed in various containers and delivered to supply and material handling points.

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.

Two-Man Rule. Requirement for two authorized individuals to be present while performing duties that require one individual to perform a task, and the other individual to assist, provide security, or insure the integrity of the process.

Unnecessary Risk. Any risk that, if taken, will not contribute meaningfully to mission accomplishment or will needlessly endanger lives or resources.

Value. The measurement of government property in monetary or material worth.

Vehicle Born Improvised Explosive Device (VBIED). A bomb fabricated in an improvised manner, placed in a car or other vehicle and then exploded. VBIEDs are commonly used as a weapon of assassination, terrorism, or guerrilla warfare, to kill the occupant(s) of the vehicle and people near the blast site and/or to cause damage to buildings or other property.

Visual Surveillance. Using ocular and photographic devices (binoculars, cameras) to monitor operations in or around facilities, assets, or positions.

Waiver. A written temporary relief, normally for a period of one year, from specific standards.

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.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX B

ACRONYMS

For the purpose of this manual, the following acronyms apply:

| | |
|-------|---|
| A&E | Ammunition and Explosives |
| AA&E | Arms, Ammunition, and Explosives |
| AACS | Automated Access Control System |
| AAV | Amphibious Assault vehicle |
| ABGD | Air Base Ground Defense |
| ACE | Air Combat Elements |
| ACP | Access Control Point |
| AFDCB | Armed Forces Disciplinary Control Board |
| AIB | Anti-Intrusion Barrier |
| AIRS | Automated Inspection Reporting System |
| AOR | Area of Responsibility |
| ARMD | Administration and Resource Management Division |
| ARS | Security Programs and Information Management Branch |
| ASL | Aviation Supply and Logistics |
| ASP | Ammunition Supply Point |
| AT | Antiterrorism |
| ATO | Antiterrorism Officer |
| ATWG | Antiterrorism Working Group |
| BATF | Bureau of Alcohol, Tobacco, and Firearms |
| BEQ | Bachelor Enlisted Quarters |

| | |
|-----------|--|
| BOQ | Bachelor Officer Quarters |
| BMS | Balanced Magnetic Switch |
| BTR | Basic Training Record |
| C4 | Command, Control, Communications, and Computers |
| C&E | Contact and Escort |
| CAC | Common Access Card |
| CAD | Cartridge Actuated Device |
| CAP | Corrective Action Plan |
| CBRNE | Chemical Biological Radiological Nuclear (high yield) Explosives |
| CCI | Controlled Cryptographic Items |
| CCN | Case Control Number |
| CCTV | Closed Circuit Television |
| CID | Commercial Item Description |
| CID | Criminal Investigative Division |
| CIP | Critical Infrastructure Protection |
| CIS | Constant Surveillance and Custody Service |
| CL | Carload |
| CMC | Commandant of the Marine Corps |
| CMR | Consolidated Memorandum Receipt |
| CO | Commanding Officer |
| COG | Corporal of the Guard |
| COMMARFOR | Commander Marine Forces |
| COMSEC | Communication Security |

| | |
|-------|---|
| CONUS | Continental United States |
| COTS | Commercial Off The Shelf |
| CPU | Central Processing Unit |
| CRT | Cathode-Ray Tube |
| DBIDS | Defense Biometric Identification System |
| DC | Deputy Commandant |
| DCI | Director, Central Intelligence |
| DDA | Designated Disposition Authority |
| DEA | Drug Enforcement Administration |
| DEERS | Defense Enrollment Eligibility Reporting System |
| DEMIL | Demilitarization |
| DIDS | Defense Integrated Data System |
| DLA | Defense Logistics Agency |
| DMCS | Director, Marine Corps Staff |
| DMDC | Defense Manpower Data Center |
| DOD | Department of Defense |
| DRMO | Defense Reutilization Marketing Office |
| DTR | Defense Transportation Regulations |
| DVR | Digital Video Recorder |
| DTTS | Defense Transportation Tracking System |
| EAF | Expeditionary Air Field |
| ECF | Entry Control Facility |
| EOC | Emergency Operations Center |

| | |
|---------|--|
| EOD | Explosive Ordnance Disposal |
| ERO | Equipment Repair Order |
| ESI | Explosive Safety Inspection |
| ESQD | Explosive Safety Quantity Distance |
| ESS | Electronic Security System |
| ESSA | Explosive Safety Self Audit |
| ESSIMS | Electronic Security System Information Management System |
| FAR | Federal Acquisition Regulations |
| FARP | Forward Arming and Refueling Point |
| FEDSPEC | Federal Specification |
| FIPS | Federal Information Processing Standards |
| FLETC | Federal Law Enforcement Training Center |
| FLIR | Forward Looking Infrared |
| FLS | Flight Line Security |
| FMS | Foreign Military Sales |
| FOB | Forward Operating Base |
| FOIA | Freedom Of Information Act |
| FOUO | For Official Use Only |
| FOV | Field Of View |
| FP | Force Protection |
| FPCON | Force Protection Condition |
| FSRM | Facility Sustainment, Repair, and Modernization |
| GCE | Ground Combat Element |

| | |
|--------------|--|
| GOV | Government Owned Vehicle |
| GPS | Global Positioning System |
| GS | Government Service |
| GSA | General Service Administration |
| HD | Historical Division |
| HERO | Hazards of Electro-magnetic Radiation to Ordnance |
| HN | Host Nation |
| HQMC | Headquarters, Marine Corps |
| I&L | Installations & Logistics |
| ID | Identification |
| IDP | Installation Design Plan |
| IDS | Intrusion Detection System |
| IGMC | Inspector General Marine Corps |
| ILD | Internal Locking Device |
| ISMT | Indoor Simulated Marksmanship Trainer |
| ISSA | Inter Service Support Agreement |
| JROTC | Junior Reserve Officers Training Corps |
| LAN | Local Area Network |
| LCD | Liquid-Crystal Display |
| LEPSAR | Law Enforcement and Physical Security Activities Report |
| LFF | Facilities and Service Division |
| LPC | Logistics, Plans, and Capabilities |
| MARCORLOGCOM | Marine Corps Logistics Command |

