Headquarters, U.S.
Marine Corps

MCO P5530.14
PCN 10208597900

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

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

MCO P5530.14
POS-10
21Dec00

MARINE CORPS ORDER P5530.14

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

Ref: (a) SECNAVINST 5212.5
(b) SECNAVINST 5510.36
(c) SECNAVINST 5510.30A
(d) OPNAVINST 5530.13B
(e) DoD Inst 2000.16
(f) MCO P11000.5F
(g) DOD 7000.14-R
(h) MCO 4340.1A
(i) DoD 5200.8R
(j) MCO 5110.1C
(k) NAVMEDCOMINST 6710.9
(l) MCO 5500.6F
(m) MCO 3574.2J
(n) MCO 5580.2
(o) NAVFAC MIL-HDBK-1013/1
(p) FMFM 7-14

Encl: (1) LOCATOR SHEET

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

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

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

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

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

d. Establishes minimum standards.

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

3. Discussion. To be effective, a physical security program must receive attention from all echelons within the chain of command. Emphasis is placed on the commanding officer's responsibility to ensure that the command security posture is accurately assessed and security resources are appropriate to execute these programs.

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

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

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

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

5. Recommendations. Recommendations for changes to this Manual are encouraged. All recommendations will be forwarded via the chain of command to the Commandant of the Marine Corps (POS-10).

6. Action

a. The Deputy Commandant for Plans, Policies, and Operations (DC, PP&O (POS)) is assigned overall coordination and program

responsibility for physical security within the Marine Corps and will:

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

(2) Develop physical security policy and oversee its implementation.

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

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

(5) Program funds in support of specific Marine Corps physical security initiatives, to include:

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

(b) Installation Physical Security Site Assistance Visits.

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

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

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

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

c. DC, I&L will:

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

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

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

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

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

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

7. Reserve Applicability. This Manual is applicable to the Marine Corps Reserve. See paragraph 7006 for limitations.

8. Records Disposition. Records required by this Manual will be maintained per part II, chapter 5, items 5500 through 5530 of reference (a).

9. Certification. Reviewed and approved this date.

E. R. BEDARD
Deputy Commandant for Plans,
Policies, and Operations

DISTRIBUTION: PCN 10208597900

Copy to: 7000099 (144)
7000110 (55)
8145005 (2)
8145001 (1)

LOCATOR SHEET

Subj: MARINE CORPS PHYSICAL SECURITY PROGRAM

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

ENCLOSURE (1)

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Making Change

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

TABLE OF CONTENTS

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 1

INTRODUCTION

CHAPTER 1

INTRODUCTION

1000. SCOPE. This Manual directs the application of physical security programs aboard Marine Corps installations, Marine Forces, and battalions/squadrons and above. Definitions applicable to this Manual are contained in Appendix A. This Manual further:

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

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

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

1001. THE SECURITY CHALLENGE

1. Protection of personnel and property is accomplished by:

    a. Identifying the personnel or property requiring protection.

    b. Determining jurisdiction and boundaries.

c. Assessing the threat.

d. Committing resources.

e. Establishing perimeters, barriers, and access control.

f. Providing the means to detect efforts to wrongfully remove, damage or destroy property.

g. Employing a security force sufficient to protect, react to, and confront situations and circumstances that threaten personnel and property.

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

3. Terrorist activity worldwide against U.S. military and business concerns poses a clear and persistent danger to Marine Corps interests. While such activity is principally targeted against commands overseas, prudence dictates recognition of the potential threat to activities within the continental United States. Additionally, military activities located within leased space facilities have unique challenges in addressing physical security issues (commercial firms and contractors located in same building(s), public facilities, shared entranceways and common spaces). Security officers shall use the guidance and policies contained in this Manual in determining security and/or protective measures deemed essential for their particular spaces, areas and/or buildings. Liaison with appropriate authorities (General Services Administration (GSA), building administrators, lessors, etc.) is essential to outline specific security measures that are necessary for protection of lives and property and tailored to the individual characteristics of the leased space. Commands should address physical security in all lease agreements, as appropriate.

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

1003. DEPUTY COMMANDANT FOR PLANS, POLICIES AND OPERATIONS (D/C PP&O). The D/C PP&O is responsible for formulation and dissemination of Marine Corps physical security policy. As such, the D/C PP&O has cognizance for implementation of this policy. All correspondence concerning physical security matters will be addressed to the CMC(POS).

1004. COMMANDER, MARINE FORCES. The Commander of Marine Forces Atlantic, Pacific, and Reserves (COMMARFORLANT, COMMARFORPAC, and COMMARFORRES) will implement and oversee requirements of this Manual within their headquarters and subordinate commands.

1005. INSTALLATION COMMANDER. The installation commander is inherently responsible for the overall command security posture to include perimeter and area security and protection of personnel and property aboard the installation. As such, the installation commander is responsible for:

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

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

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

1006. COMMANDING OFFICER. Each commanding officer (battalion/squadron and higher) is responsible for physical security within his/her organization. As such, he/she is responsible for:

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

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

3. Identifying and designating, in writing, all restricted areas within his 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. (Appendix C provides assistance.)

1007. PROVOST MARSHAL. The installation provost marshal serves as the staff officer responsible for coordinating the installation physical security and law enforcement programs. As such, the provost marshal is responsible for ensuring that those programs complement the overall installation security effort. In this capacity, the provost marshal will:

1. Conduct law enforcement operations in support of the installation physical security program, including measures to enhance security during periods of increased threat and crisis situations.

2. Determine the adequacy of the installation physical security posture with a physical security survey program. Physical security surveys identify areas requiring improvements and direct corrective measures to the responsible commanding officer. The surveys may also provide recommended actions for an improved organization security posture. Physical security surveys will be conducted as prescribed herein. An example survey is provided in Appendix D.

3. Maintain liaison with installation/regional Naval Criminal Investigative Service (NCIS) personnel in support of criminal investigations aboard the installation. Maintain liaison with federal, state, local, other military activities, and host nation officials regarding law enforcement/physical security concerns. These concerns will include mutual physical security responsibilities as applicable and according to Memorandums of Agreement (MOAs), Memorandums of Understanding (MOUs), Status of Forces Agreements (SOFAs), and Host Nation Agreements.

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

5. Support the installation commander in the development and maintenance of a comprehensive installation physical security plan.

6. Provide guidance and support to the installation physical security council as described herein.

7. Review and endorse all requests for physical security waivers and exceptions from command and tenant organizations.

8. Ensure law enforcement and physical security programs complement the installation AT/FP program. These programs are key elements of the AT/FP effort and the installation provost marshal will not be assigned as the AT/FP officer, as his focus is law enforcement and physical security functions.

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

10. Act as the manager of all centrally managed Electronic Security Systems (ESS) aboard the installation and develop

policy and procedures for ESS operation.

1008. COMMAND/ORGANIZATION SECURITY OFFICER. The command/organization security officer serves as the focal point for physical security matters and will report directly to the commanding officer in matters pertaining to physical security. Each security officer will be appointed in writing. Additionally, separate organizations such as Marine Corps Community Services (MCCS) activities, and tenant organizations will designate a security officer. Individuals assigned as security officers may be assigned such duties on a collateral basis and will be a commissioned officer, staff non-commissioned officer or equivalent civilian employee grade. In this capacity, the security officer will:

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

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

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

4. Develop and maintain an organization security education program.

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

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

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

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

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

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

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

12. Attend quarterly Physical Security Council meetings.

1009. PHYSICAL SECURITY OF ORGANIZATIONS NOT LOCATED ABOARD MARINE CORPS INSTALLATIONS. At all Marine Corps organizations not located aboard a Marine Corps installation, the commanding officer will:

1. Establish a command physical security program.

2. Appoint a command security officer in writing.

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

4. Additionally, those organizations located aboard other Department of Defense service/agency sites will coordinate physical security requirements with the host. Marine Corps organizations are encouraged to establish Inter-service Support Agreement (ISA)/MOUs/MOAs/SOFAs with the host service or nation. Topics, which should be addressed, include property boundaries, intrusion detection system monitoring, available response forces, deadly force training and issues, physical security

support, etc. Commanding officers are required to coordinate all such agreements through higher headquarters, to include Judge Advocate/legal offices.

1010. PHYSICAL SECURITY OF TENANT AND CIVILIAN AGENCIES/ ORGANIZATIONS ABOARD MARINE CORPS INSTALLATIONS. Tenant civilian organizations aboard Marine Corps installations will maintain an active physical security program that complements the installation's program. Host installations will establish a MOU/MOA/SOFA, and/or Host Nation Agreement where applicable and as directed, with tenant and civilian agencies that incorporate or recognize a physical security inspection program. Agreements will be coordinated with all special staff offices, particularly the Judge Advocate/Legal office. Tenant organizations will be made aware of all physical security initiatives to include the installation physical security council and antiterrorism contingency drills to be conducted by the host installation.

1011. PHYSICAL SECURITY COUNCIL. The installation commander/commanding officer will establish, in writing, a Physical Security Council (PSC) which will meet on a quarterly basis. The installation commander or a designated representative will chair the PSC. The PSC assists the commander by coordinating and implementing initiatives that support the installation's physical security and AT/FP program. The PSC provides a means for the commander to gain maximum participation from organizations on the installation in support of physical security interests.

