



UNITED STATES MARINE CORPS  
2D MARINE AIRCRAFT WING  
II MARINE EXPEDITIONARY FORCE  
POSTAL SERVICE CENTER BOX 8050  
CHERRY POINT, NC 28533-0050

WgO 5530.1

G-3

AUG 18 2010

WING ORDER 5530.1

From: Commanding General, 2d Marine Aircraft Wing  
To: Distribution List

Subj: STANDING OPERATING PROCEDURES (SOP) FOR PHYSICAL SECURITY PROGRAM

Ref: (a) MCO 5530.14A  
(b) OPNAVINST 5530.14E  
(c) SECNAVINST 5510.30B  
(d) SECNAVINST 5510.36A  
(e) DoD 7000.14-R  
(f) MCO 5500.6H  
(g) OPNAVINST 5530.13C

Encl: (1) SOP for Physical Security Program

1. Situation. Information, instructions, responsibilities, and procedures in this SOP are published as required by references (a) and (b). References (c) through (g) provide additional background and guidance and are referenced throughout this SOP.

2. Mission. To publish policies and establish procedures for the Physical Security Program within 2d Marine Aircraft Wing (2d MAW).

3. Execution. Should conflict arise between the procedures set forth in this SOP and the references, procedures established by higher headquarters will take precedence.

4. Administration and Logistics

a. References (a) and (b) provide specific guidance for security planning, security measures, security forces, barriers, protective lighting, and electronic security systems. Reference (g) establishes policies and procedures for arms, ammunition, and explosives.

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

b. Recommendations for changes, additions or deletions to this SOP are invited and should be submitted to 2d MAW (G-3) via the chain of command.

5. Command and Signal

a. Command. This Order is applicable to all units assigned or attached to 2d MAW.

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

  
R. W. REGAN  
Chief of Staff

DISTRIBUTION: A

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

**TABLE OF CONTENTS**

<b><u>IDENTIFICATION</u></b>	<b><u>TITLE</u></b>	<b><u>PAGE</u></b>
<b>Chapter 1</b>	<b>INTRODUCTION .....</b>	<b>1-1</b>
1.	Scope.....	1-1
2.	Objectives.....	1-1
3.	Security Challenge.....	1-1
4.	Security Responsibilities.....	1-2
5.	Commanding Officer.....	1-2
6.	Unit Security Officer.....	1-2
7.	Waiver and Exceptions.....	1-3
8.	Waiver and Exception Cancellation.....	1-4
9.	Host Nation Conflict.....	1-4
10.	Military/Minor Construction.....	1-4
<b>Chapter 2</b>	<b>SECURITY PLANNING.....</b>	<b>2-1</b>
1.	General.....	2-1
2.	Physical Security Plan.....	2-1
3.	Evaluation.....	2-1
4.	Cost of Security.....	2-2
5.	Coordination.....	2-2
6.	Security Considerations.....	2-3
7.	Calculated Risk.....	2-3
<b>Chapter 3</b>	<b>SECURITY MEASURES.....</b>	<b>3-1</b>
1.	Security Measures.....	3-1
2.	Physical Security Surveys.....	3-1
3.	Loss Prevention.....	3-2
4.	Loss Reporting.....	3-2
5.	Perimeter and Area Protection and Control.....	3-2
6.	Area Designation.....	3-3
7.	Signs and Posting of Boundaries.....	3-8
8.	Key Security and Lock Control.....	3-9
9.	Classified Security Containers, Vaults and Strong-rooms.....	3-11
10.	Security Checks.....	3-11
11.	Parking of Privately Owned Vehicles (POVs).....	3-12

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
<b>Chapter 4</b>	<b>SECURITY FORCES.....</b>	<b>4-1</b>
1.	Security Forces.....	4-1
<b>Chapter 5</b>	<b>BARRIERS AND OPENINGS.....</b>	<b>5-1</b>
1.	The Purpose of Physical Barriers.....	5-1
2.	Types of Barriers.....	5-1
3.	General Considerations.....	5-1
4.	Fences.....	5-2
5.	Temporary Barriers.....	5-4
6.	Vehicle Barriers.....	5-4
7.	Inspection of Barriers.....	5-4
8.	Walls.....	5-5
9.	Clear Zones.....	5-5
10.	Patrol Roads.....	5-6
11.	Perimeter Openings.....	5-6
12.	Doors, Windows, Skylights, and Other Openings.....	5-6
13.	Sewers, Culverts and Other Utility Openings.....	5-6
14.	Utility Poles, Signboards and Trees...	5-6
<b>Chapter 6</b>	<b>PROTECTIVE LIGHTING.....</b>	<b>6-1</b>
1.	General.....	6-1
2.	General Principles and Guidelines.....	6-1
3.	Types of Protective Lighting Systems..	6-2
4.	Protective Lighting Parameters.....	6-2
5.	Minimum Standards.....	6-3
6.	Emergency Power.....	6-3
7.	Protection-Controls and Switches.....	6-4
<b>Chapter 7</b>	<b>ELECTRONIC SECURITY SYSTEMS (ESS).....</b>	<b>7-1</b>
1.	Introduction.....	7-1
2.	General.....	7-1
3.	ESS Determination Factors.....	7-1
4.	ESS Policy.....	7-2
5.	Types of Systems.....	7-3
6.	Maintenance.....	7-4
7.	Training.....	7-4

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
APPENDIX A	DEFINITIONS.....	A-1
APPENDIX B	PHYSICAL SECURITY PLAN (FORMAT).....	B-1
APPENDIX C	WAIVER AND EXCEPTION (FORMAT).....	C-1
APPENDIX D	SECURITY SURVEY GUIDE FOR DISBURSING FACILITIES.....	D-1
APPENDIX E	SECURITY GUIDE FOR WAREHOUSES.....	E-1

## Chapter 1

### Introduction

1. Scope. This SOP directs the application of Physical Security Programs for 2d MAW units. Definitions applicable to this SOP are contained in Appendix A. This SOP further:

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

b. Directs all 2d MAW Commanding Officers, squadron level and above, to implement the contents of this SOP and augment the guidance provided with local directives as required

### 2. Objectives

a. To preserve the war fighting capability and operational readiness of 2d MAW units.

b. To deter, detect, and defend against threats to 2d MAW assets.

c. To evaluate the effectiveness of policies, doctrine, and procedures.

### 3. Security Challenge

a. Protection of personnel and property is accomplished by:

(1) Identifying the personnel or property requiring protection.

(2) Determining jurisdiction and boundaries.

(3) Assessing the threat.

(4) Committing resources.

(5) Establishing perimeters, barriers, and access control.

(6) Providing the means to detect efforts to wrongfully remove, damage, or destroy property.

4. Commanding Officer. Each Commanding Officer is responsible for physical security within his/her organization. As such, he/she is responsible for:

a. Establishing and maintaining a Command Physical Security Program that encompasses all requirements of this SOP.

b. Appointing a Unit Security Officer in writing and providing him/her with sufficient resources, staff assistance and authority to implement, manage and execute an effective Physical Security Program. It is recommended that the Unit Security Officer also be appointed as Command AT/FP Officer, as these two programs complement one another.