| | |
|--------------|--|
| MARCORSYSCOM | Marine Corps Systems Command |
| MARFOR | Marine Forces |
| MARFORRES | Marine Forces Reserve |
| MAW | Marine Air Wing |
| MCAF | Marine Corps Air Facility |
| MCAS | Marine Corps Air Station |
| MCCLEP | Marine Corps Civilian Law Enforcement Program |
| MCCS | Marine Corps Community Services |
| MCESS | Marine Corps Electronic Security System |
| MCGERR | Marine Corps Ground Equipment Resource Reporting |
| MCI | Marine Corps Installations |
| MCIA | Marine Corps Intelligence Activity |
| MCPD | Marine Corps Police Department |
| MCX | Marine Corps Exchange |
| MHE | Materials Handling Equipment |
| MILCON | Military Construction |
| MIL-DTL | Military Detail |
| MIL SPEC | Military Specification |
| MLSR | Missing, Lost, Stolen, and Recovered |
| MMEA | Marine Monitor Enlisted Assignments |
| MMOA | Marine Monitor Officer Assignments |
| MNS | Mass Notification System |
| MOA | Memorandum of Agreement |

| | |
|--------------|--|
| MOOTW | Military Operations Other Than War |
| MOS | Military Occupational Specialty |
| MOU | Memorandum Of Understanding |
| MP | Military Police |
| MPS | Military Preposition Ships |
| MRAOC | Marine Rear Area Operations Center |
| MSC | Military Sealift Command |
| MSR | Main Supply Routes |
| MTMC | Military Traffic Management Command |
| MWD | Military Working Dog |
| NACIC | National Agency Check with Written Inquiries and Credit |
| NACLC | National Agency Check, Local Agency Check, Credit Check |
| NATO | North Atlantic Treaty Organization |
| NAVFACENGCOM | Naval Facility Engineering Command |
| NAVMC | Navy and Marine Corps |
| NBC | Nuclear, Biological, and Chemical |
| NCIC | National Crime Information Center |
| NCIS | Naval Criminal Investigative Service |
| NDA | National Defense Area |
| NIST | National Institute of Standards and Technology |
| NSN | National Stock Number |
| NSWC | Naval Surface Warfare Center |

OCONUS Outside the Continental United States

OCSLA Outer Continental Shelf Lands Act

OIC Officer In Charge

OMFTS Operational Maneuver From The Sea

OOD Officer of the Day

OQR Officer Qualification Record

P&R Programs and Resources

PAO Public Affairs Office

PIN Personal Identification Number

PIP Personnel Identity Program

PM Provost Marshal

PMO Provost Marshal's Office

POA&M Plan Of Action and Milestones

POL Petroleum, Oil, Lubricants

POM Program Objective Memorandum

POV Privately Owned Vehicle

PP&O Plans, Policies, and Operations

PS PP&O, Security Division

PSC Physical Security Council

PSP Physical Security Professional

PSUP Physical Security Upgrade Projects

PSWG Physical Security Working Group

PTZ Pan-Tilt-Zoom

| | |
|-----------|--|
| PWSA | Ports and Waterfront Safety Act |
| QARS | Quarterly Automated Reporting System |
| QUAL-CERT | Qualification and Certification |
| RAM | Random Antiterrorism Measure |
| RDT&E | Research, Development, Test and Evaluation |
| RFI | Ready For Issue |
| ROICC | Resident Office in Charge of Construction |
| ROE | Rules of Engagement |
| ROTC | Reserve Officers Training Corps |
| RSL | Ready Service Lockers |
| RSO | Range Safety Officer |
| RTU | Remote Terminal Unit |
| RUF | Rules for Use of Force |
| SACO | Substance Abuse Control Officer |
| SCIF | Sensitive Compartmented Information Facility |
| SDNCO | Staff Duty Noncommissioned Officer |
| SESAMS | Special Effects Small Arms Marking Systems |
| SEV | Security Escort Vehicle |
| SEWG | Security Engineering Working Group |
| SJA | Staff Judge Advocate |
| SNS | Satellite Motor Surveillance |
| SNCO | Staff Noncommissioned Officer |
| SOFA | Status of Forces Agreement |

| | |
|-------|---|
| SOG | Sergeant of the Guard |
| SOP | Standard Operating Procedures |
| SRB | Service Record Book |
| SRT | Special Reaction Team |
| T/E | Table of Equipment |
| TL | Truckload |
| TRB | Tactical Response Boat |
| TSA | Technical Support Agency |
| UCMJ | Uniformed Code of Military Justice |
| UII | Unique Item Identifier |
| UL | Underwriters Laboratory |
| UPS | Uninterrupted Power Source |
| USACE | U.S. Army Corps of Engineers |
| U.S. | United States |
| USS | Universal Security System |
| USCG | U.S. Coast Guard |
| USPS | U.S. Postal Service |
| VBIED | Vehicle Borne Improvised Explosive Device |
| VIP | Very Important Person |
| WMD | Weapons of Mass Destruction |
| WSN | Weapon Serial Number |
| WTBN | Weapons Training Battalion |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX C

WAIVER AND EXCEPTION REQUEST 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)

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 that cite standards that 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 facility 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.

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 facility 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, and DSN and commercial phone numbers.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX D

CLASSIFICATION

PHYSICAL SECURITY PLAN (FORMAT)

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

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.

(b) Search and inspection of material for possible sabotage/terrorist hazards.

CLASSIFICATION

****CLASSIFICATION****

(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.

(a) Stationary

1. Type.

2. Current placement.

3. Maintenance requirements.

****CLASSIFICATION****

CLASSIFICATION

(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

- (1) Placement.
- (2) Maintenance.
- (3) Power failure contingency plan.
- (4) Uninterrupted Power Sources.
- (5) Emergency Lighting systems.

(a) Stationary.

(b) Mobile.

1. Staging Area.
2. Maintenance requirements.
3. Deployment schedule.

a. Support requirements for deployment.

c. Electronic Security Systems

- (1) Alarm Control Center.
- (2) Use and monitoring.