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

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

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

4. Council minutes will be recorded for accuracy and distributed to attendees for review. These minutes will be maintained on file for a period of one year.

1012. WAIVERS AND EXCEPTIONS. CMC(POS) serves as the sole authority for waivers and exceptions to physical security requirements. Requests for waivers/exceptions will be originated by the commanding officer of the affected organization and completed in the applicable prescribed format as outlined in Appendix E. The initiating command will assign a waiver or exception number per the prescribed format. All information must be provided in waiver and exception requests, to include extension requests. All requests for waivers/exceptions will contain an organization plan of action and milestones. Non-applicable 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. The installation provost marshal will endorse all requests and ensure that the most recent physical security survey for that facility is attached. The provost marshal will identify if and/or how the exception/waiver may impact the overall installation security posture. Requests will be forwarded via the chain of command to include Commanding General/Commanding Officer and higher headquarters to CMC(POS) for approval/disapproval.

1. Waivers are granted for a one-year period when corrective action of a security requirement may be accomplished by the organization. Exceptions are granted for three years when corrective action of a security requirement is beyond the capability of the organization or the condition necessitating the request cannot be corrected in the near-term. Requests for extensions will be completed in the format prescribed in Appendix E and will be processed for approval in the same manner as the original request. Additionally, all extension requests must be accompanied by the latest physical security survey

conducted for that site. Waivers and exceptions to security criteria contained in reference (b) through (d) satisfy requirements of this Manual.

2. Permanent waiver/exceptions will not be granted.

1013. WAIVER AND EXCEPTION CANCELLATION. Waivers and exceptions are self-canceling at the end of the allocated time. Request for renewal must be submitted prior to the expiration date. Commands are directed to notify CMC(POS) once the waiver/ exception deficiency(ies) has been corrected and the requirement no longer exists.

1014. HOST NATION CONFLICT. Organizations located outside of the United States (OCONUS) may not be able to implement certain requirements of this Manual. In those instances, commanders must address physical security requirements in Host-Nation or Status of Forces Agreements (SOFAs).

1015. ACTIVITY UPGRADE PROJECTS

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

2. Physical Security Upgrade Project (R-2) Funding. This funding is awarded annually in support of installation physical security upgrade projects. Consideration for funding requires the installation to initiate correspondence to CMC(LFF-2) in accordance with the procedures outlined in reference (f). Once received at CMC(LFF-2), the project will be reviewed and validated by CMC(LFF-2) and (POS) and will compete for funding against security projects initiated throughout the Marine Corps. Projects approved will be awarded design funds and installations will be notified via Naval message traffic. Construction projects are evaluated and approved based on initial correspondence; therefore installations are not required to send an additional request. Request for authority to advertise the project for execution will be submitted on the installation’s contract advertisement forecast in accordance with reference

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

1016. FACILITY MODIFICATIONS. Physical security and force protection enhancement modifications to existing buildings, facilities, sites, etc., must be reviewed by the provost marshal or designated representative, security officer and AT/FP officer during the design process, all review phases and final (100%) drawings. Modification requests will be forwarded to the facility/public works officer via the provost marshal and/or security officer who will ensure that changes are consistent with applicable security criteria. Contract for bid will not be processed without documentation of review by security and AT/FP representatives.

1017. MILTARY/MINOR CONSTRUCTION

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

2. Military/minor construction shall comply with the requirements of this and other appropriate physical security design/technical manuals. All plans for new construction must incorporate physical security and force protection features and must be reviewed by the provost marshal or designated representative, security officer, and the AT/FP officer during the design process, all review phases and final (100%) drawings. A review will be conducted during the design process and all review phases. Contract for bid will not be processed without documentation of review by security and AT/FP representatives.

CHAPTER 2

SECURITY PLANNING

CHAPTER 2

SECURITY PLANNING

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

2001. PHYSICAL SECURITY PLAN. A model physical security plan format is provided in Appendix B. The intent of the plan is to clearly identify how the command conducts day-to-day security as well as how it responds to security incidents. The plan should reflect the detailed implementation of Marine Corps policy at the installation/activity and should not be philosophical or a verbatim reiteration of this Manual. The physical security plan will be included as an annex or appendix in the installation antiterrorism/force protection (AT/FP) plan, which is detailed in reference (e). 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.

2002. EVALUATION. In evaluating the type and extent of physical protection required, the following factors should be considered in planning:

1. Overall importance/criticality of the command.

a. Mission of the command.

b. Importance of the command to essential installation operations.

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

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

b. Ease of access to vital equipment and material.

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

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

e. Legal jurisdiction.

f. Mutual aid and unilateral assistance agreements.

g. Local political climate.

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

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

j. Coordination of security forces.

k. Calculated risk.

l. Potential for increase in threat.

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

2003. COST OF SECURITY. Physical security expenditures should be based on the cost of the item to be protected, possible damage which loss of the item could inflict upon the civilian population, and importance of the item to overall national security and command readiness posture. The cost of security is frequently greater than the dollar value of the property protected. Items that are vital to national security or may pose a threat to the civilian population will be provided additional security commensurate with their sensitivity and the threat.

2004. COORDINATION. Physical security of separate installations/organizations in the immediate geographic area will be coordinated with the installations/organizations and local civilian law enforcement agencies or host government representatives. On Marine Corps installations, the installation commander will coordinate physical security measures employed by tenant activities, regardless of the military command, service or agency represented. Physical security of all AA&E and other hazardous material held by tenant activities will be closely coordinated. Planning that may result in the physical relocation of an organizational element, physical changes to a facility, or a realignment of functions will include the security officer/provost marshal to ensure that security considerations are identified.

2005. SECURITY CONSIDERATIONS. Security measures to be considered when developing physical security plans include, but are not limited to the following:

1. Personnel screening and indoctrination.

2. Security/protection for vulnerable points/assets within the activity.

3. Security force organization and training.

4. Personnel identification and control systems.

5. Use of physical security hardware (e.g., intrusion detection systems, barriers, access control systems).

6. Key and lock control.

7. Coordination with other security agencies.

8. Designation of restricted areas.

2006. 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.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 3

SECURITY MEASURES

CHAPTER 3

SECURITY MEASURES

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

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

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

2. Physical security surveys will be scheduled with the responsible organization. The command requesting/requiring the survey will assign an individual to assist the physical security

specialist during the course of the survey. Additionally, briefings will be conducted with the commander or designated representative prior to and upon completion of the survey.

3. Physical security surveys will be completed using NAVMC Form 11121 or an equivalent electronic copy. An example survey is provided in Appendix D.

4. Surveys will be conducted at the following facilities:

a. Arms, Ammunition and Explosive (AA&E) storage facilities using Appendix I of reference (d) as a guide.

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

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

d. Exchange facilities using Appendix G as a guide.

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

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

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

6. Physical security surveys of classified material storage/classified material control center (CMS/CMCC) will be structural in nature, and the installation security manager will be responsible for the inspection of administrative procedural requirements.

7. Original surveys will be maintained for a period of three years by the affected facility and the provost marshal office physical security section.

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

3003. LOSS REPORTING

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

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

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

3004. PERIMETER AND AREA PROTECTION AND CONTROL

1. Prior to making decisions to employ security measures, a threat assessment must be obtained from NCIS and a vulnerability assessment, per reference (p), 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.

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

3. Enclave ("Island") Security Concept.

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

b. Installations that elect to adopt enclaving to protect assets as a temporary or permanent alternative to required perimeter standard fencing must submit a waiver or exception request per paragraph 1013. Requests must indicate the type of perimeter fencing planned and/or other compensatory security measures planned or in place.

3005. AREA DESIGNATION. Different areas and tasks require varying degrees of security interest and importance. The degree of security is dependent upon their Purpose, the nature of the work performed within, and information and/or materials

concerned. To address these concerns, facilitate operations and simplify the security system, a careful application of restrictions, controls, and protective measures is essential. In some cases, the entire area may have a uniform degree of security importance requiring only one level of restriction and control. In others, the degree of security importance will require further segregation of certain security interests.

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

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

b. Installation commanders will publish a consolidated list of all restricted areas aboard the installation to include tenant command restricted areas. This list will be published annually, and will specify whether or not an area is vital or substantial to national security. This list will be designated for official use only.

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

a. Level 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 the Level Three restricted area constitutes, or is considered to constitute, actual access to the security interest or asset.

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

c. 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 may or may not permit access to a security interest or asset.

d. Restricted areas will be designated as specified below:

(1) Level Three

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

(2) Level Two

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

(b) Aircraft rework areas.

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

(d) Arms, ammunition and explosives (AA&E) storage facilities and processing areas (including gunparks and ammunition supply points). (Additional requirements are outlined in reference (d).)

(e) Fuel depots and bulk storage tanks.

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

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

(h) Tank ramps, compounds, and housing facilities.

(3) Level One

(a) Motor Pools.

(b) Fuel issue points.

(c) Funds and negotiable instrument storage areas.

(d) Provost Marshal Office (PMO) Desk Sergeant/Dispatcher area, ESS monitoring spaces, and Military Working Dog (MWD) facility.