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

5. Unit Security Officer. The Unit Security Officer serves as the focal point for physical security matters and will report directly to the Commanding Officer in matters pertaining to physical security. Each Security Officer will be appointed in writing. Individuals assigned as Security Officers may be assigned such duties on a collateral basis and will be a Commissioned Officer, Staff Non-Commissioned Officer or equivalent civilian employee grade. In this capacity, the Security Officer will:

a. Plan, manage, implement, and direct the Unit Physical Security Program.

b. Establish physical security requirements for the unit with assistance from the Installation Provost Marshal, Public Works Officer and facilities engineer as appropriate.

c. Develop, implement and maintain a Unit Physical Security Plan. This plan should be incorporated into the unit AT/FP plan.

d. Develop and maintain a Unit Security Education Program.

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

f. Coordinate identification of restricted areas with the Provost Marshal. Ensure these areas are designated in writing by the Commanding Officer and provided to the Installation Commander/Commanding Officer for inclusion in the installation SOP/directive that identifies all restricted areas.

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

h. Assist the Commanding Officer in specifying facility, training, construction, and equipment requirements necessary to comply with this SOP.

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

j. Serve as the unit point of contact for all requests for physical security and loss prevention to include exceptions/waivers, Missing Lost Stolen Reports (MLSRs), etc.

k. Coordinate all AT/FP and physical security matters with the installation Provost Marshal.

6. Physical Security Council (PSC). Installations are required to have a PSC, established in writing, which meets on a quarterly basis. The PSC coordinates and implements initiatives that support the installation's Physical Security and AT/FP Program.

a. When agenda items directly impact their command, 2d MAW Unit Security Officers will attend their installation's PSC.

b. Council minutes are recorded for accuracy and distributed to attendees for review. 2d MAW Unit Security Officers will obtain a copy of the minutes when they attend a PSC. These minutes will be maintained on file for a period of one year.

7. Waiver and Exceptions. The Security Division (PS) serves as the sole authority for waivers and exceptions to physical security requirements. Requests for waivers/exceptions will be originated by the Commanding Officer of the affected unit and completed in the applicable prescribed format as outlined in Appendix C of reference (a). The initiating command will assign a waiver or exception number per the prescribed format. All

information must be provided in waiver and exception requests, to include extension requests. All requests for waivers/exceptions will contain a unit plan of action and milestones. Non-applicable (N/A) elements shall be noted as N/A. Requests will contain an analysis of the problem and a detailed description of equivalent security measures in effect. The Commanding Officer will ensure that compensatory measures have been implemented and that such measures are identified within the request. All requests must be endorsed by the installation Provost Marshal. Ensure that the most recent Physical Security Survey for that facility is attached. Requests will be forwarded via the chain of command to Security Division (PS) for approval/disapproval.

a. Waivers are granted for a one year period when corrective action of a security requirement may be accomplished by the unit. Exceptions are granted for three years when corrective action of a security requirement is beyond the capability of the unit or the condition necessitating the request cannot be corrected in the near-term. Requests for extensions will be completed in the format prescribed in Appendix C of reference (a) and will be processed for approval in the same manner as the original request. Additionally, all extension requests must be accompanied by the latest Physical Security Survey conducted for that site.

b. Permanent waiver/exceptions will not be granted.

8. Waiver and Exception Cancellation. Waivers and exceptions are self-canceling at the end of the allocated time. Requests for renewal must be submitted prior to the expiration date. Unit commanders are directed to notify Security Division (PS), via higher headquarters, once the waiver/exception deficiency(ies) has been corrected and the requirement no longer exists.

9. Facility Modifications. Physical security and force protection enhancement modifications initiated by 2d MAW units to existing buildings, facilities, sites, etc., will be reviewed by the Provost Marshal or designated representative, Security Officer and AT/FP Officer during the design process, all review phases and final (100%) drawings. Modification requests will be forwarded via the Provost Marshal and/or Security Officer who will ensure that changes are consistent with applicable security criteria.

10. Military/Minor Construction

a. All military construction projects will be sent to CMC Installation and Logistics (I&L) and Security Division (PS) for review to ensure physical security and force protection requirements have been addressed. Installation facility engineers, AT/FP officers, and physical security personnel will review all military/minor construction projects to ensure that physical security and force protection requirements have been addressed.

b. Military/minor construction shall comply with the requirements of this SOP and other appropriate physical security design/technical manuals.

AUG 18 2010

## Chapter 2

Security Planning

1. General. Each unit (squadron and above) will develop and publish a Physical Security Plan as part of its AT/FP Plan. Unit physical security plans will be integrated into the installation plan.

2. Physical Security Plan. A model Physical Security Plan format is provided in Appendix B. The plan should reflect the detailed implementation of Marine Corps policy at the unit and should not be philosophical or a verbatim reiteration of this SOP. The Physical Security Plan is not intended to replace the AT/FP plan; it will complement the plan with detailed information concerning daily application of access control material control, barriers, etc., aboard the installation. The Physical Security Plan will be reviewed annually in conjunction with the AT/FP Plan.

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

- a. Overall importance/criticality of the command.
  - (1) Mission of the command.
  - (2) Importance of the command to essential installation operations.
- b. Overall susceptibility/vulnerability of the command to threats.
  - (1) The threat to a specific command as defined by military intelligence and investigative agencies.
  - (2) Ease of access to vital equipment and material.
  - (3) Location, size, deployment, and vulnerability of facilities within the activity and the number of personnel involved.
  - (4) Need for tailoring security measures to mission critical operating constraints and other local considerations.
  - (5) Legal jurisdiction.

(6) Mutual aid and unilateral assistance agreements.

(7) Local political climate.

(8) Adequacy of storage facilities for valuable assets and other war fighting materials.

(9) Accessibility of the activity to disruptive, criminal, subversive, or terrorist elements.

(10) Coordination of security forces.

(11) Calculated risk.

(12) Potential for increase in threat.

(13) Possible damage or harm to the civilian community if the item is stolen or lost.

4. Cost of Security. Physical security expenditures should be based on the cost of the item to be protected, the possible damage or the loss of the item could inflict upon the civilian population and the importance of the item to overall national security and command readiness posture. Items that are vital to national security or may pose a threat to the civilian population will be provided additional security commensurate with their sensitivity and the threat.

5. Coordination. All physical security measures employed by 2d MAW units will be coordinated through the installation commander. Physical security of all Arms, Ammunition and Explosives (AA&E) and other hazardous material held by units 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 Security Officer/Provost Marshal to ensure that security considerations are identified.

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

- a. Personnel screening and indoctrination.
- b. Security/protection for vulnerable points/assets within the unit.
- c. Security force organization and training.

