DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO
OPNAVINST 5530.14C
N09N
10 December 1998

OPNAV INSTRUCTION 5530.14C

From: Chief of Naval Operations
To: All Ships and Stations (less Marine Corps field addressees not having Navy personnel attached)

Subj: NAVY PHYSICAL SECURITY

Encl: (1) Navy Physical Security Manual

1. Purpose. To issue revised physical security and loss prevention policy and guidance concerning uniform standards for safeguarding warfighting assets and war material at Navy shore installations and activities. This instruction is a complete revision and must be read in its entirety.

2. Cancellation. OPNAVINST 5530.14B.

3. Scope. Enclosure (1) addresses physical security and loss prevention responsibilities, and standards for safeguarding personnel, property, and material at Navy shore installations and activities.

4. Discussion. To be effective, physical security functions must be carried out by properly trained and equipped personnel. It is the commanding officer's responsibility to ensure that the command security posture is accurately assessed and security resources are appropriate to execute these programs.

5. Responsibilities

a. Commanding officers are responsible for physical security and loss prevention within their commands. The security officer as the designated representative of the commanding officer is responsible for planning, implementing, enforcing and supervising the physical security program of the command.

b. Department of the Navy Echelon 2 and subordinate commanders are responsible for overseeing implementation of this instruction to include checking for compliance by their subordinate activities and by promoting use of physical security resources on a regional basis where appropriate and feasible.

6. Applicability. This instruction is applicable to all Navy shore activities, installations, headquarters commands, deployable units stationed ashore, reserve components, and all Navy military and civilian personnel employed/located thereon.

7. Action

a. Director, Antiterrorism and Force Protection (CNO (N34)) under the Deputy Chief of Naval Operations (Plans, Policy and Operations) is the focal point for force protection and naval operations.

b. The Special Assistant for Naval Investigative Matters and Security (Chief of Naval Operations ((CNO) (N09N)) will develop physical security policy and oversee its implementation.

c. Director, Naval Criminal Investigative Service is assigned coordination and program management responsibilities for physical security and antiterrorism programs, and will provide advice and assistance to commanders to enable them to develop and maintain effective physical security and antiterrorism programs.

d. The Special Assistant for Inspection Support (CNO (N09G)) will ensure reviews are conducted as part of the Navy command inspection program, to determine compliance with the requirements contained in enclosure (1).

e. The Director of Naval Training (CNO (N7)) will ensure that:

(1) Marksmanship and antiterrorist training is included in the Master-at-Arms "A" Course and the Navy Law Enforcement Specialist Course curricula.

(2) Recruit training and officer accession courses include watch qualification in pistol, rifle, and shotgun fire; watch standing and terrorism awareness training.

(3) Training is available for security officers, such as the Navy Security Officer Course.

f. Naval base and station commanding officers, and other host/separate activities (referred here as installation commanding officers) will integrate security forces at major installations, including integration on a regional basis where appropriate and practical, to ensure continuity of purpose in providing effective defense of installations and associated areas of responsibility.

g. Commanding officers at all echelons will evaluate the physical security programs of subordinate activities, including headquarters commands, and ensure compliance with enclosure (1).

8. Reports. The reporting requirements contained in appendix IV are exempt from reports control in accordance with SECNAVINST 5214.2B.

DAVID L. BRANT
Special Assistant for Naval Investigative Matters and Security

Distribution:
SNDL Parts 1 and 2

Navy

Physical Security Manual

TABLE OF CONTENTS

CHAPTER 1 - INTRODUCTION		PAGE
0100	- References and Guidance	1-1
0101	- Definitions	1-1
0102	- Purpose	1-1
0103	- Objectives	1-1
0104	- Scope	1-2
0105	- Physical Security Program	1-2
0106	- Security Responsibilities	1-3
0107	- Chief of Naval Operations	1-3
0108	- Fleet Commanders in Chief/Echelon 2 Commanders/Other Echelons of Command	1-3
0109	- The Commanding Officer	1-4
0110	- The Security Officer	1-5
0111	- Organizational Relationships	1-6
0112	- The Security Problem	1-6
0113	- The Security Management Philosophy	1-6
0114	- Command Physical Security Review and Assessment	1-7
0115	- Installation Physical Security Review and Assessment	1-9
0116	- Regional Physical Security Review and Assessment	1-9
0117	- Physical Security Surveys	1-10
0118	- Vulnerability Assessments	1-10
0119	- Threat Assessments	1-11
0120	- New Construction	1-11
0121	- Facility Modifications	1-11
0122	- Navy Military Construction Projects	1-12