3. Minimum Security Measures Required for Restricted Areas.

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

(1) 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 Manual. Barrier and lighting requirements are set forth in Chapters 5 and 6. Points of ingress will be posted in accordance with paragraph 3006.1 of this Manual.

(2) 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.

(3) 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.

(4) 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 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.

(5) 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.

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

(1) 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 Manual. Barrier and lighting requirements are set forth in Chapters 5 and 6. Points of ingress will be posted in accordance with paragraph 3006.1 of this Manual.

(2) 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). 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.

(3) 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.

(4) 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 access to security interest contained within a Level Two 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.

(5) When secured, 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.

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

(1) 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 Manual. Barrier and lighting requirements are set forth in Chapters 5 and 6. Points of ingress will be posted in accordance with paragraph 3006.1 of this Manual.

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

(3) Controlled ingress and egress.

(4) 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.

(5) When secured, 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.

d. Assets that are considered as vital or important to the overall mission and national security are identified in reference (i). Figure 2-2 from reference (i) is provided in Appendix C. It contains information designed to assist commanders in determining the levels of security that should be provided for various types of assets beyond the standards contained in paragraph 3005.2d of this Manual.

4. 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 activity security officer will ensure they are conducted. Procedures will be coordinated with the cognizant Staff Judge Advocate and approved, in writing, by the installation commander/commanding officer or authorized representative.

5. Limited Waterway Areas. Installation commanders adjacent to waterfront property and waterways, who desire to enhance the security of installation/site, will ensure these areas are designated by proper authority. The following paragraphs and table provide information for commanders required to establish control mechanisms to limit persons, vehicles, vessels and

objects within designated areas. This paragraph describes the different types of limited waterway areas available based on the level of threat.

The U. S. Coast Guard (USCG) and U. S. Army Corps of Engineers (USACE) may when safety, security, or other national interests dictate, control access to and movement within certain areas under their jurisdiction.

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

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

a. The USCG and USACE are the implementing authority under the Ports and Waterway Act of 1972 (PWSA) (33 USC 1221 et seq.),

the Magnuson Act of 1950 (50 USC 191), the Outer Continental Shelf Lands Act (OCSLA) (43 USC 1331 et seq.), and the Deepwater Port Act (33 USC 1501 et seq.).

b. Commanding officers will make every effort to coordinate protection of adjacent waterway areas with the proper agency. Commanding officers will review operations and/or security plans to ensure areas of responsibility/jurisdiction are properly identified. Liaison between security personnel and local Coast Guard officials should be maintained to ensure designation of Limited Waterway Areas and procedural aspects are kept current. The following matrix describes the purpose, major features and application of each type of Limited Waterway Areas.

6. Establishing Limited Waterway Areas. The cognizant 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 USCG, as appropriate. Commanding officers desiring adjacent waterway or waterfront access controls must provide a written request 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 CMC(POS).

7. Non-Restricted Areas

a. A non-restricted area is an area under the jurisdiction of an organization where access is either minimally controlled or uncontrolled. Such an area may be fenced, or open to uncontrolled movement of the general public. An example of a non-restricted area is a visitor or employee parking lot that is open and unattended by guards. After working hours it may be closed, patrolled, and converted to a restricted area. Another example is a personnel office where the general public is authorized access during working hours without being required to check in or register with duty personnel. 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.

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

3006. SIGNS AND POSTING OF BOUNDARIES

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

WARNING
RESTRICTED AREA - KEEP OUT
AUTHORIZED PERSONNEL ONLY

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

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

WARNING
RESTRICTED AREA - KEEP OUT
Authorized Personnel Only

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

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

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

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

U. S. GOVERNMENT PROPERTY
NO TRESPASSING

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

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

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

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

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

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

b. The word "WARNING" will be red.

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

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

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

3007. KEY SECURITY AND LOCK CONTROL. Each Marine Corps organization must establish a strict key and lock control program managed and supervised by the command 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. The Navy Lock and Key Control Guide (Ashore), June 1988, prepared by the Naval Facilities Engineering Service Center, 1100 23rd Avenue, Port Hueneme, CA 93043-4370,is an excellent source for additional data regarding establishing and maintaining a key and lock control program.

1. Key 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 organization security officer. At those organizations where the security and lock program is too small to warrant a subordinate designation, the security officer may assume this function. The key 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.

2. Key Custodian. The head of each major functional area (e.g., department, directorate, etc.) within an organization 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 semiannually. The record of this inventory shall be retained for three years or completion of the next Inspector General's inspection cycle whichever is greater.

3. Central Key Room. Duplicate keys, key blanks, padlocks (key and combination type), and key-making equipment will be stored in a central key room. Access must be controlled and the space must be secured when not in use. Duplicate keys will be provided protection equivalent to the asset/area that original keys are used to secure. Controlled keys (e.g. AA&E, master, and classified material storage area keys) will not be duplicated at any time for any reason nor removed from the installation/ site without prior written consent of the security officer/ provost marshal.

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

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

4. Rotation and Maintenance. Security locks, padlocks, combinations, and lock cores designated as high security shall be rotated from one location to another within the same level areas of protection (e.g., Level Two area locks and cores stay within Level Two areas, etc.) at least annually. Rotation is

accomplished to guard against the use of illegally duplicated keys and for regular maintenance to avoid lockouts or security violations due to malfunctions.

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

6. Key Control. The central keyroom and each key custodian and sub-custodian must develop and maintain a system identifying keys on hand, keys issued, to whom, date and time the keys were issued and returned, and the signatures of persons drawing or returning a security key. Continuous accountability of keys is required.

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

8. Lock Control Seals. Inactive or infrequently used gates must be locked and have seals affixed. The approved seal is the car ball end seal, Military Specification MIL-S-23769C. Security personnel should be instructed that lack of free play (approximately one-eighth inch) indicates the possibility of tampering and a follow-up examination of the seal should be conducted. Seals will be serialized, stored in the same manner as prescribed herein for keys, and all seals will be inventoried annually. The security officer will control placement of entrance seals and account for seal numbers on-hand, issued and used.

9. Procurement of Locks and Padlocks. All locks and padlocks used for low, medium and high security applications will meet

the minimum military specifications for that level of security use. The security officer must approve all security lock and padlock procurements.

10. Lockouts. All lockouts at restricted areas or buildings will be reported to the 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.

3008. CLASSIFIED SECURITY CONTAINTERS, VAULTS AND STRONGROOMS. Security containers, vaults and strongrooms will conform to the specifications contained in reference (b).

3009. SECURITY CHECKS

1. Each organization must establish a system for daily after-hours security checks of restricted areas, facilities, containers, barriers and buildings to detect any deficiencies or violations of security standards. Deficiencies or violations must be reported to the security officer, commanding officer, and PMO. Each deficiency or violation will be reviewed by the organization security officer, and a record maintained of all corrective actions taken. Records of security checks will be maintained for a period of one year.

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

3. All deficiencies, violations, breaches of rules and regulations, and criminal incidents discovered and handled by the security force will be recorded.

3010. PARKING OF PRIVATELY OWNED VEHICLES (POV)

1. 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. Privately owned vehicles 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 MILCON and renovations projects as outlined in Antiterrorism/Force Protection orders and directives. Management of the parking assignments is not a function of the security officer.

2. At activities where parking is allowed inside Level One 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.

3011. TRAFFIC CONTROL. The installation provost marshal will establish a traffic control program in accordance with reference (j).

3012. SECURITY OF SELECTED, SENSITIVE INVENTORY ITEMS, DRUGS, DRUG ABUSE ITEMS AND PRECIOUS METALS

1. The following definitions describe sensitive items:

a. Selected Sensitive Inventory Items. Those items security coded "Q" or "R" in the Defense Integrated Data System (DIDS) that are controlled substances, drug abuse items or precious metals.

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

c. Code "R" Items. Precious metals and drugs or other controlled substances designated as Schedule I or II items per 21 Code of Federal Regulations, Part 1308 (Appendix G).

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

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

3013. SECURITY REQUIREMENTS FOR "R" CODED ITEMS AT BASE/INSTALLATION SUPPLY LEVEL OR HIGHER

1. "R" coded items maintained at base/installation level and higher will be stored in vaults or strongrooms in accordance with reference (b) or 750 pound or heavier General Services Administration (GSA) approved security containers. Smaller GSA approved security containers are authorized but must be securely anchored to the floor or wall. All security containers will be secured with built-in X07 combination locks.

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

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

3014. SECURITY REQUIREMENTS FOR "Q" CODED ITEMS AT BASE/ INSTALLATION SUPPLY LEVEL OR HIGHER

1. The preferred storage for sensitive inventory items coded "Q" is in vaults or strongrooms.

2. Small quantities may be stored in security containers approved for items coded "R". Larger or bulk quantities may be stored in a Level Three restricted area as described in paragraph 3005.3(a)1. The storage area will have an IDS which is connected to a central monitoring station with personnel who can provide rapid armed response to an alarm signal.

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

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

3015. SECURITY REQUIREMENTS FOR "R" AND "Q" CODED ITEMS FOR SMALL UNITS/INDIVIDUALS

1. The preferred storage for sensitive inventory items coded "Q" is in vaults or strongrooms.

2. Small quantities may be stored in security containers approved for items coded "R". Larger or bulk quantities may be stored in a Level Three restricted area as described in paragraph 3005.3(a)1. The storage area will have an IDS which is connected to a central monitoring station with personnel who can provide rapid armed response to an alarm signal.