AUG 18 2010

- d. Personnel identification and control systems.
- e. Use of physical security hardware (e.g., intrusion detection systems, barriers, access control systems).
- f. Key and lock control.
- g. Coordination with other security agencies.
- h. Designation of restricted areas.

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

## Chapter 3

### Security Measures

1. 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.

2. Physical Security Surveys. A Physical Security Survey is a systematic evaluation of the overall security of a given facility or unit and should not be regarded as an inspection or investigation. Surveys identify deficiencies and corrective measures to the commander. Programs and systems examined will be physical (e.g., lighting, barriers, locks) and procedural (e.g., access control, lock and key control, property accountability). The concept is to design and implement a system that uniformly protects the facility. Some units will have specific security requirements outlined in additional orders that compliment the requirements of this SOP. In those instances, the security requirements set forth in those directives will be addressed as part of the survey.

a. Physical Security Surveys will be scheduled with the responsible organization. The command requesting/requiring the survey will assign an individual to assist the Physical Security Specialist during the course of the survey. Additionally, briefings will be conducted with the commander or designated representative prior to and upon completion of the survey.

b. Physical Security Surveys will be completed using NAVMC Form 11121 or an equivalent electronic copy.

c. Surveys will be conducted at the following facilities:

(1) AA&E storage facilities.

(2) Disbursing offices.

(3) Storage facilities containing sensitive and/or high value materials.

(4) All other restricted areas and facilities not previously identified and mission-critical areas designated in writing by the installation commander.

d. Physical Security Surveys of classified facilities will be stored and protected in accordance with and pursuant to the security classification afforded the highest level of material contained within.

e. Physical Security Surveys of classified material storage/classified material control center will be structural in nature. The installation security manager is responsible for the inspection of administrative procedural requirements.

f. Original surveys will be maintained for a period of three years by the affected unit.

3. Loss Prevention. Losses can be minimized by application of a comprehensive loss prevention program consisting of, but not limited to: loss analysis, proper use of available investigative and police resources, employee loss prevention education, application of firm corrective measures, administrative personnel actions, and pursuit of prosecution.

#### 4. Loss Reporting

a. MLSR government property report will be submitted as required by reference (a). The Unit Security Officer is the focal point for MLSR reporting.

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

c. Actual losses must be reported so that accurate assessments can be made. Steps must be taken to ensure those reportable losses and accountable individuals are identified. This can be accomplished by matching property inventories, requests for investigations, inventory adjustments, and submitting loss reports.

5. Perimeter and Area Protection and Control

a. Prior to making decisions to employ security measures, a threat assessment must be obtained from Naval Criminal Investigative Service and a vulnerability assessment must be performed to determine the degree of physical security required. Extensive and costly security measures may be necessary to protect certain items of security interest. However, in each case the commander is responsible for complying with established security requirements while working to achieve economy. To achieve this objective, security requirements must be clearly understood. Additionally, the criticality and vulnerability of the asset must be evaluated in relationship to a ranking of a potential threat. A specific level of security must be calculated to ensure the best possible protection for the threat level in a cost-effective manner. Only after the above preliminary factors are addressed can proper controls be instituted.

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

c. Enclave ("Island") Security Concept

(1) Enclaving involves the provision of concentrated security measures at specific sites within an 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

(2) Units that elect to adopt enclaving to protect assets as a temporary or permanent alternative to required perimeter standard fencing must submit a waiver or exception request per Chapter 1, paragraph 8. Requests must indicate the type of perimeter fencing planned and/or other compensatory security measures planned or in place.

6. Area Designation. Different areas and tasks require varying degrees of security interest and importance. The degree of security is dependent upon their purpose, the nature of the work performed within, and information and/or materials concerned. To address these concerns, facilitate operations and simplify the security system, a careful application of restrictions, controls, and protective measures is essential. In some cases, the entire area may have a uniform degree of security importance requiring only one level of restriction and control. In others, the degree of security importance will require further segregation of certain security interests.

a. Areas will be designated as either restricted areas or non-restricted areas. Restricted areas are established in writing by a Commanding Officer within his/her jurisdiction. Commanding Officers will publish and inform the Installation Commander, in writing, of all areas under their control that are designated as restricted areas. Particular attention will be paid to those areas that are vital to or of substantial importance to national security.

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

(1) Level Three. The most secure type of restricted area, it may be within less secure types of restricted areas. It contains a security interest that if lost, stolen, compromised, or sabotaged would cause grave damage to the command mission or national security. Access to a Level Three restricted area is to be limited to relevant personnel with the appropriate clearances and designation letter.

(2) Level Two. The second most secure type of restricted area, it may be inside a Level One area, but is never inside a Level Three area. It contains a security interest that if lost, stolen, compromised, or sabotaged would cause serious damage to the command mission or national security. Uncontrolled or unescorted movement is prohibited to the fullest extent possible ensuring adherence to Level Three clearance and designation as much as possible.

(3) Level One. The least secure type of restricted area, it contains a security interest that if lost, stolen, compromised, or sabotaged would cause damage to the command mission or national security. It may also serve as a buffer zone for Level Three and Level Two restricted areas, thus providing administrative control, safety, and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement is to be minimized to relevant personnel in accordance with Levels Two and Three to the fullest extent practicable.

(4) Restricted areas will be designated as specified below:

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

(b) Level Two

1. Aircraft hangars, ramps, parking aprons, flight lines, and runways.

2. Aircraft rework areas.

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

4. AA&E storage facilities and processing areas (including gun parks and ammunition supply points). (Additional requirements are outlined in reference (g)).

5. Fuel depots and bulk storage tanks.

6. Installation, depot and critical communications, computer facilities, and antenna sites.

7. Installation, depot, and critical assets power stations, transformers, master valve, and switch spaces.

8. Tank ramps, compounds, and housing facilities.

(c) Level One

1. Motor Pools.

2. Fuel issue points.

3. Funds and negotiable instrument storage areas.

4. Provost Marshal's Office (PMO) Desk Sergeant/Dispatcher area, Electronic Security System monitoring spaces, and Military Working Dog facility.

c. Minimum Security Measures Required for Restricted Areas

(1) Level Three. The following minimum security measures are required for Level Three restricted areas:

(a) A clearly defined and protected 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 wall, it must be posted with restricted area signs per this SOP. Points of ingress will be posted in accordance with this SOP.

(b) A personnel identification and access control system (an electronic control system with the capability of recording ingress and egress may be used to accomplish this requirement). If a computer access control or logging system is used, it must be safeguarded against tampering. All visitors will be logged in and out in an entry/departure log at all times.

(c) Ingress and egress controlled by guards or appropriately trained and cleared personnel. When secured, an electronic security system or security personnel must control access to the area.

AUG 18 2010

(d) Access restricted to personnel who have duty requirements within and have been authorized in writing by the Commanding Officer. People who have not been cleared for access to the security interest contained within a Level Three restricted area may be admitted to the facility with approval, in writing, from the Commanding Officer. Such persons and all visitors will be escorted by an authorized/cleared activity escort at all times and the security interest will be protected from compromise.