CLASSIFICATION

****CLASSIFICATION****

- (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.)
- e. Equipment.
 - (1) Weapons.
 - (a) Training.
 - (b) Qualification requirements.
 - (2) Vehicles.
 - (3) Support Equipment (hand irons, flashlight.)

****CLASSIFICATION****

CLASSIFICATION

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

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX E

WARNING

PHYSICAL SECURITY
SURVEY



PHYSICAL SECURITY
SURVEY

**The Attached Document is a Report From the
Physical Security Office**

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 herein is not released to unauthorized persons. Requests for access to or disclosure of the attached document(s) must be referred to the Provost Marshal/Chief of Police.

Date : _____

Survey Control No. : _____

From :

To :

1. This Document is Furnished for Your Information And/Or Action as Deemed Appropriate.
2. When This Document is No Longer Needed it Should Be Destroyed by Burning or Shredding.

FOR OFFICIAL USE ONLY

IF CLASSIFIED - SECNAVINST 5510.36 APPLIES

NAVMC 11121 (Rev. 02-09) (EF)

**United States Marine Corps Physical Security/Crime Prevention Survey (1600)
NAVMC 11121 (Rev. 02-09) (EF)**

Print Form

| |
|--------|
| Date |
| |
| Status |
| |

| | |
|------------------------------------|---|
| Survey Control Number | Type of Survey |
| | |
| Inspecting Unit | Requesting Unit |
| | |
| Organization | |
| | |
| Address of Unit Inspected/Surveyed | Distribution |
| | |
| Comments | |
| | |
| | |
| | |
| | |
| Signature of Inspector | Signature of Approving Officer |
| | |
| Typed Name and Grade of Inspector | Typed Name and Grade of Approving Officer |
| | |

Reset Form

Adobe Designer 8.0

BUILDING AND AREA

PHYSICAL SECURITY BARRIERS

1. Walls -

Requirement -

Recommendations -

2. Doors -

Requirement -

Recommendations -

3. Floors -

Requirement -

Recommendations -

4. Ceiling/Roof -

Requirement -

Recommendations -

5. Windows/Other Openings -

Requirement -

Recommendations -

6. Natural -

Requirement -

Recommendations -

PAGE 2 OF 4

FOR OFFICIAL USE ONLY

PHYSICAL SECURITY AIDS, EQUIPMENT, AND DEVICES

1. Lighting (Exterior/Interior) -

Requirement -

Recommendations -

2. Fencing -

Requirement -

Recommendations -

3. Locks -

Requirement -

Recommendations -

4. Vaults/Safes/Containers -

Requirement -

Recommendations -

5. Electronic Security System (ESS) -

Requirement -

Recommendations -

6. Key and Lock Control -

Requirement -

Recommendations -

7. Security Force -

Requirement -

Recommendations -

PREVENTIVE MEASURES AND PROCEDURES

1. Security Orders/SOP -

Requirement -

Recommendations -

2. Access Control -

Requirement -

Recommendations -

3. Property Accountability -

Requirement -

Recommendations -

4. Robbery/Burglary Procedures -

Requirement -

Recommendations -

5. Crime/Loss Prevention Awareness Training -

Requirement -

Recommendations -

ACTION/COMMENT

PAGE 4 OF 4

FOR OFFICIAL USE ONLY

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX F

INSTRUCTIONS FOR PREPARATION, COMPLETION, AND
DISTRIBUTION OF A 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 in Appendix E. 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 will 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.)

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 () and (), 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 to 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 - Typed Name and Grade of Inspector. Name of individual who conducted the survey will be entered as first and middle initials, last name and grade. (e.g., G.E. Davis, Sgt.)

Block 13 - Typed Name and Grade of Approving Officer. Name of officer approving the survey will be entered as first and middle initials, last name and grade; e.g., I.R. Grow, GySgt.

Block 14 - 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 (5) Assault, etc.)

Block 15 - Building and Area. Identify the building by number and type of construction (stories and type of material) and location (describe surrounding area, industrial, business, 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.)

5 Jun 09

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)).

Block 16 - Physical Security Equipment. These items provide protection in relationship to the sensitivity of the property being protected. Address each category separately.

1. Fencing - Describe type, type of construction, 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.)
 - 1-a. Vehicle/Personnel Gates - 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 with four personnel and one vehicle gate.)
 - 1-b. Clear Zones - Describe number, distance, and location of, and any deficiencies. (Example: There is a fence surrounding the facility. There are 30 feet interior and 20 feet exterior

clear zones around the entire facility.)

2. Barriers (natural/man-made) - Describe type, number, location, and any deficiencies. (Example: There are no man-made or natural barriers that affect this facility.)

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. Racks/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. Lighting

5-a. Interior Lighting - 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.)

5-b. Exterior Lighting - 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.)

6. Electronic Security System (ESS) - Describe type, where the system annunciates, and any deficiencies. (Example: There is a Marine Corps Electronic Security System, which annunciates at the Provost Marshal Office, which is staffed on a 24-hour basis.)

6-a. Intrusion Detection System (IDS) - Describe type of sensors and any deficiencies. (Example: There are balanced magnetic switches and passive infrared motion detectors. There is also a duress switch utilized in the facility.)

6-b. Closed Circuit Television (CCTV) - Describe type, locations, views, and any deficiencies. (Example: There is CCTV located atop the facility, which is used to provide surveillance of areas of the flight line in alarm.)

6-c. Automated Access Control System (AACS) - Describe type, location of readers, where the badging system is located, and any deficiencies. (Example: There is magstripe reader located at the entrance of the facility that uses the Common Access Card as the access token.)

6-d. Mass Notification System (MNS) - Describe type, interior components, where the system annunciates, and any deficiencies. (Example: There is a mass notification system installed within this facility. There are wireless speakers located on all floors, which are activated from the base wide system located at the installation PMO.)

Block 17 - Preventive Measures and Procedures. Address each category separately and provide recommendations accordingly.

1. 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 ().

2. Security Orders and Plans. 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).

3. Security Training. Identify training provided by the command or by the Provost Marshal's 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.)

4. 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).

5. 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.)

Block 18 - 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.