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

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

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

3016. SECURITY OF FUNDS. Physical security requirements for funds under control of a disbursing officer or stored within a disbursing office are contained in reference (g). Appendix F is provided as a guide.

3017. GOVERNMENT PROPERTY

1. All U.S. Government computers, typewriters, calculators, adding machines, and similar items of 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.

2. Video recorders, televisions, film projectors, radio receivers, and similar items used for mission-related audio-visual Purposes will be stored in spaces where access is controlled during normal duty hours. These items will also be marked with identification tags identifying them as U.S. Government property. After normal duty hours, these items will be locked in a room and security measures implemented.

3. 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.

CHAPTER 4

SECURITY FORCES

CHAPTER 4

SECURITY FORCES

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

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

1. Prevent/deter theft and other losses caused by fire damage, accident, trespass, sabotage, espionage, etc.

2. Protect life, property and the rights of individuals.

3. Enforce rules, regulations and statutes.

4. Detect, deter and defeat terrorism.

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

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

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

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

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

1. Size and location of the installation/site.

2. Geographic characteristics of the installation/site.

3. Mission.

4. Number, type, and size of restricted areas.

5. Use and effectiveness of physical security equipment.

6. Availability of non-organic, supporting security forces.

7. Installation population and composition.

8. Criticality of assets being protected.

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

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

4005. POST REQUIREMENTS AND CONSIDERATIONS

1. Gates. Gates will be limited to the minimum number required to permit expeditious flow of traffic in and out of the installation or activity. Except where justified by consistently heavy traffic throughout the day or by other security considerations, one sentry per gate will normally suffice. Rush hour augmentation manning must be included in post calculations. Using personnel obtained temporarily from mobile posts to man fixed posts reduces emergency response capability.

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

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

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

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

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

1. Special orders for each post which specify the limits of the post, specific duties to be performed, hours of operation, and required uniform, arms, and equipment.

2. Specific instructions in the application and use of deadly force as provided in reference (l), and detailed guidance in the safe handling of weapons.

3. Training requirements for security personnel and designated posts.

4. Security force chain of command.

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

1. The use of force and the safe handling of firearms, to include issue and turn in.

2. Weapons training and qualification as outlined in reference (l).

3. Legal aspects of jurisdiction and apprehension.

4. Mechanics of apprehension, search, and seizure.

5. General and special orders and all aspects of the security force order.

6. Use of security force equipment.

7. Threat specific training (e.g., vehicle bomb searches, terrorism awareness, weapons of mass destruction (WMD) awareness).

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

1. Weapons and Ammunition. Weapons and ammunition will be standard issue items of government property. The use and possession of privately owned weapons by military personnel in the performance of assigned duties is strictly prohibited. Security force personnel will be assigned a service pistol, service rifle, or shotgun while in the performance of their duties, as determined by the installation/organization commanding officer. Requirements for carrying configuration and additional ammunition are provided in reference (l). The commanding officer may authorize the issue of special equipment (shotguns, machine guns, grenade launchers), provided security force personnel have received required weapons training as directed by reference (m).

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

a. Equipped with radios.

b. Configured for the safe transportation of additional passengers and those persons apprehended or detained by security force personnel.

c. Operated by personnel possessing valid U.S. Government Motor Vehicle Operator's Identification Card (SF-46) for all vehicles that they may be assigned to operate as required by TM 11-240.

d. Military police vehicles will conform to requirements identified in reference (n). In addition to the above, military police vehicles will be equipped with law enforcement specific equipment (mobile radios, sirens, code-lights, prisoner security cages, and spotlights/takedown lights). Law enforcement equipment will conform to both federal and state regulations.

3. Communications

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

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

(2) Criticality of assets.

(3) Susceptibility to interference or unauthorized monitoring.

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

(5) Requirement and placement of repeaters.

(6) Terrain and structures.

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

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

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

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 5

BARRIERS AND OPENINGS

CHAPTER 5

BARRIERS AND OPENINGS

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

1. Defining the perimeter of restricted areas.

2. Establishing a physical and psychological deterrent to entry and providing notice that entry is not permitted.

3. Optimizing use of security forces.

4. Enhancing detection and apprehension opportunities by security personnel in restricted and non-restricted areas.

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

5001. TYPES OF BARRIERS. Major types of physical barriers are:

1. Natural, such as mountains, swamps, thick vegetation, rivers, bays, cliffs, etc.

2. Structural, such as fences, walls, doors, gates, roadblocks, vehicle barriers, etc.

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

1. Physical barriers will be established around all restricted areas. The barrier or combination of barriers used must afford an equal degree of continuous protection along the

entire perimeter of the restricted area. When a section or sections of natural/structural barriers provide a lesser degree of protection, other supplementary means to detect and assess intrusion attempts must be used.

2. In cases of a high degree of relative criticality and vulnerability, it may be necessary to establish two lines of physical barriers at the restricted area perimeter. Such barriers should be separated by not less than 30 feet for optimum protection and control. Two lines of barriers should only be used either in conjunction with an 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 electronic security system.

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

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

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

5003. FENCES

1. 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:

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

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

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

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

e. 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.

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

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

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

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

2. Taut Wire Fences. A taut wire fence may be installed as a stand-alone 7-foot fence with 31-inch double outriggers equipped with sensor devices. A three-quarter inch steel cable

will be attached to support posts 30 inches above the ground to stop lightweight vehicles from crashing through the barrier. The sensor system consists of horizontal wires spaced about 4 inches apart and connected to a central detection device tensioned between two anchor devices. Attempts to cut or climb this type fence will generate an alarm at the central monitoring station.

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

5004. 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.

5005. VEHICLE BARRIERS. The use of vehicle barriers such as crash barriers, obstacles, or reinforcement systems for chain link gates at uncontrolled avenues of approach can impede or prevent unauthorized vehicle access. See reference (o) for guidance on exterior barriers. Additionally, the manual entitled "Terrorist Vehicle Bomb Survivability Manual (Vehicle Barriers)" is available from the Naval Facilities Engineering Service Center, 1100 23rd Avenue, Port Hueneme, CA 93043-4370.

5006. INSPECTION OF BARRIERS. Security force personnel will check security barriers at least weekly for defects that would facilitate unauthorized entry. Personnel must be alert to the following:

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

2. Deterioration (corrosion).

3. Erosion of soil beneath the barrier.

4. Loose fittings (barbed wire, outriggers, fabric fasteners).

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

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

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

5007. 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.

5008. CLEAR ZONES

1. An unobstructed area or clear zone will be maintained on both sides of and between permanent physical barriers of restricted and non-restricted areas. Vegetation in such areas will not exceed 6 inches in height.

2. 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.

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

4. In those activities where space on government land is available, but the fence does not meet clear zone requirements in its present location, relocating the fence to obtain a clear zone may not be feasible or cost effective. Some alternatives

to extending the clear zone would be increasing the height of the perimeter fence, extending outriggers, installing double outriggers, and in some cases installing concertina or general purpose barbed tape obstacle to compensate for the close proximity of aids to concealment or access. Where property owners do not object, the area just outside the fence should be cleared to preclude concealment of a person. All fencing will be kept clear of visual obstructions such as vines, shrubs, tree limbs, etc., which could provide concealment for an intruder.

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

6. 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.

7. Commands must ensure that clear zone requirements are addressed in MILCON and renovation projects as outlined in Antiterrorism/Force Protection orders and directives.

5009. 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.

5010. 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.

5011. GATES

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

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

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

4. Vehicular Gates. Vehicular gates when physically practical wi1l 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.

5012. DOORS, WINDOWS, SKYLIGHTS, AND OTHER OPENINGS. Building exterior doors will provide protection commensurate with the requirement for proper protection of the assets accessible through those doors. Unless the width-to-height ratio absolutely eliminates the physical possibility of intruder

entry, openings will be protected by securely fastened 9 gauge wire mesh, framed and permanently bolted to the structure. Such openings are also considered inaccessible to personnel when they are 18 feet or more above ground level and 14 feet or more distant from buildings, structures, etc., outside the perimeter. Protective screens have the additional value of preventing projectiles such as rocks, hand grenades, bombs and incendiaries from being hurled through the windows from outside the perimeter. Hinges to all doors will be located on the interior of the door. In locations where the hinge pin is exposed to the exterior, hinges will be peened, spot welded, or equipped with a hinge secure pin.

5013. SEWERS, CULVERTS, AND OTHER UTILITY OPENINGS. Unless the width-to-height ratio absolutely eliminates the physical possibility of intruder entry (for example, one inch by 6 inches) all utility openings which penetrate the perimeter or restricted area barrier will be protected against surreptitious entry. Protection of these opening may be accomplished by securely fastened bars, grills, locked manhole covers or other equivalent means which provide security commensurate with that of the perimeter or restricted area barrier. Bars and grills across culverts, sewers, storm sewers, etc., create a hazard and are susceptible to clogging. This hazard must be considered during construction planning. All drains/sewers will be designed to permit rapid clearing or removal of grating when required. Removable grates will be locked in place.