		PAGE
0123	- Security of Leased Facilities	1-12
0124	- Activity Upgrade Requirements/ Waivers/Exceptions	1-12
CHAPTER 2	- **SECURITY PLANNING**	
0200	- General	2-1
0201	- Physical Security Plan Content	2-1
0202	- Planning Process	2-3
0203	- Planning Considerations	2-4
0204	- Physical Security Performance Goal, DOD Threat Matrix, and DOD Assets Prioritization	2-5
0205	- Threat Assessments	2-6
0206	- Risk Management	2-6
0207	- Crisis Situations	2-6
0208	- Sabotage	2-10
0209	- Terrorism	2-10
0210	- Threat Conditions (THREATCONs) for Combating Terrorism	2-10
0211	- Coordination	2-10
CHAPTER 3	- **PART ONE: PHYSICAL SECURITY MEASURES**	
0300	- Security Measures	3-1
0301	- Antiterrorism and Force Protection Measures	3-1
0302	- Security of Funds	3-1
0303	- Loss Reporting	3-1
0304	- Key Security and Lock Control	3-2
0305	- Security Checks	3-2

		PAGE
	- **PART TWO: SECURITY OF AIRCRAFT, SHIPS IN PORT, AND OTHER WEAPON SYSTEMS AND PLATFORMS ASHORE**	
0306	- General	3-3
0307	- Policy	3-3
0308	- Aircraft Security Planning	3-3
0309	- Transient or Deployed Aircraft	3-4
0310	- Other Situations	3-4
0311	- Emergency Situations	3-5
0312	- Pierside Protection of Ships	3-5
0313	- Harbor Surveillance and Waterside/ Waterway Security	3-5
	- **PART THREE: PROTECTION OF BULK PETROLEUM PRODUCTS**	
0314	- General	3-7
0315	- Policy	3-7
0316	- Security Planning and Liaison	3-7
0317	- Physical Security Inspections	3-7
	- **PART FOUR: SECURITY OF COMMUNICATIONS SYSTEMS**	
0318	- General	3-8
0319	- Policy	3-8
0320	- Responsibilities	3-9
0321	- Mobile Communications Systems	3-10
	- **PART FIVE: SECURITY OF MATERIEL**	
0322	- General	3-11
0323	- Policy	3-11
0324	- Responsibilities	3-11
0325	- Controlled Substance Inventory	3-12

		PAGE
0326	- Security Requirements for "R" Coded Items at Base and Installation Supply Level or Higher	3-12
0327	- Security Requirements for "Q" Coded Items at Base and Installation Supply Level or Higher	3-12
0328	- Security Requirements for "R" and "Q" Coded Items Below Base and Installation Level (i.e., Small Unit/Individual)	3-12
0329	- Loss Prevention Measures	3-13
CHAPTER 4	- **THE SECURITY FORCE**	
0400	- General	4-1
0401	- Functions of the Security Force	4-1
0402	- Size of the Security Force	4-2
0403	- Determination of Posts	4-2
0404	- Security Force Orders	4-3
0405	- Arming	4-3
0406	- Use of Force Including Deadly Force	4-4
0407	- Privately-Owned (Personal) Weapons Prohibited	4-4
0408	- Composite Security Force	4-4
0409	- Marine Corps Security Forces (MCSF)	4-4
0410	- Civilian Members of a Commanding Officer's Security Force	4-5
0411	- Augmentation of Security Force for Emergencies	4-5
0412	- Auxiliary Security Forces (ASF)	4-6
CHAPTER 5	- **INSTALLATION ACCESS AND CIRCULATION CONTROL**	
0500	- General	5-1
0501	- Policy	5-1
0502	- Installation Access	5-2