3. IDENTIFIED DEFICIENCY REQUIREMENTS. For all deficiencies identified in a survey category, the requirement and the applicable reference will be listed. (Example: Requirement - The intrusion detection system has no emergency backup power. Reference (), paragraph 9999 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.)

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 in Appendix E, page E-1.

6. SURVEY FORMAT. The survey format may not be modified, with the exception of the Discrepancy/Reference Tables. If a survey discussion point (e.g. 6-d. Mass Notification Systems (MNS)) is determined to be completely compliant with requirements and no

MCO 5530.14A

5 Jun 09

discrepancies are identified, then the Discrepancy/References Table can be deleted. In the above example, a description of the mass notification system is still required. In cases where a mass notification system does not exist, the discussion point would simply be marked with N/A.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX G

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

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX H

SECURITY RISK CATEGORIES

1. GENERAL. This appendix lists specific AA&E items in Security Risk Categories I through IV and provides a Decision Logic 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) anti-armor 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

a. Category II. Light automatic weapons, MK-19 (other 40mm high velocity), multi-shot grenade launchers (MSGL), M-2, M107 (other .50 Caliber), M240 series machineguns (other 7.62mm machineguns), M249, Infantry Automatic Rifle (IAR), M16 and M4 Series rifles (other 5.56mm (semi) automatic rifles). Foreign

weapons that fall within the categories listed above.

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

- (1) Hand or rifle grenades – high explosive and white phosphorus.

5 Jun 09

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

(3) Explosives used in demolition operations, 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

(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).

d. 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 the numbers to determine the appropriate security risk category using the rankings below.

| 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 |

d. 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. |

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 Materials Handling Equipment (MHE). |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX I
AA&E SCREENING PACKAGE
FOR OFFICIAL USE ONLY

NAVMC 11386 (04-00) (EF)
FOUO - Privacy Sensitive when filled in.

**PERSONNEL SCREENING FORM
FOR ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)
(REV DTD 29 JAN 00)**

Screening (check one): INITIAL ANNUAL

Ref: (a) MCO 5530.14____
(b) MCO P440.150____

| | | | |
|---------------------------|-------------|----------|--|
| Individual Being Screened | | | |
| Rank : | Name : | | |
| SSN : | MOS : | Billet : | |
| Date of screening : | Signature : | | |

| | | | |
|---------------------------------|-------------|----------|--|
| Individual Conducting Screening | | | |
| Rank : | Name : | | |
| SSN : | MOS : | Billet : | |
| Date of screening : | Signature : | | |

| SUBJECT | YES | NO | N/A | REMARKS |
|--|-----|----|-----|---------|
| Individual's medical record has been screened by a competent medical authority. There are no medical conditions that would prevent this individual from handling AA&E. | | | | |
| Individual's service record book or officer qualification record has been screened. There is no derogatory information that would prohibit this individual from handling AA&E. | | | | |
| Individual has no pending legal action and/or convictions by court-martial, civilian courts, or non-judicial punishment that would prohibit this individual from handling AA&E. | | | | |
| Individual demonstrates the requisite maturity, judgment, and leadership required to handle AA&E. | | | | |
| Has the Individual had a National Agency Check (NAC) or Entrance National Agency Check (ENTNAC) completed and is the result posted in the MMS system? | | | | |
| Has the Individual qualified with the required security weapon within the last 12 months? | | | | |
| Has the Individual 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 individual (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. Individual 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 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.

FOR OFFICIAL USE ONLY.

Adobe Designer 8.0

FOR OFFICIAL USE ONLY

MCO 5530.14A
5 Jun 09



FOR OFFICIAL USE ONLY
UNITED STATES MARINE CORPS
UNIT HEADING

IN REPLY REFER TO:
5530
Ord
Date

From: Arms, Ammunition, and Explosives (AA&E) Officer
To: Medical Officer

Subj: MEDICAL SCREENING FOR AA&E DUTIES ICO LCPL JOE B. MARINE XXX
XX 6789/21XX

Ref: MCO 5530.14_

1. Please screen the above individual's health record for assignment to Arms, Ammunition, and Explosives (AA&E) duty. A positive response to any of the questions listed below may disqualify the individual from assignment to working with AA&E in the performance of his/her duties.

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/her mental capacity?

YES _____ NO _____

2. The above Marine's Medical Record Book has been reviewed.

MEDICAL OFFICER SIGNATURE AND DATE

FOR OFFICIAL USE ONLY

MCO 5530.14A
5 Jun 09



FOR OFFICIAL USE ONLY

UNITED STATES MARINE CORPS

UNIT HEADING

IN REPLY REFER TO:
5530
Ord
Date

From: Commanding Officer
To: AA&E Officer

Subj: MONTHLY ADJUDICATION INQUIRY, C/O LCPL I. M. MARINE
XXX XX 6789/21XX

Ref: MCO 5530.14

1. Per the reference the status of LCpl _____ NACLIC has been verified, through JPAS. This Marine will continue to perform assigned duties while awaiting adjudication of the investigation. All other screening requirements have been completed and filed accordingly.
2. LCpl _____ investigation was submitted to DONCAF on DATE, and his/her interim clearance date began: DATE.
3. The point of contact regarding this matter is (list name of person with JPAS account/verification ability).

I. M. INCHARGE

FOR OFFICIAL USE ONLY

MCO 5530.14A
5 Jun 09



FOR OFFICIAL USE ONLY

UNITED STATES MARINE CORPS
UNIT HEADING

IN REPLY REFER TO:
8000
ORD
Date

From: Arms, Ammunition, and Explosives Officer
To: Personnel Officer

Subj: **UNIT DIARY ENTRIES FOR AA&E SCREENING**

Ref: (a) MCO P4400.150_
(b) MCO 5530.14_

1. Per the references, the below listed personnel have been screened and found qualified for duties involving Arms, Ammunition, and Explosives:

| <u>NAME</u> | <u>RANK</u> | <u>SSN</u> |
|-----------------|-------------|-------------|
| Incharge, I Am, | SSgt | 123 45 6789 |
| Marine, I Am, | LCpl | 987 65 4321 |

2. It is requested that the individuals listed above have a Type Transaction Code (TTC) 483, Arms AA&E screen entered into the Marine Corps Total Force System (MCTFS). Provide a copy of the certified unit diary printout to the Arms, Ammunition, and Explosives Officer.