5014. UTILITY POLES, SIGNBOARDS, AND TREES. Utility poles, signboards, trees, etc., located outside of and within 15 feet of the perimeter barrier of the activity, present a possible assistance to entry. To reduce this possibility, the perimeter barrier will be staggered to increase the distance to more than 20 feet and may be heightened to the extent necessary to prevent entry. Otherwise, the hazard must be removed. Should these utility poles, signboards, trees, etc., also obstruct the visibility of the guards, they must be at least 20 feet outside the perimeter barriers.

CHAPTER 6

PROTECTIVE LIGHTING

CHAPTER 6

PROTECTIVE LIGHTING

6000. GENERAL. Protective, or security, lighting is an integral part of both the command security and safety posture. This lighting provides a continuing degree of security commensurate with that during daylight hours. It increases the effectiveness of security forces performing their duties and has considerable value as a deterrent to criminal activity. Requirements for protective lighting at an activity are determined by the asset(s)/area(s) to be protected, facility layout, terrain, and weather conditions. In the interest of finding the best possible mix between resource allocation, financial commitment, and effective security, each situation must be carefully studied. The overall goal is to provide the proper environment to perform duties such as identification of badges and personnel at gates, inspection of unusual or suspicious circumstances, etc. Where lighting is impractical, additional compensating measures must be instituted.

6001. GENERAL PRINCIPLES AND GUIDELINES. Paragraph 4.3 of reference (o) provides general principles and guidelines for exterior protective (security) lighting. These guidelines, including Table 25 (Lighting Specification (Foot Candles)), and Table 26 (Illuminated Area Specification) should be applied by activities when determining protective lighting requirements. When protective lighting is installed and used, the following basic principles, in addition to those provided in reference (o) should also be applied:

1. 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.

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

3. Locate light sources so that illumination is directed toward likely avenues of approach and provides relative darkness

for patrol roads, paths and posts. To minimize exposure of security force personnel, lighting at entry points will be directed at the gate and the guard shall be in the shadows. This type of lighting technique is often called glare projection (see paragraph 6002.1a).

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

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

6. Avoid drawing unwanted attention to restricted areas.

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

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

6002. TYPES OF PROTECTIVE LIGHTING SYSTEMS.

1. 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.

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

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

b. Controlled Lighting. Best used when it is necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways, railways, navigable water or airports. The width of the lighted strip can be controlled and adjusted to fit a particular need such as illumination of a wide strip inside a fence. Care should be taken to minimize or eliminate silhouetting or illuminating security personnel on patrol.

2. 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. Lamps with short restart times are essential if this technique is chosen. This technique may offer significant deterrent value while also offering economy in power consumption.

3. 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.

4. Emergency Lighting. May duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies which render the normal system inoperative. It depends on alternative power sources, such as installed or portable generators or batteries.

6003. PROTECTIVE LIGHTING PARAMETERS. It is not the intent of this Manual to prescribe specific protective lighting requirements. Except for minimum standards described in paragraph 6004, 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:

1. Relative value of items being protected.

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

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

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

5. Energy conservation.

6004. MINIMUM STANDARDS

1. 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.

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

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

4. 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.

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

6005. 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.

6006. 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.

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

CHAPTER 7

ELECTRONIC SECURITY SYSTEMS (ESS)

CHAPTER 7

ELECTRONIC SECURITY SYSTEMS (ESS)

7000. INTRODUCTION. Electronic Security Systems 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.

7001. GENERAL. Electronic security systems are used to accomplish the following:

1. Permit more economical and efficient use of security personnel through the employment of mobile responding security forces instead of fixed guard posts and/or patrols.

2. Provide additional controls at critical areas or points.

3. Enhance the security force capability to detect and defeat intruders.

4. Provide the earliest practical warning to security forces of any attempted penetration of protected areas.

7002. ESS DETERMINATION FACTORS. For those facilities requiring ESS, specific regulatory guidance has been provided. In addition to regulatory guidance, the following factors must be addressed to determine the necessity for installation of ESS:

1. Mission.

2. Criticality.

3. Threat.

4. Geographic location of the installation or facility and location of facilities to be protected within each activity or installation.

5. Accessibility to intruders.

6. Availability of other forms of protection.

7. Life cycle costs of the system.

8. Construction of the building or facility.

9. Hours of operation.

10. Availability of a security force and expected response time to an alarm activation.

7003. ESS POLICY

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

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

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

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

5. CMC (POS) 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. This will eliminate the proliferation of alarm system types currently installed at PMO.

a. HQMC (POS) 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. Installations may continue to use current alarm systems. When these systems reach the end of life cycle, they will be replaced with AA&E/flightline compatible systems.

b. In procuring these non-AA&E/flightline systems, installations may, when using local funding, elect to have the Marine Corps ESS TSA install said system, or they may elect to use a contractor of their choice. To maintain system integrity, however, final installation to the PMO annuciator will be accomplished/supervised by engineers and technicians from the Marine Corps ESS TSA.

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

d. In cases where the installation/organization commander determines that an ESS system will annunciate at the PMO, these systems will be compatible with MCESS. Costs of installation will be borne by the command or responsible agency.

e. MCESS technical support may be arranged for installation and maintenance. With prior CMC(POS) approval, local contractors may install and maintain the system provided that

the system and components are compatible with MCESS. Compatibility must be certified by the MCESS TSA prior to the integration/connection to MCESS. Additionally, the MCESS TSA must approve the maintenance plan submitted by the contractor. Compatibility review costs will be borne by the installation.

c. ESS not compatible with MCESS systems will not annunciate at PMO and do not require approval from CMC(POS). These systems will annunciate at an off base location with personnel who notify installation military police of an alarm. These systems do not require coordination with MCESS TSA.

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

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

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

a. If computerized ESS is used, it will be safeguarded against tampering by the operator. Supervisory personnel will regulate operator access levels.

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

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

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

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

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

7004. TYPES OF SYSTEMS

1. Local Alarm. Local alarms actuate a visible and/or audible signal, usually located on the exterior of the facility. Alarm transmission lines do not leave the facility. Response is generated from security forces located in the immediate area. Without security forces in the area, response may only be generated upon report from a person(s) passing through the area or during security checks. Maintenance is conducted through a civilian agency.

2. Central Station. Central station system signals are transmitted to and annunciate in an independent monitoring

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

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

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

7005. MAINTENANCE. Proper maintenance of an ESS is imperative. Systems not properly maintained may fail to detect intrusion and may yield a high number of false/nuisance alarms. Such alarms cause security forces to lose faith in the system and may result in activations being ignored. Maintenance requirements will be established per the manufacturer. At a minimum, all ESS systems will receive semi-annual preventive maintenance service. All performed maintenance will be recorded and records will be maintained for a period of one year. Additionally:

1. Follow recommendations of equipment manufacturers and installers.

2. Consider actual experience with systems installed.

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

4. Testing. All ESS will be tested at least quarterly to ensure systems are functional. In the conduct of these tests, all individual sensors will be tested to determine the continued adequacy of their application. Tests will include an interruption of the AC power source to ensure proper transfer to alternate power sources in order to determine functionality of the source. Test results will be retained for a period of one year. For perimeter and exterior ESS, randomly selected zones should be tested daily. Depending on the type of sensor, such alarm activations could include touching the fence, walking or running over protected ground, or passing through a sensor beam.

7006. TRAINING. Personnel, who operate, perform basic troubleshooting, maintenance, or repairs of ESS will be trained by certified personnel.

1. Marine Corps site representatives will possess MOS 5814.

2. 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 CMC(POS).

7007. MARINE FORCES RESERVE. Because the facilities used by the reserve component are both unique and usually geographically separated from Marine Corps installations, the policies contained in this Manual cannot be strictly applied. Therefore, the Commander Marine Forces Reserve will incorporate the policies of this Manual where applicable. In all other cases, the spirit and intent of this Manual will be adhered to wherever possible. For Marine Corps Reserve Centers, where there is no government response force available, the system may be police connection or central station. Telephone answering services will not be utilized. All requirements for clarification will be addressed to CMC (POS).

APPENDIX A

DEFINITIONS

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

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

b. 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 (l) and qualified with the firearm in accordance with reference (m).

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 Provost Marshal Office (PMO) during increased threat conditions. The auxiliary security force may fall under the control of the Provost Marshal or an officer designated by the Commanding Officer.

e. Commanding Officer. The term commanding officer used throughout this Manual refers to, yet is not limited to, installation commanding generals and commanding officers, organization officers and officers in charge.

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 manual.

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 UN observer, counterintelligence, or similar duties) that exists in a designated country. This billet may make personnel filling it an especially attractive or accessible terrorist target.

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, because of mission sensitivity, ease of access, isolation, and symbolic value, may be especially attractive accessible 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. Loss prevention requires developing trend analyses to plan and implement reactive and pro-active loss prevention measures.

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. Physical security 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. Physical security inspections are normally conducted by the Inspector General of the Marine Corps (IGMC) or as part of the command inspection program and should not be confused with annual physical security surveys as discussed below. Commanding officers will establish local physical security inspection programs for their subordinate commands.

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. For crimes of sabotage see Title 18, United States Code, Sections 2151-2157.