(e) When secured, check at least once per 12-hour shift if adequately equipped with an operational Intrusion Detection System (IDS) or twice per 12-hour shift for those facilities without an IDS. Security force personnel will check for signs of attempted or successful unauthorized entry and for other activity that could degrade the security of the Level Three restricted area.

(2) Level Two. The following minimum security measures are required for Level Two restricted areas:

(a) A clearly defined and protected 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 wall, it must be posted with restricted area signs per this SOP. Barrier and lighting requirements are set forth in Chapters 5 and 6.

(b) A personnel identification and access control system (advise that an electronic control system with the capability of recording ingress and egress be used). If a computer access control or logging system is used, it must be safeguarded against tampering. All visitors will be logged in and out in an entry/departure log at all times.

(c) Ingress and egress controlled by guards, receptionists or other appropriately trained and cleared personnel. When secured, an electronic security system or security personnel must control access to the area.

(d) Access restricted to personnel who have duty requirements within and have been authorized in writing by the Commanding Officer. Persons who have not been cleared for shall be admitted only upon approval, in writing, from the Commanding Officer.

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

(e) At a minimum, the secured area should be checked once per 12-hour shift if adequately equipped with an operational IDS or twice per 12-hour shift for those facilities without an operational IDS. Security force personnel will check for signs of attempted or successful unauthorized entry and for other activity which could degrade the security of the Level Two restricted area.

(3) Level One. The following minimum security measures are required for Level One restricted areas:

(a) A clearly defined protected 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 wall it must be posted with restricted area signs per this SOP. Barrier and lighting requirements are set forth in Chapters 5 and 6.

(b) A personnel identification and control system for those personnel assigned to the activity.

(c) Controlled ingress and egress.

(d) Controlled admission of individuals (military, civil service, contractors, official visitors) who require access for reasons of official business, who render a service (vendors, delivery people), and other visitors as authorized by the Commanding Officer. All visitors will be escorted and the security interest protected from compromise.

(e) At a minimum, the secured area should be checked once per 12-hour shift if adequately equipped with an operational IDS or twice per 12-hour shift for those facilities without an operational IDS. Security force personnel will check for signs of attempted or successful unauthorized entry and for other activity which could degrade the security of the Level One restricted area.

(4) Assets that are considered as vital or important to the overall mission and national security are identified in reference (a).

d. Personnel and Vehicle Administrative Inspections. All instructions designating restricted areas shall include procedures for conducting inspections of persons and vehicles entering and leaving such areas. To be effective, administrative vehicle and personnel inspection operations must be conducted on a random basis. The unit Security Officer will ensure they are conducted. Procedures will be coordinated with the cognizant Staff Judge Advocate (SJA) and approved, in writing, by the Installation Commander/Commanding Officer or authorized representative.

e. Limited Waterway Areas. Unit commanders adjacent to waterfront property and waterways who desire to enhance the security of a site will coordinate efforts with the Installation Commander to ensure these areas are designated by proper authority. The following paragraphs provide information for commanders required to establish control mechanisms to limit persons, vehicles, vessels, and objects within designated areas. These paragraphs describe the different types of limited waterway areas available based on the level of threat. Commanding Officers will make every effort to address concerns and coordinate protection of adjacent waterway areas through the Installation Commander. Commanding Officers will review operations and/or security plans to ensure areas of responsibility/jurisdiction are properly identified. Liaison with the Installation Commander is critical to ensure timely designation of Limited Waterway Areas and procedural aspects are kept current.

f. Establishing Limited Waterway Areas. The cognizant United States Army Corps of Engineers (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. Public notification of designated Limited Waterway Areas is the responsibility of the local USACE or United States Coast Guard (USCG), as appropriate. Commanding Officers desiring adjacent waterway or waterfront access controls must provide a written request to the Installation Commander for forwarding to the appropriate local office of the USCG or USACE. Requests will include complete justification and details regarding the type of designation desired and area(s) to be designated. A copy of initial requests and final approval/disapproval correspondence will be forwarded to Security Division (PS).

AUG 18 2010

g. Non-Restricted Areas

(1) A non-restricted area is an area under the jurisdiction of a unit 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. A non-restricted area may be enclosed by a fence or other barrier. Access is normally minimally controlled. In most cases, further security authorization, such as a security clearance, would not be required for access. An off base housing area would normally be considered a non-restricted area. Non-restricted areas will not be located inside restricted areas.

(2) Units may contain a number of facilities where military personnel, their dependents, civilian employees and their families are permitted access by displaying vehicle decals or by presenting appropriate identification cards (issued based on employment or status only). 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.

7. Signs and Posting of Boundaries

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

WARNING RESTRICTED AREA-KEEP OUT  
AUTHORIZED PERSONNEL ONLY  
AUTHORIZED ENTRY INTO THIS RESTRICTED AREA CONSTITUTES CONSENT  
TO SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL.  
INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U.S.C. 797

b. Perimeter barriers of all restricted areas will be posted with signs measuring approximately 12 inches by 18 inches in size with proportionate lettering. Signs will read as follows:

WARNING RESTRICTED AREA-KEEP OUT

AUTHORIZED PERSONNEL ONLY

c. Unit 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 UNIT PROPERTY CONSTITUTES CONSENT TO  
SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL.  
INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U.S.C. 797

d. Perimeter boundaries will be posted with signs measuring approximately 11 inches by 12 inches in size with proportionate lettering. Signs will read:

U. S. GOVERNMENT PROPERTY  
NO TRESPASSING

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

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

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

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

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

(1) All words except "WARNING" will be black.

(2) The word "WARNING" will be red.

(3) All wording will be on white backgrounds to obtain maximum color contrast.

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

k. These signs may be contracted for or produced locally through facility maintenance.

## 8. Key Security and Lock Control

a. Each unit within 2d MAW must establish a strict key and lock control program managed and supervised by the unit Security Officer. Included in this program are all keys, locks, padlocks, and locking devices used to protect or secure restricted areas, activity perimeters, security facilities, critical assets, classified material, sensitive material, and supplies. Not included in this program are keys, locks and padlocks for convenience, privacy, unclassified administrative, or personal use.

b. Key Control Officer. The Key Control Officer will be designated in writing by the Commanding Officer and be directly responsible for all security-related key and lock control functions. Normally, the Key Control Officer will be subordinate to the unit Security Officer. At those organizations where the security and lock program is too small to warrant a subordinate designation, the Security Officer may assume this function. The Key Control Officer will conduct an annual inventory of all controlled issued keys and will maintain appropriate logs and records. Inventory records will be retained for three years or completion of the next Inspector General inspection cycle, whichever is greater.

c. Key Custodian. The head of each major functional area within a unit will designate, in writing, a Key Custodian who will be responsible to the Key Control Officer for all keys controlled by that functional area. Each custodian will inventory keys and log accounts at least semi-annually. The record of this inventory shall be retained for three years or until completion of the next Inspector General's inspection cycle, whichever is greater.

d. Central Key Room. Duplicate keys, key blanks, padlocks (key and combination type), and key-making equipment will be stored in a central key room. Access must be controlled and the space must be secured when not in use. Duplicate keys will be provided protection equivalent to the asset/area that original keys are used to secure. Controlled keys (e.g., AA&E, master, and classified material storage area keys) will not be duplicated at any time for any reason nor removed from the

installation/site without prior written consent of the Security Officer/Provost Marshal.