3. Point of contact for this matter is AA&E Officer at XXX-XXXX.

A. A. ANDY

FOR OFFICIAL USE ONLY

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX J

AA&E FACILITY MINIMUM CONSTRUCTION REQUIREMENTS

TABLE 1 - MINIMUM CONSTRUCTION REQUIREMENTS
FOR RISK CATEGORIES I THROUGH IV

| MINIMUM CONSTRUCTION REQUIREMENT | | MINIMUM PENETRATION TIME (MINUTES) | | | |
|----------------------------------|---|---------------------------------------|-----|-------|-----------|
| | | LOW | MED | HIGH | VERY HIGH |
| WALLS | 8-inch (200 mm) concrete reinforced with No.4 (12.7 mm) reinforcing bars, 9 inches (225 mm) on center, in each direction and staggered on each face to form a grid approximately 4-1/2 inches (114 mm) square or | (a) | (a) | 15 | <1 |
| | 8-inch (200 mm) concrete block (or concrete masonry unit) with No.4 (12.7 mm) bars threaded through block cavities filled with mortar or concrete and with horizontal joint reinforcement at every course or | (a) | 4.0 | 4.0 | <1 |
| | 8 inches (200 mm) of brick interlocked between inner and outer courses | (a) | 2.5 | 2.5 | <1 |
| FLOORS | 6-inch (150 mm) concrete construction reinforced with 6-inch (150 mm) by 105 mm) W4 by W4 mesh or equivalent bars | (a) | (a) | 18(b) | <1 |
| | Arms storage areas constructed on a second deck or having a floor that serves as a roof/ceiling for a space beneath, will be constructed of 8-inch (200 mm) concrete reinforced with two grids of Number 4 (12.7 mm) rebar on 9-inch (225 mm) centers NOTE: All reinforcing bar spacing will form a grid using No.4 (12.7 mm) bars or larger so that the area of any opening does not exceed 96 square inches (0.6 sq. m.) | (a) | (a) | 7.6 | <1 |
| ROOF/ CEILING | 8-inch (200 mm) concrete reinforced with Number 4 (12.7 mm) reinforcing bars, 9-inches (225 mm) on center or | (a) | (a) | 15 | <1 |
| | If the roof or ceiling is of concrete pan-joint construction, the thinnest may not be less than 6-inches (150 mm) and the clear space between joists may not exceed 20 inches (500 mm) NOTE: All reinforcing bar spacing will form a grid using No.4 (12.7 mm) bars or larger so that the area of any opening does not exceed 96 square inches (0.6 sq. m.) | (a) | (a) | 7.6 | <1 |

(a) Cannot be defeated at this threat severity level.

(b) Penetration is for an upward attack for other than floors on grade (not practical to attack)

TABLE 1 - MINIMUM CONSTRUCTION REQUIREMENTS
FOR RISK CATEGORIES I THROUGH IV

| MINIMUM CONSTRUCTION REQUIREMENT | | MINIMUM PENETRATION TIME (MINUTES) | | | |
|----------------------------------|---|---------------------------------------|-----|------|-----------|
| | | LOW | MED | HIGH | VERY HIGH |
| EXTERIOR DOORS | ALL NEW ARMORY EXTERIOR DOORS WILL BE CONSTRUCTED WITH Class 5 or Class 8 Armory Vault Doors | (a) | 10 | 2 | <1 |
| | THE FOLLOWING EXISTING DOORS ARE APPROVED: 1-3/4-inch (44 mm) solid or laminated wood with 12-gauge (2.7 mm) steel plate on the exterior face | (a) | 0.8 | <1 | <1 |
| | 1-3/4-inch (44 mm) hollow metal, industrial type construction with minimum 14-gauge (1.9 mm) skin plate thickness, internally reinforced vertically with continuous steel stiffeners spaced 6-inches (150 mm) maximum on center | (a) | 2 | <1 | <1 |
| LOCKS/ HASP | Vault Doors will be secured with Combination Dials meeting Group 1, UL Standard 768 Other doors will be secured with High a Security Lock meeting MIL-DTL-43607 and a High Security Hasp meeting MIL-DTL-29181 or Internal Locking Device (ILD) | (a) | 4 | <1 | <1 |
| MISC OPENINGS | Openings of 96 sq. in (0.06 sq m) or more with the least dimension greater than 6 inches (150 mm) will be protected by: Minimum 3/8-inch (9.5 mm) hardened steel rods with maximum 4-inch (100 mm) spacing with horizontal bars so that openings do not exceed 32 sq. in. (0.02 sq m) or Riveted steel grating (weight of 13.2 lb/sq ft (64.5 kg/sq m) or welded steel grating (weight of 8.1 lb/sq ft (39.6 kg/sq m) with 1 by 3/16-inch (25.4 mm by 4.7 mm) bearing bars | 0.8 | 0.8 | 0.3 | <0.1 |
| | | (a) | 4.0 | 1.0 | <1 |

(a) Cannot be defeated at this threat severity level.