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

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 Manual, pending actions or accomplishment of actions which wi1l result in conformance with the standards. Interim compensatory security measures are required.

APPENDIX B

****CLASSIFICATION****

PHYSICAL SECURITY PLAN

Activity: Date:

1. Purpose. State the purpose of the plan.

2. General. Mission and size of the installation, average population of Marines and family members, overall daily population including civilian personnel.

3. Area Security. Identify overall size of the installation, to include inhabited and uninhabited areas. Identify restricted and non-restricted areas, buildings, and other structures considered critical. Provide requirements for resource protection and established priorities for their protection.

4. Control Measures. Detail established restrictions on ingress/egress into critical areas (e.g., guards, badge systems, etc.) in accordance with applicable orders.

a. Access Control

(1) Installation access control requirements.

(a) Individual

1) Military personnel.

2) Family members.

3) Civilian Employees.

4) Maintenance personnel

5) Contractor personnel.

6) Vendors.

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

(2) Restricted and non-restricted areas.

(a) Restricted area access requirements for individuals:

1) Military personnel.

2) Family members.

3) Civilians.

4) Maintenance.

5) Contractors.

6) Vendors.

(b) Restricted area access requirements for vehicles:

1) Military and government owned vehicles.

2) Privately owned vehicles.

3) Emergency vehicles.

4) Taxis, buses, etc.

b. Material Control

(1) Inbound

(a) Requirements for admission of material and supplies.

(b) Search and inspection of material for possible sabotage/terrorist hazards.

(c) Special controls on delivery of supplies and/or personnel shipments in restricted areas.

(d) Established controlled holding areas and safe havens for classified, AA&E, and hazardous material.

(2) Outbound

(a) Required documentation.

(b) Transfer areas for controlled, classified, AA&E, and hazardous material.

5. Aids to security

a. Protective barriers

(1) Natural.

(2) General.

(a) Fencing.

1) Clear zone requirements.

2) Maintenance.

3) Perimeter ingress/egress points (gates).

4) Gatehouses. (Location, hours of operation, construction)

(3) Specific barriers.

(a) Stationary

1) Type.

2) Current placement.

3) Maintenance requirements.

(b) Mobile

1) Type.

2) Current placement and/or staging area.

3) Deployment schedule.

4) Support requirements for deployment.

5) Maintenance requirements.

b. Protective Lighting

(a) Placement.

(b) Maintenance.

(c) Power failure contingency plan.

(d) Uninterrupted Power Sources.

(e) Emergency Lighting systems.

1) Stationary.

2) Mobile.

a) Staging Area.

b) Maintenance requirements.

c) Deployment schedule.

d) Support requirements for deployment.

c. Electronic Security Systems

(1) Alarm Control Center.

(2) Use and monitoring.

(3) Alarm response policy.

(4) Alarm response drills.

(5) Training requirements.

(6) Component testing requirements.

(7) Component testing schedule.

(8) Maintenance responsibilities.

(9) Power failure contingency plan.

(10) Uninterrupted power sources.

6. Security Forces

a. Table of organization.

b. Tour of duty.

c. Posts.

(1) Stationary.

(2) Mobile.

d. Available resources (e.g., SRT, MWD, CID, Auxiliary.)

e. Equipment.

(1) Weapons.

(a) Training.

(b) Qualification requirements.

(2) Vehicles.

(3) Support Equipment (hand irons, flashlight.)

f. Communications.

(1) Monitoring location.

(2) Authorized users.

(3) Authorized frequencies.

(4) Shared frequencies.

(5) Mobile Assets (vehicle & portable.)

(6) Location of support equipment (repeaters, etc.)

APPENDIX C

PHYSICAL SECURITY THREAT MATRIX

THREAT TYPE	THREAT DESCRIPTION	THREAT EXAMPLE
MAXIMUM	INDIVIDUAL IN ORGANIZED AND TRAINED GROUPS ALONE OR WITH ASSISTANCE FROM AN INSIDER; SKILLED ARMED AND EQUIPPED INTRUDERS WITH PENETRATION AIDS	TERRORISTS AND SPECIAL PURPOSE FORCE; HIGHLY TRAINED INTELLIGENCE AGENTS
ADVANCED	INDIVIDUAL(S) WORKING ALONE OR IN COLLUSION WITH AN INSIDER; SKILLED OR SEMISKILLED WITHOUT PENETRATION AIDS	HIGHLY ORGANIZED CRIMINAL ELEMENTS; TERRORISTS OR PARAMILITARY FORCES; FOREIGN INTELLIGENCE AGENTS WITH ACCESS
INTERMEDIATE	INDIVIDUAL(S) OR INSIDER(S) WORKING ALONE OR IN SMALL GROUPS; SOME KNOWLEDGE OR FAMILIARITY OF SECURITY SYSTEM	CAREER CRIMINALS; ORGANIZED CRIME; WHITE COLLAR CRIMINALS; ACTIVE DEMONSTRATORS; COVERT INTELLIGANCE COLLECTORS; SOME TERRORIST GROUPS
LOW	INDIVIDUAL(S) OR INSIDERS WORKING ALONE OR IN A SMALL GROUP	CASUAL INTRUDERS; PILFERERS AND THIEVES; OVERT INTELLIGENCE COLLECTORS; PASSIVE DEMONSTRATORS

DOD ASSET PRIORITIZATION

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
A INTEGRATED ELECTRONIC SECURITY SYTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, ACCESS DELAY AND DENIAL SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED IMMEDIATE RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE WILL RESULT IN GREAT HARM TO THE STRATEGIC CAPABILITY OF THE UNITED STATES	NUCLEAR AND CHEMICAL WEAPONS AND ALERT/MATED DELIVERY SYSTEMS CRITICAL COMMAND,CONTROL, COMMUNICATIONS FACILITIES AND SYSTEMS CRITICAL INTELLIGENCE GATHERING FACILITIES AND SYSTEMS PRESIDENTIAL TRANSPORT SYSTEMS NUCLEAR REACTORS AND CATEGORY I AND II SPECIAL NUCLEAR MATERIALS RESEARCH, DEVELOPMENT, AND TEST ASSETS

APPENDIX D

INSTRUCTIONS FOR PREPARATION AND DISTRIBUTION OF PHYSICAL SECURITY SURVEY

1. GENERAL. The following instructions are intended to provide guidance for the uniform preparation and distribution of physical security surveys.

2. BLOCK PREPARATION INSTRUCTIONS. Each block appearing in the United States Marine Corps Physical Security/Crime Prevention Survey (NAVMC 11121), identifies, controls and records each survey and therefore will be filled in completely. A NAVMC 11121 example is located on PAGE D-7. The blocks listed below identify required information. Provided examples are not all inclusive.

Block 1 - Date. This block is completed on the date of final typing and should be entered as follows: day, month and year.

Block 2 - Status. Completed.

Block 3 - Survey Control Number. This block contains the control date of the survey, identification of the organization (Monitored Command Code (MCC)) conducting the survey, survey number, and project code identifier (Physical Security (PS), Crime Prevention (CP), Marine Activity (MA), Navy Activity (NA), etc.). (Example: 3AUG00-008-0001-PSMA)

Block 4 - Inspecting Unit. The provost marshal’s office preparing the physical security/crime prevention survey. (Example: Provost Marshal Office, Marine Corps Base Quantico, VA.)

Block 5 - Requesting Unit. This block contains the title of the commanding officer of the organization requesting the survey. (Example: Commanding Officer, Headquarters and Service Battalion, Marine Corps Base, Quantico, VA.)

Block 6 - Organization and Address of Unit Inspected/ Surveyed. Organization, activity or area to be surveyed; (Example: H&S Battalion Armory, Bldg 2171, MCB Quantico, VA.)

Block 7 - Distribution. An original and one copy will be typed and disseminated as follows:

a. Original - Commanding Officer of activity surveyed.

b. File - Local installation provost marshal office.

Block 8 - Type of Survey. Surveys will be titled "Physical Security."

Block 9 - References. List all references.

Block 10 - Basis for Survey. (Example: As set forth in references (a) and (b), the provost marshal directed that a physical security survey be conducted (date, building, unit/activity, and base/station.) Contact was made with (grade, name, and title) and a survey was initiated.)

Block 11 - Synopsis of Survey. This is a summation of deficiencies identified during the survey and will serve as the basis for prioritizing corrective action should be accomplished. This block may also be used to provide recommended actions.
(Example: The following deficiencies were identified during the course of the survey and require corrective action:

1. The intrusion detection system has no emergency backup power.

Block 12 - Data Affecting the Survey Site. This includes a canvass of local provost marshal office crime analysis records affecting the survey site and surrounding area. (Example: The following crimes have been reported in the vicinity of Bldg. 25 during the previous 12 month period: (3) Larceny of Private Property.)

Block 13 - Building and Area. Identify the building by number and type of construction (stories and type of material) and location (describe surrounding area, industrial, business,

residential, barracks, etc., and location in relation to the installation). (Example: Building 2111 is a three-story building constructed of brick veneer. The building is located in a business section in the southwest area of the installation.)

Block 14 - Physical Security Barriers. Address each category separately and fully.