(1) At those units where the security key and lock program is too small to warrant a central key room, a locked security container may be used to provide protection of duplicate keys, blanks and associated equipment.

(2) Access to the container will be strictly controlled and the container custodian will be assigned in writing.

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

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

g. Key Control. The central key room and each key custodian and sub-custodian must follow the criteria as set forth in this SOP and any additional guidance from their respective Group/Squadron. Continuous accountability of keys is required.

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

i. Lock Control Seals. Inactive or infrequently used gates must be locked and have seals affixed. The approved seal is the car ball end seal, Military Specification MIL-S-23769C. Security personnel should be instructed that lack of free play (approximately one-eighth inch) indicates the possibility of tampering and a follow-up examination of the seal should be

conducted. Seals will be serialized, stored in the same manner as prescribed herein for keys, and all seals will be inventoried annually. The Security Officer will control placement of entrance seals and account for seal numbers on-hand, issued and used.

j. 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.

k. Lockouts. All lockouts at restricted areas or buildings will be reported to the Key Control Officer (or Duty Officer, as appropriate) for the organization having responsibility for the facility. The Commanding Officer of the facility will direct an investigation of the incident.

9. Classified Security Containers, Vaults and Strong-rooms. Security containers, vaults and strong-rooms will conform to the specifications contained in reference (a).

10. Security Checks

a. 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 PMO. Each deficiency or violation will be reviewed by the unit Security Officer and a record maintained of all corrective actions taken. Records of security checks will be maintained for a period of one year.

b. This review of subsequent actions is intended to resolve the present deficiency or violation and to prevent recurrence.

c. All deficiencies, violations, breaches of rules and regulations, and criminal incidents discovered and handled by the Security Force will be recorded.

11. Parking of Privately Owned Vehicles (POVs)

a. Vehicle parking is prohibited within 30 feet of any inhabited structure or 80 feet from troop housing and primary gathering places in order to minimize danger in the event of fire or explosion. POVs will not be parked in Level Three and

Level Two restricted areas or within 30 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 Military Construction (MILCON) and renovations projects as outlined in AT/FP orders and directives. Management of the parking assignments is not a function of the Security Officer.

b. At locations where parking is allowed inside Level One areas, parking areas will be located away from Level Two and Three restricted areas and separately fenced in such a manner that occupants of vehicles must pass through an access control point prior to entering the actual restricted area facility.

12. Security of Funds. Physical security requirements for funds under control of a disbursing officer or stored within a disbursing office are contained in reference (a).

13. Government Property

a. All U.S. Government office equipment will be secured to preclude pilferage. These items will also be marked with identification tags identifying them as U.S. Government property. When an office space is vacant during non-duty hours, doors will be secured and access controlled, or these items of equipment will be secured in security containers, or storage cabinets. As an alternative, items may be secured to desks with commercially available anchor pads or similar securing devices.

b. All audio visual equipment 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. After normal duty hours, these items will be locked in a room and security measures implemented.

c. Government owned televisions 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 items in place with commercially available anchor pads or similar securing devices.

AUG 18 2010

## Chapter 4

1. Security Forces. Per references (f) and (h) as necessary, assign a security force using the proper amount of force necessary to safeguard personnel and equipment. If personnel are required to augment each installations' Security Force, ensure that they are properly equipped, trained and organized to perform the requisite guard duties as assigned.

AUG 18 2010

## Chapter 5

### Barriers and Openings

1. 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:

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

2. Types of Barriers. Major types of physical barriers are:

- a. Natural, such as mountains, swamps, thick vegetation, rivers, bays, cliffs, etc.
- b. Structural, such as fences, walls, doors, gates, roadblocks, vehicle barriers, etc.

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

- a. Physical barriers will be established around all restricted areas. The barrier or combination of barriers used must afford an equal degree of continuous protection along the entire perimeter of the restricted area. When a section or sections of natural/structural barriers provide a lesser degree of protection, other supplementary means to detect and assess intrusion attempts must be used.

b. In cases of a high degree of relative criticality and vulnerability, it may be necessary to establish two lines of physical barriers at the restricted area perimeter. Such barriers should be separated by not less than 30 feet for optimum protection and control. Two lines of barriers should only be used either in conjunction with an ESS or other form of alarm system supported by a Security Force capable of immediate response. The use of two barriers alone provides little extra protection beyond a few seconds of delay to a determined intruder and may actually be counter productive in identifying the location of high risk items. The criticality, sensitivity, and vulnerability of certain areas may require the use of a taut wire fence, which provides the added advantages of an ESS.

c. 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.

d. 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.

#### 4. Fences

a. Chain Link Fencing. Chain link fencing is the type of structural barrier most commonly used and recommended for security purposes. Chain link fencing will be used to enclose restricted areas where fencing is required. Mesh openings will not be covered, blocked, or laced with material that would prevent a clear view of personnel, vehicles, or material in outer perimeter zones/areas. In those instances where a Commanding Officer determines application of a covering to be more advantageous to protecting the asset within the fenced area, a waiver or exception request must be submitted per paragraph 1013. The following standards apply:

(1) 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.

(2) 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.

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

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

(5) Reinforcement. Taut reinforcing wires will be installed and interwoven or affixed with fabric ties along the top and bottom of the fence to stabilize the fence fabric.

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

(7) Culverts and Openings. Culverts under or through a fence shall be of 10 inch pipe or a cluster of such pipe. Openings under or through a fence will be secured with material of equal or greater strength than the overall barrier. All openings which have an area of 96 square inches or greater and which penetrate the restricted area perimeter barrier will be protected by securely fastened 9-gauge wire mesh, framed and permanently bolted to the structure.

(8) Fence Placement. No fence will be located so that the features of the land (its topography) or structures (buildings, utility tunnels, light and telephone poles, ladders, etc.) allow passage over, around or under the fence.

AUG 18 2010

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

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

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

5. 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.

6. 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.

7. Inspection of Barriers. Security Force personnel will check security barriers at least weekly for defects that would

AUG 18 2010

facilitate unauthorized entry. Personnel must be alert to the following:

- a. Damaged areas (cuts in fabric, broken posts).
- b. Deterioration (corrosion).
- c. Erosion of soil beneath the barrier.
- d. Loose fittings (barbed wire, outriggers, fabric fasteners).
- e. Growth in the clear zones that would afford cover for possible intruders.
- f. Obstructions which would afford concealment or aid entry/exit for an intruder.
- g. Evidence of illegal or improper intrusion or attempted intrusion.