(b) Penetration is for an upward attack for other than floors on grade (not practical to attack)

TABLE 2 - MINIMUM CONSTRUCTION REQUIREMENTS FOR RISK CATEGORIES II THROUGH IV, ARMS AND EARTH-COVERED MAGAZINES

| MINIMUM CONSTRUCTION REQUIREMENT | | MINIMUM PENETRATION TIME (MINUTES) | | | |
|----------------------------------|---|------------------------------------|-----|-------|-----------|
| | | LOW | MED | HIGH | VERY HIGH |
| WALLS | 8-inch (200 mm) concrete reinforced with No.4 (12.7 mm) reinforcing bars, 9 inches (225 mm) on center, in each direction and staggered on each face to form a grid approximately 4-1/2 inches (114 mm) square or 8-inch (200 mm) concrete block (or concrete masonry unit) with No.4 (12.7 mm) bars threaded through block cavities filled with mortar or concrete and with horizontal joint reinforcement at every course or 8 inches (200 mm) of brick interlocked between inner and outer courses NOTE: All magazine headwall construction for Risk Category I AA&E and Category II bulk explosives will be 12-inches (200 mm), or greater, of concrete reinforced with two grids of No. 6 (19 mm) steel bars spaced 12-inches (300 mm) apart, both horizontally and vertically and staggered on each face to form a grid approximately 6-inches (150 mm) square. | (a) | (a) | 15 | <1 |
| | | (a) | (a) | 4.0 | <1 |
| | | (a) | (a) | 2.5 | <1 |
| FLOORS | 6-inch (150 mm) concrete construction reinforced with 6-inch by 6-inch (150 mm by 150 mm) W4 by W4 mesh or equivalent bars NOTE: All reinforcing bar spacing will form a grid using No.4 (12.7 mm) bars or larger so that the area of any opening does not exceed 96 square inches (0.6 sq. m.) | (a) | (a) | 18(b) | <1 |
| ROOF/ CEILING | 8-inch (200 mm) concrete reinforced with two grids of Number 4 (12.7 mm) rebar on 9-inch (225 mm) centers or If the roof or ceiling is of concrete pan-joint construction, the thinnest may not be less than 6-inches (150 mm) and the clear space between joists may not exceed 20 inches (500 mm) NOTE: All reinforcing bar spacing will form a grid using No.4 (12.7 mm) bars or larger so that the area of any opening does not exceed 96 square inches (0.6 sq. m.) | (a) | (a) | 7.6 | <1 |
| | | (a) | (a) | 7.6 | <1 |

(a) Cannot be defeated at this threat severity level.

(b) Penetration is for an upward attack for other than floors on grade (not practical to attack)

TABLE 2 - MINIMUM CONSTRUCTION REQUIREMENTS FOR RISK CATEGORIES II THROUGH IV, ARMS AND EARTH-COVERED MAGAZINES

| MINIMUM CONSTRUCTION REQUIREMENT | | MINIMUM PENETRATION TIME (MINUTES) | | | |
|----------------------------------|--|------------------------------------|-----|------|-----------|
| | | LOW | MED | HIGH | VERY HIGH |
| EXTERIOR DOORS | Magazine Door construction requirements are outlined in Table 3 of this Appendix | | | | |
| LOCKS/HASP | Doors will be secured with a High Security Lock meeting MIL-DTL-43607 and a High Security Hasp meeting MIL-DTL-29181 or Internal Locking Device (ILD) | (a) | 4 | <1 | <1 |
| MISC OPENINGS | Openings of 96 sq. in (0.06 sq m) or more with the least dimension greater than 6 inches (150 mm) will be protected by: | 0.8 | 0.8 | 0.3 | <0.1 |
| | Minimum 3/8-inch (9.5 mm) hardened steel rods with maximum 4-inch (100 mm) spacing with horizontal bars so that openings do not exceed 32 sq. in. (0.02 sq m) or Riveted steel grating (weight of 13.2 lb/sq ft (64.5 kg/sq m) or welded steel grating (weight of 8.1 lb/sq ft (39.6 kg/sq m) with 1 by 3/16-inch (25.4 mm by 4.7 mm) bearing bars | (a) | 4.0 | 1.0 | <1 |

(a) Not practical to attack.

(b) DOD 5100.76-M requires 3/8-inch (9.5 mm) rods as a minimum.

TABLE 3 - TYPICAL MAGAZINE DOOR PANELS FOR EXPLOSIVE SAFETY
FOR CATEGORIES I THROUGH IV FOR AMMUNITION AND EXPLOSIVES

| OVERALL THICKNESS INCHES (mm) | STEEL PLATE FACES | | STIFFENERS | | MINIMUM PENETRATION TIME (Minutes) | | | |
|-------------------------------------|------------------------|-----------------------|---|---|------------------------------------|-----|------|-----------|
| | OUTSIDE INCHES (mm) | INSIDE INCHES (mm) | TYPE | SPACING | LOW | MED | HIGH | VERY HIGH |
| 10.75 (270) | 1/2 (12.5) | 1/4 (6.25) | 10-inch (250 mm) wide range flange 49 lb/ft (75 kg/m) | 18 inches (450 mm), apart Horizontal spaces | (b) | (b) | 4 | <1 |
| 7.75 (194) | 3/8 (9.4) | 3/8 (9.4) | 7-inch (175 mm) Structural Tee from wide flange 17 lb/ft (25 kg/m) | 17 inches (425 mm) apart | (b) | (b) | 4 | <1 |
| 4.62 (115) | 5/16 (7.8) | 5/16 (7.8) | 4-inch (100 mm) Structural Tee from wide flange 12 lb/ft (18 kg/m) | 17 inches (425 mm) apart, horizontal spaces | (b) | (b) | 4 | <1 |

- (a) Category I and II storage magazines have an IDS requirement.
(b) Cannot be defeated at this threat severity level.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX K

AA&E SURVEILLANCE REQUIREMENTS

NOTE: Pre-existing Substandard storage is unauthorized unless a waiver or exception is submitted to HQMC PS Division. Surveillance must meet requirements outlined in Chapter 8.

| Security Risk Category | Storage Location | IDS Status | Physical Checks |
|--|--|--|---|
| CATEGORY I MISSILES AND ROCKETS | All storage locations ashore and afloat | Without IDS | Constant surveillance. Afloat: each 4 hours at sea; each hour in port |
| | | With IDS | Patrol each 24 Hours |
| CATEGORY II (HIGH RISK) AMMUNITION AND EXPLOSIVE | Approved storage locations afloat. | Without IDS but with high security locks/hasps | Patrol each 24 hours |
| | | With IDS | Patrol each 24 Hours |
| | Approved Navy Magazines | Without IDS | Constant Surveillance |
| | | With IDS | Patrol each 24 Hours |
| | Temporary storage in open areas; vehicles, inadequately secured structures, aircraft ready service magazines and lockers, rooms, RDT&E test ranges/areas, production buildings | Without IDS | Constant Surveillance by station or security personnel |
| | | With IDS | Patrol each 8 hours |
| ALL SMALL ARMS (RISK CATEGORY II THROUGH IV, ASHORE) | All types of storage | Without IDS | Constant Surveillance |
| | | With IDS, including volumetric | Patrol each 24 hours for Category II; no patrol for Category III & IV |