1. Walls - Describe material, type of construction, and any deficiencies. (Example: Exterior walls for the facility are constructed of eight-inch mortar reinforced brick. Interior walls are constructed of plaster mounted on metal studs.)

2. Doors - Describe number, material, type of construction, and any deficiencies. (Example: There are five doors in the exterior walls of this facility. The main entrance exit door is constructed of 1-3/4 inch hollow metal secured to the walls in a metal frame, hinge pins are located on the interior of the door. (describe locking devices in Block 15, section d)).

3. Floor - Describe material, type of construction, and any deficiencies. (Example: The floor of this facility is constructed of an eight inch poured concrete pad.)

4. Ceiling/Roof - Describe material, type of construction, and any deficiencies. (Example: The ceiling of the facility is constructed of metal I beams with an exterior covering of tar and gravel.)

5. Windows/Other Openings - Describe number, material, type of construction, and any deficiencies. (Example: There are sixteen windows in the exterior walls of the facility. The windows are constructed of standard pane glass in wood frames, secured to the walls in metal frames (describe locking devices in Block 15, section d)).

6. Natural - Describe and indicate whether there are natural barriers.

Block 15 - Physical Security Aids, Equipment and Devices. These items provide protection in relationship to the

sensitivity of the property being protected. Address each category separately.

1. Lighting (Exterior/Interior) - Describe type, location (exterior location in relation to the facility), mount type, and any deficiencies. Include a night light survey. (Example: There is an incandescent light fixture located above the main entrance/exit door. There are exterior building mounted high pressure sodium fixtures located on the east and west walls.)

2. Fencing - Describe type, type of construction, number of personnel/vehicle gates in the fence line, and any deficiencies. (Example: There is a fence surrounding the facility. The fence is constructed of nine-gauge chain link and is seven feet high with an outrigger. There are four personnel and one vehicle gate within the fenceline.)

3. Locks - Describe type for windows and doors, and any deficiencies. (Example: The main entrance/exit door is secured with a mortise lock supported by a deadbolt assembly with a one-inch throw. Windows for the facility are secured with a crescent sash lock.)

4. Vaults/Safes/Containers - Describe to include number in the facility, make, type, weight, use, and any deficiencies. (Example: There is one safe in use in the facility. The safe is a Mosler brand five-drawer safe weighing approximately 750 pounds. The safe is utilized to store negotiable instruments).

5. Electronic Security System (ESS) - Describe type, interior components, where the system annunciates, and any deficiencies. (Example: There is an intrusion detection system in use in this facility. The interior system is comprised balanced magnetic switches and passive infrared motion detectors. There is also a duress switch utilized in the facility. The system annunciates at the Provost Marshal Office, which is staffed on a 24-hour basis.)

6. Key and Lock Control - Describe the program and any deficiencies. (Example: Key control has been established for this facility. All keys to the facility are signed out in a key control logbook that is maintained by the SNCOIC.)

7. Security Force - Describe. (Example: There are no guards posted at this facility. Military Police provide a response to all alarms received from this facility. Military police have been provided training concerning the use of force in accordance with reference ( ).

Note: Provide adequate protection in relationship to the sensitivity of the property being protected.

Block 16 - Preventive Measures and Procedures. Address each category separately and provide recommendations accordingly.

1. Security Orders/SOP. Will include site specific security orders that address security in conjunction with MCO 5530.14, and any deficiencies. (Example: Reference ( ) provides detailed information concerning security of disbursing currency and negotiable instruments).

2. Access control. Describe facility access control to include locally alarm fire doors, buzzer assemblies, and any deficiencies. (Example: Access to the facility is the responsibility of and controlled by personnel assigned to the facility. Two of the doors are provided additional protection by local "fire door" alarms that annunciate in the event the door is opened).

3. Property accountability. Includes inventories required by specific directives, installation CMR requirements, and any deficiencies. (Example: Inventories on all currency and negotiable instruments are conducted by disinterested personnel on a monthly basis. Plant property is inventoried on a semi-annual basis.)

4. Robbery/burglary procedures. Addresses installation crime prevention orders, local SOPs that identifies Robbery/Burglary Procedures, and any deficiencies. (Example: Robbery/Burglary procedures are outlined in references ( )
and ( ).

5. Crime/Loss Prevention Awareness Training. Identify training provided by the command or by the Provost Marshal’s

Office, and any deficiencies. (Example: Crime/Loss Prevention training is conducted on an annual basis in conjunction with the Provost Marshal Office Crime Prevention Office.)

Block 17 - Action/Comment. Example:

1. Questions concerning comments or recommendations contained in this report may be addressed to the Provost Marshal's Office Physical Security Section, extension 614-1414.

2. Action taken as a result of this survey will be forwarded to the installation Provost Marshal's Office, via the chain of command, within 90 days of receipt.

Block 18 - Typed Name and Grade of Inspector. Name of individual who conducted the survey should be entered as first and middle initials, last name and grade. (e.g., G.E. Davis, Sgt.)

Block 19 - Typed Name and Grade of Approving Officer. Name of officer approving the survey should be entered as first and middle initials, last name and grade; e.g., P.M. Grow, Capt.

3. IDENTIFIED DEFICIENCY REQUIREMENTS. For all deficiencies identified in a survey category, the requirement and the applicable reference should listed. (Example: Requirement - The intrusion detection system has no emergency backup power. Reference (a), paragraph 0803 requires that all IDS be provided emergency backup power.)

4. RECOMMENDED CORRECTIVE ACTIONS. Physical Security Inspectors identify deficiencies and provide the requirement as directed by applicable orders. Unit Commanders are given the latitude to correct identified deficiencies as long as those corrective measures employed meet the requirements of the applicable orders. Recommended Corrective Actions are just that, a recommendation that will assist the Unit Commander in alleviating the deficiency and coming in compliance with the applicable order. (Example: Recommendation - A Key Control log Book should be utilized vice single sheet Key Control log in order to prevent the surreptitious removal of log pages.)

5. SURVEY COVER SHEET. The Survey Cover Sheet is intended to provide a means of control during the distribution, filing, and disposal of Crime Prevention/Physical Security Surveys. Each survey will be accompanied by a Survey Cover Sheet. A Survey Cover Sheet example is located on PAGE D-10.

PHYSICAL SECURITY SURVEY EXAMPLE

{li P5530143.gif:Physical Security Survey Example}

PHYSICAL SECURITY SURVEY EXAMPLE (CONTINUED)

SURVEY CONTROL NUMBER *(See Block 3 For Guidance)*

BUILDING AND AREA

(See Block 13 For Guidance)

PHYSICAL SECURITY BARRIERS

(See Block 14 For Guidance)

1. Walls -
2. Doors -
3. Floor -
4. Ceiling/Roof -
5. Windows/Other Openings -
6. Natural -

PHYSICAL SECURITY AIDS, EQUIPMENT, AND DEVICES

(See Block 15 For Guidance)

1. Lighting (Exterior/Interior) -
2. Fencing -
3. Locks -
4. Vaults/Safes/Containers -
5. Electronic Security System (ESS) -
6. Key and Lock Control

PAGE 2 OF 3

PHYSICAL SECURITY SURVEY EXAMPLE *(CONTINUED)*

SURVEY CONTROL NUMBER *(See Block 3 For Guidance)*

7. Security Force -

PREVENTIVE MEASURES AND PROCEDURES

(See Block 16 For Guidance)

1. Security Orders/SOP -

2. Access Control -

3. Property Accountability -

4. Robbery/Burglary Procedures -

5. Crime/Loss Prevention Awareness Training -

ACTION/COMMENT

(See Block 17 For Guidance)
PAGE 3 OF 3

PHYSICAL SECURITY SURVEY COVER SHEET EXAMPLE

WARNING

CRIME PREVENTION SURVEY

PHYSICAL SECURITY SURVEY

THE ATTACHED DOCUMENTATION IS A REPORT FROM THE
PHYSICAL SECURITY/CRIME PREVENTION SECTION

This document must not be left unattended or where an unauthorized person may have access to it. When not in use, it must be stored in a safe place. While this document is in your possession, it is your responsibility that the information contained therein is not released to unauthorized persons. Requests for access to or disclosure of the attached document(s) must be referred to the originating command's Criminal Investigation Division Officer.

DATE:

SURVEY CONTROL NO.:

FROM:

TO:

1. THIS DOCUMENT IS FURNISHED FOR YOUR INFORMATION OR/AND ACTION AS DEEMED APPROPRIATE.

2. WHEN THIS DOCUMENT IS NO LONGER NEEDED IT SHOULD BE DESTROYED BY BURNING OR SHREDDING.

☐ Releasing Authority

FOR OFFICIAL USE ONLY

IF CLASSIFIED - OPNAVINST 5510.1 APPLIES

MCB FORM 5530/3 FEBRUARY 1997 (EF)

APPENDIX E

WAIVER AND EXCEPTION FORMAT

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

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

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

c. The characters after the W or E will represent subsequent numbers of request during the calendar year beginning with 01. Waiver and exception numbers will run sequentially, i.e., W-01-99, W-02-99, W-03-99 and E-01-99, E-02-99, E-03-99.

d. Original waiver and exception numbers will be utilized for all extension requests. Subsequent extension requests will be identified by successive letters of the alphabet beginning with A, i.e., W-01A-99, E-02C-99, etc.