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

9. Clear Zones

a. 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 six inches in height.

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

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

AUG 18 2010

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

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

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

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

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

12. Gates

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

b. Inspection. When not in active use and controlled by a guard, gates, turnstiles and doors in the perimeter barrier will be locked and frequently inspected by security patrols. Locks will be rotated at least annually. Security for the keys and

combinations to locks on these gates is the responsibility of the Key Control Officer or Key Custodian, as determined by the Commanding Officer.

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

d. Vehicular Gates. Vehicular gates when physically practical will be set well back from any public highway in order that 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.

13. Doors, Windows, Skylights, and Other Openings. Building exterior doors will provide protection commensurate with the requirement for proper protection of the assets accessible through those doors. Unless the width-to-height ratio absolutely eliminates the physical possibility of intruder entry, openings will be protected by securely fastened 9-gauge wire mesh, framed and permanently bolted to the structure. Such openings are also considered inaccessible to personnel when they are 18 feet or more above ground level and 14 feet or more distant from buildings, structures, etc., outside the perimeter. Protective screens have the additional value of preventing projectiles such as rocks, hand grenades, bombs, and incendiaries from being hurled through the windows from outside the perimeter. Hinges to all doors will be located on the interior of the door. In locations where the hinge pin is exposed to the exterior, hinges will be pended, spot welded, or equipped with a hinge secure pin.

14. Sewers, Culverts and Other Utility Openings. Unless the width-to height ratio absolutely eliminates the physical possibility of intruder entry (for example, one inch by six inches) all utility openings which penetrate the perimeter or restricted area barrier will be protected against surreptitious entry. Protection of these opening may be accomplished by securely fastened bars, grills, locked manhole covers, or other equivalent means which provide security commensurate with that of the perimeter or restricted area barrier. Bars and grills across culverts, sewers, storm sewers, etc., create a hazard and

are susceptible to clogging. This hazard must be considered during construction planning. All drains/sewers will be designed to permit rapid clearing or removal of grating when required. Removable grates will be locked in place.

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

## Chapter 6

### Protective Lighting

1. General. Protective, or security, lighting is an integral part of both the command security and safety posture. This lighting provides a continuing degree of security commensurate with that during daylight hours. It increases the effectiveness of Security Forces performing their duties and has considerable value as a deterrent to criminal activity. Requirements for protective lighting at an activity are determined by the asset(s)/area(s) to be protected, facility layout, terrain, and weather conditions. Where lighting is impractical, additional compensating measures must be instituted.

2. General Principles and Guidelines. Reference (a) provides general principles and guidelines for exterior protective (security) lighting. When protective lighting is installed and used, the following basic principles should be applied:

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

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

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

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

e. Design the system to provide overlapping light distribution.

f. Avoid drawing unwanted attention to restricted areas.

g. During planning stages, consideration should be given to future requirements of Closed Circuit Television and recognition factors involved in selection of the type of lighting to be installed. Where color recognition will be a factor, full

spectrum (high pressure sodium vapor, etc.) lighting vice single color should be used.

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

### 3. Types of Protective Lighting Systems

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

(1) Glare Projection Lighting. This system uses lights slightly inside a security perimeter and directed outward. This method is useful where the glare of lights directed across surrounding territory will neither annoy nor interfere with adjacent operations.

(2) Controlled Lighting. Best used when it is necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways, railways, navigable water, or airports.

b. Standby Lighting. A standby system differs from continuous lighting in that its intent is to create an impression of activity. The lights are not continuously lighted, but are either automatically or manually turned on randomly or when suspicious activity is detected or suspected by security personnel or ESS.

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

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

4. Protective Lighting Parameters. It is not the intent of this SOP to prescribe specific protective lighting requirements. Except for minimum standards described in reference (a), the Commanding Officer must decide what other areas or assets to illuminate and how to do it. This decision must be based upon the following:

a. Relative value of items being protected.

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

c. Availability of Security Forces to patrol and observe illuminated areas.

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

e. Energy conservation.

5. Minimum Standards

a. Unpatrollable fence lines, water boundaries and similar areas need not be illuminated. Where these areas are patrolled, sufficient illumination should be provided to assist the Security Force in preventing intrusion.

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

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

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

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

6. Emergency Power. Restricted areas with protective lighting should have an emergency power source located within the restricted area and provisions must be made to ensure immediate availability of emergency power in the event of primary power source failure. The emergency power source shall be adequate to sustain security lighting and communications requirements and other essential services. Emergency power sources should start automatically. Battery-powered lights and essential communications should be available at all times at key locations within the restricted area in the event of complete failure of primary and emergency sources of power. Emergency power systems will be tested quarterly and the results will be recorded/logged and maintained for a period of three years.

AUG 18 2010

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

## Chapter 7

### Electronic Security Systems (ESS)

1. Introduction. ESS' are an essential element of any in-depth physical security program. ESS consist of sensors capable of detecting one or more types of phenomena, signal media, and energy sources for signaling the entry or attempted entry into the protected area. The design, implementation, and operation of ESS must contribute to the overall physical security posture and the attainment of security objectives. ESS is designed to detect, not prevent, actual or attempted penetrations.

2. General. ESS' are used to accomplish the following:

- a. Permit more economical and efficient use of security.
- b. Provide additional controls at critical areas or points.
- c. Enhance the Security Force capability to detect and defeat intruders.
- d. Provide the earliest practical warning to Security Forces of any attempted penetration of protected areas.

3. ESS Determination Factors. For those facilities requiring ESS, specific regulatory guidance has been provided in reference (a). In addition to regulatory guidance, the following factors must be addressed to determine the necessity for installation of ESS:

- a. Mission.
- b. Criticality.
- c. Threat.
- d. Geographic location of the facility and location of facilities to be protected within each activity.
- e. Accessibility to intruders.
- f. Availability of other forms of protection.
- g. Life cycle costs of the system.

AUG 18 2010

- h. Construction of the building or facility.
- i. Hours of operation.
- j. Availability of a Security Force and expected response time to an alarm activation.

#### 4. ESS Policy

a. The Marine Corps ESS (MCESS) program was established to ensure that all Marine Corps ESS is standardized. The background and policy as listed in reference (a) will be applied and followed by all 2d MAW units.

b. Under MCESS, Security Division (PS) is the program manager for ESS and oversees the funding, procurement, installation, and maintenance of ESS. The focal point for the operation of these systems is the installation Provost Marshal.

c. Access codes for manager level access to Marine Corps ESS will be restricted to site representatives only.

d. Site representatives will be the only personnel allowed to make notification of a trouble nature to the MCESS TSA.

e. Security Division (PS) has the responsibility for managing the ESS program for the Marine Corps. All armories, magazines, and flightlines in the Marine Corps are serviced by a single alarm type. Any commercial alarm systems procured that will annunciate at, or be monitored by, PMO will be compatible with the AA&E/Flightline ESS.