AA&E STORAGE AREA SURVEILLANCE REQUIREMENTS

| Security Risk Category | Storage Location | IDS Status | Physical Checks | |
|---|--|--|--|--|
| CATEGORY III (MODERATE RISK) AMMUNITION AND EXPLOSIVES, ASHORE | On station reinforced concrete construction | Without IDS | Patrol each 24 hours | |
| | | With IDS | No patrol required | |
| | On station frame construction | Without IDS | Patrol each 12 hours | |
| | | With IDS | Patrol each 24 hours | |
| | Temporary storage in open areas, railcars, vehicles, aircraft, etc. | Without IDS | Continuous surveillance by activity personnel during operating hours; one patrol per hour during non-operating hours | |
| | | With IDS | Patrol each 24 hours | |
| | Temporary storage in ready service magazines and lockers, rooms, RDT&E test ranges/areas, production buildings | Without IDS | Each 4 hours during non-operating hours | |
| | | With IDS | Patrol each 24 hours | |
| | CATEGORY IV (LOW RISK) AMMUNITION AND EXPLOSIVES, ASHORE | On-station reinforced concrete or frame construction | Without IDS | Patrol each 24 hours and check each 48 hours |
| | | | With IDS | No patrol required |
| Temporary storage in open areas, railcars, vehicles, aircraft, etc. | | Without IDS | Constant surveillance by activity personnel during operating hours; one patrol per hour during non-operating hours | |
| | | With IDS | Patrol each 24 hours | |
| Temporary storage in ready service lockers, room, production buildings | | Without IDS | Patrol each 24 Hours | |
| | | With IDS | Patrol each 24 hours | |

TEMPORARY STORAGE IN BARGES AT
ANCHORAGE OR AT AMMUNITION PIERS

| SECURITY RISK CATEGORY | IDS STATUS | PHYSICAL CHECKS |
|---|-------------|--|
| CATEGORY I (HIGH RISK) | Without IDS | 24-hour armed guard |
| | With IDS | Patrol each 8 hours |
| CATEGORY II (HIGH RISK) | Without Ids | 24 hour surveillance during operating hours. Armed guard during non-operating hours. |
| | With IDS | Patrol each 8 hours |
| CATEGORY III (MODERATE RISK) and CATEGORY IV (LOW RISK) | Without IDS | Physical check each 4 hours (by boat when at anchorage) during operating and no-operating hours. |
| | With IDS | Patrol each 12 hours. |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX L

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 rounds;
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. Any fragmentation, concussion, or high explosive grenades including artillery or ground burst simulators, or other type of simulator or device containing explosive material;
8. One or more mines (antipersonnel and antitank);
9. 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.
10. Armed robberies or attempted armed robberies of AA&E facilities;
11. Forced entries or attempted forced entries into AA&E facilities;
12. Evidence of terrorist involvement in the theft of AA&E;
13. Incidents involving AA&E that cause significant news coverage, or appear to have the potential to cause such coverage; and

MCO 5530.14A

5 Jun 09

14. Evidence of trafficking or bartering involving AA&E, illegal drugs, etc., regardless of the quantity of AA&E involved.

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX M

MISSING, LOST, STOLEN AND RECOVERED (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. The Provost Marshal's Office or NCIS will be notified so the recovered items may be checked against the National Crime Information Center (NCIC). The command must also check the property against accountability data bases for correlation to any prior MLSR reports submitted by other commands. If the property item(s) recovered is identified as belonging to another service, the MLSR report will be submitted to the service owning the property and the reporting organization's headquarters. Initial/final MLSR reports will only be submitted for the purposes as outlined above.

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)
NAVSURFWARCENDIV CRANE IN (Code JXNP) (uc)
COMMARLOGCOM ALBANY GA (uc)
COMMARCORSYSCOM AM-IMS (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 (MIN: CONSIDERED)

c. Only prior MLSR property reports on the same incident will be referenced. References will 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.

g. 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. Number and status separated by a hyphen. The RPT must be indicated on every report. Each incident may involve one or more property items. Incident reports will be numbered consecutively by each reporting activity for each year. Examples: 1994/03-INITIAL, 1994/03-FINAL, 1994/03-SUPPLEMENTAL.

5 Jun 09

h. 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.

i. 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 February 1994.

j. 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.
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).

5 Jun 09

(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 if 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.

(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).

5 Jun 09

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

(4) Commercial Phone Number

(5) E-Mail address

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX N

INSTRUCTIONS FOR COMPLETING THE LAW ENFORCEMENT AND PHYSICAL
SECURITY ACTIVITY REPORT (LEPSAR)

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 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 March 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:

a. If a person in one incident commits offenses, report each offense the person is charged with. Do not report lesser-included offenses. For guidance, see the Manual for Courts-

Martial (MCM) United States 2005 Edition.

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) 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.

5 Jun 09

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. Definitions

a. Crimes Against Persons. Those crimes listed in section I of NAVMC 11197.

b. Crimes Against Property. Those crimes listed in section II of NAVMC 11197. "Others" in this category could include counterfeiting, wrongful appropriation, wrongful disposition, postal violations, receiving stolen property, and forgery. This category does not include those crimes involving fraud.

c. Criminal Complaint. An alleged criminal offense reported to, or observed by, law enforcement or criminal investigative personnel, whether subsequently determined to be founded or un-founded. (Will not be included on report unless determined to be founded.)

d. Offense. Any violation of law, lawful order, regulation, or direction which the offender has a duty to obey.

e. Founded Offense. A criminal complaint in which a determination is made that a criminal offense was committed. This determination is based on police action, not on a court-martial or civilian court verdict.

f. Unfounded Offense. A criminal complaint in which a determination is made that a criminal offense was not committed. This determination is based on a completed police investigation, not on a court-martial or civilian court verdict.