EXAMPLE: M02222-E01-99

M - Marine Corps Organization
02222 - Unit Identification Code
E - Identifies an exception request
01 - Identifies initial exception request (Second request would read E01A, third request E01B, etc.)
99 - 1999 (year initial exception was requested)

2. WAIVER FORMAT

Line 1 - Waiver number.

Line 2 - Specific statement of actual requirement with reference to chapter, section, and paragraph in the applicable security manual which cite standards which cannot be met.

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

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

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

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

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

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

Line 9 - Point of contact to include name, rank, autovon and commercial phone numbers.

3. EXCEPTION FORMAT

Line 1 - Exception number

Line 2 - Statement of the specific requirement with reference to chapter, section, and paragraph in the applicable security manual which cite standards which cannot be met.

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

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

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

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

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

MARINE CORPS PHYSICAL SECURITY PROGRAM MANUAL

APPENDIX F

SECURITY SURVEY GUIDE FOR DISBURSING FACILITIES

DOD 7000.14R

DOD FINANCIAL MANAGEMENT REGULATION, VOLUME 5 CHAPTER 3

1. Has 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? (par 030302A(2))

2. Does the commander conduct periodic reviews of the program for adequacy of current security measures? (par 030302A(3))

3. Are all fund transfers coordinated and conducted with military police and/or armed personnel? (par 030302A(4))

4. Are deputies, agents, cashiers, and/or custodians each provided a separate secure container? (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?
(par 030302B)

6. Is vault access limited to only authorized personnel?
(par 030302B(1))

7. If a vault day gate is utilized, have keys been issued to only authorized personnel? (par 030302B(1))

8. Are windows and doors kept to a minimum and barred and/or locked at all times? (par 030302B(3)

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? (par 030302B(4))

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? (par 030302B(5))

11. Has responsibility for receipt, holding, and final distribution of checks been assigned in writing?(par 030302B(6))

12. Has the Disbursing Officer provided written and oral instructions to all deputies, agents, cashiers, and custodians concerning the proper care and handing of cash and other accountable docments? Have all personnel signed affadavits attesting to receipt of these instructions? (par 030302B(9))

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? (par 030302B(10))

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? (par 030302B(11))

15. Are all fund containers visible to the exterior of the office, illuminated to allow observation from security patrols? (par 030302B(12))

16. Are the combinations of each vault, safe, and fund container changed at least every 6 months and upon releif, transfer, separation, or discharge, of the accountable individual?
(par 030302B(13))

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? (par 030302B(13))

18. Is the combination to the Disbursing Officer’s safe maintained in a signed, sealed envelope by the commander or command security officer? (par 030302B(13))

19. Is a signed and dated record of all safe combination changes maintained in each safe or container? (par 030302B(14))

20. Is the dial to each vault, safe, or container shielded to limit the possibility of the combination being observed (par 030302B(15))

21. Is the name and phone number of the accountable individual posted on the interior of the vault, safe, or container? (par 030302B(16))

22. Has a key control been established per MCO P5530.14, Chapter 3, paragraph 3007?

23. Has a key custodian been assigned per MCO P5530.14, Chapter Chapter 3, paragraph 3007?

24. Are keys to the individual work space or disbursing office strictly controlled? (par 030302B(17))

25. Is a key control logbook maintained to identify individuals assigned keys, when they were issued, and when they were surrendered? (par 030302B(17))

26. Is an Intrusion Detection Sytem (IDS) in use? Is the existence of the IDS system posted? (par 030303B)

27. Is the IDS protected against tampering, bypassing, and foolproofing? (par 030303C)

27. Is the IDS tested quarterly per MCO P5530.14, Chapter 7, paragraph 7005?

28. Is the disbursing office conspicuously posted as a restricted area per MCO P5530.14, Chapter 3, paragraph 3006?

29. Do all fund containers meet requirements? (par 030304)

APPENDIX G

SECURITY SURVEY GUIDE FOR BUSINESSES

AND CASH AND MERCHANDISE SECURITY

1. Has the commanding officer responsible for security issued orders or directives covering all phases of security?

2. Has an officer/SNCO been appointed with the responsibility of security?

3. Is exterior security adequate (e.g., guards, lights, fences, vegetation, etc.)?

4. Are all accessible openings adequately secured (e.g., doors, windows, vents, skylights, etc.)?

5. Are security screens, bars, and gates properly mounted and in good state of repair?

6. Are exterior doors of solid construction or adequately protected?

7. Are exposed hinge pins welded or penned to prevent removal?

8. Are doors exiting to the outside provided with double locking devices?

9. Are locks, sliding bolts, hasps and receivers for padlocks and crossbars properly installed?

10. Are soft walls between exchange premises and boiler rooms‘ outside rest rooms, or adjoining buildings adequately reinforced?

11. Are air ducts, heating shafts, trap doors or similiar apertures penetrating exterior walls, roof, or floor adequately secured?

12. Are intake/exhaust fans or air-conditioners installed in outer walls adequately secured to prevent removal?

13. Are crawl spaces beneath buildings and in the interior between roof and ceiling adequately secured?

14. Are fire exit doors equipped with a day alarm or similiar warning devises?

15. Are stockrooms/service doors kept locked when not in use?

16. Is the activity protected by an operable intrusion detection system?

17. What are the number/causes of false/nuisance alarms in the past 12 months?

a. User error.

b. Weather.

c. Other.

INTERNAL SECURITY

1. Do employees enter/exit through one designated door?

2. Are adequate locker facilities available and used by employees?

3. Are adequate background checks made on all employees?

4. Are critical items properly secured during non-operational hours?

5. Are critical items properly safeguarded during operational hours?

6. Are customer identification requirements complied with?

7. Is adequate control and supervision being maintained over janitorial/custodial personnel?

8. Are venders, rack jobbers, etc., accompanied by responsible activity personnel when on exchange premises?

GENERAL SECURITY

1. Are frequent accountability control training sessions conducted?

2. Are employees aware of their responsibilities for accountability control?

3. Are employees cognizant of standing operating procedures?

4. Is an effective orientation program for newly hired personnel in effect?

MERCHANDISE/CASH SECURITY

1. Are incoming shipments carefully checked for signs of pilferage, damage, etc.?

2. Are merchandise shipping and receiving procedures in compliance with directives?

3. Are van-type exchange/contracter trucks used exclusively to transport merchandise?

4. Are employee activities in the facility supervised during nonoperating hours?

5. Does management conduct spot checks of the premises to discourage concealment of merchandise by employees?

6. Are friends and relatives of employees discouraged from loitering in the facility?

7. Are trash disposal areas spot checked for evidence of pilferage?

8. Are boxes, cartons, and containers flattened before disposal?

9. Are incoming/outgoing shipments properly checked/documented?

10. Are all shipments recorded immediately upon receipt?

11. Are pricing procedures in conformance with directives?

12. Are employee’s personal effects kept in a location other than the selling/stock area?

13. Are employees prohibited from making sales to themselves?

14. Are employee’s purchases made in the presence of the manager or designee?

15. Are employee’s purchases bagged and stapled and is a cash register receipt affixed to the bag?

16. Are employee purchases stored in a central location and spot checked by management?

17. Does each sales clerk have a separate cash drawer?

18. Are sales rung up immediately?

19. Does each sale clerk close the cash drawer immediately after sales?

20. Are zero rings strictly controlled and affixed to daily clerk reports?

21. Are customer purchases bagged and stapled?

22. Are cash register receipts affixed to customer purchases?

23. Are cash register readings made only by the manager or the designee?

24. Are overings authenticated by management?

25. Are unannounced cash register spot checks made?

26. Are excessive or recurring cash discrepancies investigated by management?

27. Do sales personnel lock their register drawers and remove the keys when leaving the cash register unattended?

28. Are cash register areas spot checked by management for evidence of manipulation?

29. Is the safe(s) combination entrusted to an accountable individual and not divulged or entrusted to any other person or written down anywhere?

30. Are the safe combination changed at least once every 6 months or upon transfer of the accountable individual?

31. Are the combination dials of the fund containers concealed or shielded from the view of all except the accountable individual?

32. Is the name and telephone number of the responsible individual affixed to the inside of the funds container?

33. Whenever possible, are funds containers located in a single room where security standards can be concentrated?

34. Are public funds, documents, and other records stored separately from all cash material?

35. Are all funds containers weighing less than 750 pounds or on wheels secured to prevent movement?

36. Are all fund containers that are visible from the exterior illuminated at night?

37. Are all transactions conducted from behind a physical barrier (e.g., cage, counter or room)?

38. Are work areas where cash is handled conspicuously marked "RESTRICTED AREA AUTHORIZED PERSONNEL ONLY?"

39. Are adequate security measures provided to cash transfers and escort/courier service?

40. Are there emergency reaction procedures/plans established for burglary, robbery, fire alarms, and bomb threats?

APPENDIX H

SECURITY SURVEY GUIDE FOR WAREHOUSES

1. Has a command security officer been appointed in writing?

2. Are hinges to doors non-removable or provided with inside hinge protection?

3. Are high value dollar, sensitive, and highly pilferable items protected with approved locking devise?

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 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?