(1) Security Division (PS) is responsible for funding ESS installation for AA&E and flightline security applications. Any other ESS security projects will be funded by the command/installation.

(2) Installation Commanders are responsible for coordinating the procurement, installation, and maintenance of ESS at facilities on their installations, therefore, unit commanders identifying a need to obtain these non-AA&E/flightline systems will forward requests to the Installation Commander.

(3) Keyswitches, controllers, or other mechanisms used to activate and deactivate the ESS will be installed inside the protected area whenever possible. Components mounted on the exterior will be provided additional protection with a locking

assembly or outfitted with an anti-tamper device. Alarm activation delay devices are installed in order to allow sufficient time for personnel to exit the area after the system has been activated. AUG 18 2010

(4) 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.

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

## 5. Types of Systems

a. Local Alarm. Local alarms actuate a visible and/or audible signal, usually located on the exterior of the facility. Alarm transmission lines do not leave the facility. Response is generated from Security Forces located in the immediate area.

b. Central Station. Central station system signals are transmitted to, and annunciate in, an independent monitoring station that records activations and maintains the on-site equipment. The monitoring station is usually managed through a civilian firm with operators and guards/response forces available on a 24-hour basis. Connection to the station is primarily over leased telephone lines.

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

d. Proprietary ESS Station. Proprietary ESS stations currently exist on, and are the prescribed ESS for Marine Corps installations. The MCESS proprietary station incorporates both the central station and police connection concept. Alarmed facilities aboard installations are connected to an ACC that is monitored 24 hours a day by Military Police and in some cases, civilian employees. Military Police are the primary response force; however, in some cases personnel assigned duties as

**AUG 18 2010**

interior guard may be assigned as the response force. Maintenance for the proprietary Marine Corps ESS system is conducted by the TSA and is coordinated with the installation Provost Marshal.

6. 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. Maintenance requirements will be established per the manufacturer. At a minimum, all ESS systems will receive semi-annual preventive maintenance service. All performed maintenance will be recorded and records will be maintained for a period of one year. Additionally:

a. Follow recommendations of equipment manufacturers and installers.

b. Consider actual experience with systems installed.

c. Comply with more stringent criteria in other security directives when they apply.

d. Testing. All ESS will be tested at least quarterly to ensure systems are functional. In the conduct of these tests, all individual sensors will be tested to determine the continued adequacy of their application. Tests will include an interruption of the AC power source to ensure proper transfer to alternate power sources in order to determine functionality of the source. Test results will be retained for a period of one year.

7. Training. Personnel who operate, perform basic troubleshooting, maintenance, or repairs of ESS will be trained by certified personnel.

a. Marine Corps site representatives will possess Military Occupation Specialty (MOS) 5814.

b. Site representatives are the only personnel authorized to perform basic troubleshooting and first echelon maintenance and will be trained and certified by the Marine Corps contracted ESS TSA in basic troubleshooting and first echelon maintenance. First echelon maintenance will be defined by Security Division (PS).

AUG 18 2010

APPENDIX A

DEFINITIONS

1. For the purpose of this manual, the following definitions apply:

a. Administrative Vehicle Inspection. A cursory inspection of the contents of a vehicle with full consent of the operator or owner. Administrative inspections are conducted with prior written authorization and direction by the installation or activity Commanding Officer as to the methods and procedures to be employed.

b. Antiterrorism. Defensive measures used by the United States Marine Corps to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

c. Armed Guard. A person equipped with a firearm and ammunition whose primary function is to protect property and who has received training in accordance with reference (c) and qualified with the firearm in accordance with reference (g).

d. Auxiliary Security Force (ASF). A local, non-deploying military asset derived from host and tenant commands. The ASF is used to augment the installation PMO during increased threat conditions.

e. Commanding Officer. The term Commanding Officer used throughout this order refers to, yet is not limited to, installation Commanding Officers and Commanding Officers, and Officers-In-Charge.

f. Counterterrorism. Offensive measures taken to prevent, deter, and respond to terrorism.

g. Espionage. Acts directed toward the acquisition of information through clandestine operations.

h. Exception. A written, approved, long-term (36 months or longer) or permanent deviation from a specific provision of this order.

AUG 18 2010

i. 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.

j. High-Risk Billet. Personnel billet external to the Marine Corps (such as United Nation observer, counterintelligence, or similar duties) that exists in a designated country.

k. High-Risk Personnel. U.S. personnel and their family members whose assignment or symbolic value may make them especially attractive or accessible terrorists target.

l. High-Risk Target. U.S. material resources and facilities which, because of mission sensitivity, ease of access, isolation, and symbolic value, may be especially attractive terrorist targets.

m. 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.

n. 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.

o. 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. The Physical Security Program is further concerned with means and measures designed to achieve force protection and anti-terrorism readiness.

p. Physical Security Inspection. An examination of the Physical Security Programs of an organization to determine compliance with physical security policy.

q. Physical Security Survey. A specific on-site examination of any facility or activity conducted by a trained Physical Security Specialist (MOS 5814) to identify security weaknesses and recommend corrective measures.

r. Sabotage. An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources.

s. Special Reaction Team. An element of PMO organized, trained and equipped to provide rapid armed response to critical incidents beyond the normal capability of the Military Police.

t. 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.

u. Waiver. A written temporary relief, normally for a period of one year, from specific standards imposed by this SOP.

APPENDIX B

PHYSICAL SECURITY PLAN (FORMAT)

**\*\*CLASSIFICATION\*\***

Activity:    Date:

1. Purpose. State the purpose of the plan.
2. General. Mission and size of the unit, average population of Marines and family members, overall daily population including civilian personnel.
3. Area Security. Identify overall size of the unit, 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

(b) Vehicle. Registration, including state and/or host country. Policy on administrative inspection of military and POVs.

**\*\*CLASSIFICATION\*\***

(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. POVs
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.

(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.

**\*\*CLASSIFICATION\*\***

**\*\*CLASSIFICATION\*\***

(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

(b) Mobile

1. Type

2. Current Placement and/or Staging Area

**\*\*CLASSIFICATION\*\***

AUG 18 2010

**\*\*CLASSIFICATION\*\***

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
    4. Support Requirements for Deployment

c. Electronic Security Systems

- (1) Alarm Control Center
- (2) Use and Monitoring
- (3) Alarm Response Policy
- (4) Alarm Response Drills
- (5) Training Requirements

**\*\*CLASSIFICATION\*\***

**\*\*CLASSIFICATION\*\***

- (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)
- f. Communications
  - (1) Monitoring Location
  - (2) Authorized Users

**\*\*CLASSIFICATION\*\***

AUG 18 2010

**\*\*CLASSIFICATION\*\***

- (3) Authorized Frequencies
- (4) Shared Frequencies
- (5) Mobile Assets (Vehicle and Portable)
- (6) Location of Support Equipment (Repeaters, etc)

**\*\*CLASSIFICATION\*\***

APPENDIX C

WAIVER AND EXCEPTION (FORMAT)

1. Waiver and Exception Identification. This appendix provides guidance for the assignment of waiver or exception numbers for deviations from established physical security standards. This format is also applicable when requesting extensions. The objective is to provide a ready identification of any given waiver or exception with respect to the organization involved, year of issue, and current status. The following paragraphs apply to each waiver or exception in regard to identification purposes to ensure compatibility with the automated database.

a. The first character will be the letter M, followed by the Unit Identification Code (UIC) of the organization initiating the request. The letter M is required to maintain compatibility with the automated database.

b. The character after the UIC will be W for waiver or E for exception.

c. The characters after the W or E will represent subsequent numbers of requests 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 which cite standards which cannot be met.