g. Solved. A founded criminal offense in which the subject is identified based on the results of a police investigation, not on a court-martial or civilian court verdict.

h. Unsolved. A founded criminal offense in which a subject has not been identified, or a determination cannot be made based on police action that the identified subject committed the offense.

i. Identified Subject. A person identified on an Incident Complaint Report (ICR) as the subject of a criminal offense.

j. Sex Offenses. Offenses or incidents of child molestation, indecent acts, trafficking in pornography, carnal knowledge, exhibitionism, incest, obscene communications, transvestitism, voyeurism, prostitution, pandering, and criminal abortion.

k. Fraud Offenses. Offenses or incidents of bribery and fraud involving conflict of interest, dependency assistance, personnel action, non-appropriated funds, and pay and allowances. This category does not include forgery, which is included in crimes against property.

l. Military Offenses. Military offenses are violations of a military order, regulation, or directive which the offender has a duty to obey. The offense may or may not be classified as a felony. For example, missing a troop movement is a military offense because there is no corresponding civilian law pertaining to troop movements. Similarly, certain civilian laws do not have parallels in military environments.

m. Narcotic. Opium, opium derivatives (morphine, codeine, heroin); synthetic opiates (meperidine, methadone); the coca leaf and its derivatives; cocaine; and crack;

n. Dangerous Drugs. Any substance listed in Schedules I through V in Title 21, U.S. Code, Section 812 (21 USC 812), which does not fall into the definition of narcotic or cannabis products.

o. Cannabis products. The intoxicating products of the hemp plant (cannabis sativa) including hashish.

10. 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.

11. 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.

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.

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 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.

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.

f. 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.

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.

g. 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.

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.

h. Section IX - Personnel Strength.

53-60) Personnel Strength. Enter (by MOS) the number of personnel assigned to the installation Provost Marshal's Office, whose primary duties include the performance of law enforcement or security duties. Enter the number of personnel as follows:

| Block - MOS | Block - MOS |
|-------------|-------------|
| 53 - 5801 | 57 - 5812 |
| 54 - 5803 | 58 - 5813 |
| 55 - 5805 | 59 - 5821 |
| 56 - 5811 | 60 - Other |

Additionally, in Block Number 56, enter the number of Marines possessing the additional MOS of 5814 (and working in the

MCO 5530.14A

5 Jun 09

Physical Security Section of the PMO) by placing the number in parentheses. In Block Number 59, enter the number of personnel possessing an additional MOS of 5822 in the same manner. In Block Number 60, enter the number of non-5800 personnel temporarily assigned to the Provost Marshal's Office for law enforcement or security duties.

Law Enforcement and Physical Security Activities
NAVMC 11197 (Rev. 01-09) EF
 Report Control Symbol No. - DD-1630-02

Print Form

| |
|-----------------|
| Period Covered: |
| Date Prepared: |
| Prepared By: |

| | |
|-------|--|
| From: | To: COMMANDANT OF THE MARINE CORPS HEADQUARTERS U.S. MARINE CORPS SECURITY DIVISION (PS) 3000 PENTAGON ROOM 4A324 WASHINGTON D.C. 20380-3000 |
|-------|--|

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 | # Cases Unidentified Subject | Drugs | Alcohol | Juveniles | |
| 1. Murder | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Rape | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Robbery | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Aggravated Assault | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. Assault Against On Duty Police Officer | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. Simple Assault | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7. Manslaughter | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8. Sex Offenses | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9. Suicide | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 10. Domestic Disturbances | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

II. Crimes Against Property

| | | | | | | | | | | | | | |
|--|--|--------------------------|--------------------------|--|--|--|--|--|--|--------------------------|--------------------------|--------------------------|--------------------------|
| 11. Arson | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 12. Burglary/ Housebreaking | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 13. Larceny Government | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 14. Larceny Non-Government | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 15. Auto Theft | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 16. Willful Property Destruction Gov't | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 17. Willful Property Destruction Non-Gov't | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 18. Other | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| 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 | # Cases Unidentified Subject | Drugs | Alcohol | Juveniles | |
| 19. Fraud | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 20. Smuggling | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 21. Black Marketing | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 22. Trespassing | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 23. Prowler | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 24. Homosexuality | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 25. Disturbance | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 26. Disorderly Conduct | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 27. Other | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| IV. Drug Offenses | | | | | | | | | | | | | |
| A. Use/Possesion | | | | | | | | | | | | | |
| 28. Narcotics | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 29. Dangerous Drugs | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 30. Cannabis Products | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| B. Sales/Trafficking | | | | | | | | | | | | | |
| 31. Narcotics | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 32. Dangerous Drugs | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 33. Cannabis Products | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| V. Other Security Response Activities | | | | | | | | | | | | | |
| 34. Unsecure Buildings | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 35. IDS / Duress Alarms | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 36. Animal Control | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 37. Other | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| VI. Traffic Law Enforcement | | | | | | | | | | | | |
|--|---------------------|--|--------------------------|-------------------------------|----------------------|------------------------|----------------------|---|------------------------------|--------------------------|--------------------------|--------------------------|
| | | Location | | Number of Subjects Identified | | | | | | Involvement | | |
| A. Alcohol Related Driving Offenses | | | | | | | | | | | | |
| Type of Offense | Number of Incidents | On Base | Off Base | USMC | Other Service | DOD CIV | Mil Depen | Others | # Cases Unidentified Subject | Drugs | Alcohol | Juveniles |
| 38. .10% BAC & Above | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 39. .05% - .09% BAC | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 40. .04% BAC & Below | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 41. Refusals | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| B. Other Traffic Data | | | | | | | | | | | | |
| 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 | Fatal | Non-Fatal | | | | | |
| 44. On Base | | | | | | | | | | | | |
| 45. Off Base | | | | | | | | | | | | |
| VII. Physical Security/Crime Prevention Activities | | | | | | | | | | | | |
| 46. Child ID Program | | Number of Dependent Children on Base | | | | | | Number of Children Fingerprinted | | | | |
| 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. | | |

MCO 5530.14A
5 Jun 09

THIS PAGE LEFT INTENTIONALLY BLANK