**Line 3** - Specific description of condition(s) that cause the need for the waiver and reason(s) why applicable standards cannot be met.

**Line 4** - Complete description of the physical location of affected facilities or area. Structures will be identified by building number.

**Line 5** - Identify interim mandatory compensatory measures in effect or planned.

**Line 6** - Describe the impact on mission and any problems that will interfere with safety or operating requirements if the waiver is not approved.

**Line 7** - Identify resources, including estimated cost, to eliminate the waiver.

**Line 8** - Identify actions initiated or planned to eliminate the waiver or estimated time to complete, to include the organization plan of action and milestones.

**Line 9** - Point of contact to include name, rank, DSN, 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 facilities or area. Structures will be identified by building number.

**Line 5** - Identify, in detail, equivalent security measures and/or compensatory measures that are being applied. Also indicate the organization plan of action and milestones.

**Line 6** - Describe the impact on mission and any problems that will interfere with safety or operating requirements if the exception is not approved.

**Line 7** - Point of contact to include name, rank, DSN, and commercial phone numbers.

APPENDIX D

SECURITY SURVEY GUIDE FOR DISBURSING FACILITIES

1. Has the commander responsible for the security of the disbursing office developed a security program and issued a command instruction or notice covering adequate protection of funds, documents, and instruments? (Reference (e), par 030302A(2))
2. Does the commander conduct periodic reviews of the program for adequacy of current security measures? (Reference (e), par 030302A(3))
3. Are all fund transfers coordinated and conducted with Military Police and/or armed personnel? (Reference (e), par 030302A(4))
4. Are deputies, agents, cashiers, and/or custodians each provided a separate secure container? (Reference (e), par 030302B)
5. Does the Disbursing Officer or designated representative, at least semi-annually, conduct an inspection of office security measures? Are records maintained of such inspections? (Reference (e), par 030302B)
6. Is vault access limited to only authorized personnel? (Reference (e), par 030302B(1))
7. If a vault day gate is utilized, have keys been issued to only authorized personnel? (Reference (e), par 030302B(1))
8. Are windows and doors kept to a minimum and barred and/or locked at all times? (Reference (e), par 030302B)
9. Are all transactions conducted from behind a physical barrier (cage, room, counter) which restricts normal traffic and interference by other activities and personnel in the office? (Reference (e), par 030302B)
10. Are all security devices for the check signing machines, meters, and plates kept in the custody of the Disbursing Officer or designated representative at all times? (Reference (e), par 030302B)

11. Has responsibility for receipt, holding, and final distribution of checks been assigned in writing? (Reference (e), par 030302B)

12. Has the Disbursing Officer provided written and oral instructions to all deputies, agents, cashiers, and custodians concerning the proper care and handling of cash and other accountable documents? Have all personnel signed affidavits attesting to receipt of these instructions? (Reference (e), par 030302B)

13. Are all cash, blank U.S. Treasury Checks, blank U.S. Savings Bonds, blank depositary checks, and related items kept in a vault, safe, or security container meeting the requirements set forth in paragraph 030304 of reference (e)? (Reference (e), par 030302B)

14. Are all fund containers, on wheels or weighing less than 750 pounds, stored in a vault or secured in a way to prevent movement? (Reference (e), par 030302B)

15. Are all fund containers visible to the exterior of the office illuminated to allow observation from security patrols? (Reference (e), par 030302B)

16. Are the combinations of each vault, safe, and fund container changed at least every six months and upon relief, transfer, separation, or discharge, of the accountable individual? (Reference (e), par 030302B)

17. Are safe combinations and duplicate keys of strong boxes maintained in a sealed, signed and dated envelope? Is the envelope maintained in the Disbursing Officer's safe? (Reference (e), par 030302B)

18. Is the combination to the Disbursing Officer's safe maintained in a signed, sealed envelope by the Commander or command Security Officer? (Reference (e), par 030302B)

19. Is a signed and dated record of all safe combination changes maintained in each safe or container? (Reference (e), par 030302B)

20. Is the dial to each vault, safe, or container shielded to limit the possibility of the combination being observed? (Reference (e), par 030302B)

21. Is the name and phone number of the accountable individual posted on the interior of the vault, safe, or container? (Reference (e), par 030302B)
22. Has a Key Control been established per reference (a), Chapter 3?
23. Has a Key Custodian been assigned per reference (a), Chapter 3?
24. Are keys to the individual work space or disbursing office strictly controlled? (Reference (e), par 030302B)
25. Is a Key Control Logbook maintained to identify individuals assigned keys, when they were issued, and when they were surrendered? (Reference (e), par 030302B)
26. Is an Intrusion Detection System (IDS) in use? Is the existence of the IDS system posted? (Reference (e), par 030303B)
27. Is the IDS protected against tampering, bypassing, and fool proofing? (Reference (e), par 030303C)
28. Is the IDS tested quarterly per reference (a), Chapter 6?
29. Is the disbursing office conspicuously posted as a restricted area per reference (a), Chapter 3?
30. Do all fund containers meet requirements? (Reference (e), par 030304)

Note\* Reference (e), volume 5, chapter 3 is the source document for questions 1 to 21, 24 to 27, and 30.

APPENDIX E

SECURITY GUIDE FOR WAREHOUSES

1. Has a unit Security Officer been appointed in writing?
2. Are hinges to doors non-removable or provided with inside hinge protection?
3. Are high dollar value, sensitive, and highly pilferable items protected with approved locking devices?
4. Has a Key Custodian been appointed in writing?
5. Are lock cores rotated at least annually or when deemed necessary?
6. Are only those personnel with the need issued keys with the approval of the Security Officer?
7. Is a key control logbook maintained?
8. Are physical and comprehensive key inventories conducted?
9. Are lock cores changed upon notification of lost or stolen keys?
10. Is the building afforded appropriate lighting?
11. Is the building checked after normal working hours by the Security Force?
12. Are security checks conducted prior to securing?
13. Is all business conducted behind a counter/barrier which precludes unauthorized access to storage area?
14. Are air ducts, heating shafts, trap doors, or similar apertures penetrating exterior walls, roof, or floor adequately secured?