		PAGE
0503	- Access Authorization and Control System Requirement	5-2
0504	- Emergency Planning	5-2
0505	- Area Protection and Control	5-3
0506	- Water Boundaries	5-4
0507	- Enforcement of Movement Control	5-4
0508	- Signs and Posting of Boundaries	5-5
0509	- Vehicle Movement Control	5-5
0510	- Parking of Privately Owned Vehicles	5-5
0511	- Administrative Inspection of Vehicles	5-5
0512	- Special Precautions	5-6
0513	- Control and Accountability of Personal Weapons	5-6
CHAPTER 6	**- BARRIERS AND OPENINGS**	
0600	- The Purpose of Physical Barriers	6-1
0601	- Types of Barriers	6-1
0602	- General Considerations	6-1
0603	- Fences	6-2
0604	- Walls	6-2
0605	- Temporary Barriers	6-2
0606	- Clear Zones	6-2
0607	- Inspection of Barriers	6-3
0608	- Restricted Area Perimeter Openings	6-4
0609	- Vehicle Barriers	6-4
CHAPTER 7	**- PROTECTIVE LIGHTING**	
0700	- General	7-1
0701	- General Principles and Guidelines	7-1

		PAGE
0702	- Protective Lighting Parameters	7-2
0703	- Emergency Power	7-2
0704	- Wiring System	7-2
0705	- Protection - Controls and Switches	7-3
CHAPTER 8	- **ELECTRONIC SECURITY SYSTEMS**	
0800	- Purpose	8-1
0801	- ESS Determination Factors	8-1
0802	- Intrusion Detection System Policy	8-1
0803	- Maintenance	8-3
0804	- Closed Circuit Television	8-3
0805	- Electronic Access Control Systems Using Magnetic Stripes	8-4
CHAPTER 9	- **PART ONE: SECURITY EDUCATION AND TRAINING**	
0900	- Security Education Program	9-1
	- **PART TWO: SECURITY FORCE TRAINING**	
0901	- General	9-3
0902	- Duties and Responsibilities	9-3
0903	- Training Requirements	9-3
0904	- In-Service Training Program	9-4
0905	- Specialized and Advanced Training	9-4
0906	- Firearms Proficiency Training	9-4
0907	- Contract Guard Training	9-5
CHAPTER 10	- **SECURITY FORCE COMMUNICATIONS**	
1000	- General	10-1
1001	- General Requirements	10-1
1002	- Communications Equipment	10-1

CHAPTER 11 - SECURITY DEVICES AND EQUIPMENT		PAGE
1100	- General	11-1
1101	- Security/Law Enforcement Vehicles	11-1
1102	- Firearms and Ammunition for Security Forces	11-4
1103	- Camouflage Utility Uniform and Protective Equipment	11-5
1104	- Military Working Dogs	11-5
1105	- Security Badges	11-5

APPENDIX I	References
APPENDIX II	Definitions
APPENDIX III	Duties of Security Officer
APPENDIX IV	Waivers and Exceptions
APPENDIX V	Auxiliary Security Force Minimum Training Requirements
APPENDIX VI	Restricted Areas and Limited Waterway Areas
APPENDIX VII	Signs and Posting of Boundaries
APPENDIX VIII	Physical Security/Law Enforcement Phase I (Basic) Minimum Training Standards
APPENDIX IX	Annual Phase II (In-Service) Training Program

CHAPTER 1

INTRODUCTION

0100. REFERENCES AND GUIDANCE. Appendix I lists references (a) through (ae) which are cited in this manual.

0101. DEFINITIONS. For the purpose of this manual, definitions in appendix II apply. The language in this manual separates mandatory standards, measures, or actions from recommended measures or actions.

a. Directive words (e.g., shall, will, must, etc.) indicate that the standard or measure is mandatory.

b. The use of "should" means that the measure or action is required unless the commanding officer has justifiable reason for not implementing the measure or not taking the action. These reasons will be documented during the review and assessment process outlined in this chapter.

0102. PURPOSE. To establish policy and standards for physical security and loss prevention at Navy shore activities. Specifically, this manual:

a. Establishes minimum standards.

b. Provides guidance for evaluating, planning, and implementing each command's Physical Security Program.

c. Relates security measures to assets requiring protection.

d. Provides a basis for determining cost effective security measures/upgrades.

e. Assists those responsible for security in their efforts to carry out their assigned tasks.

0103. OBJECTIVES

a. The objectives of this instruction are to do the following:

(1) Establish general policy for the security of personnel, installations, and certain assets.

(2) Provide realistic guidance, general procedures, and the necessary flexibility for commanders to protect personnel, installations, assets from typical threats.

(3) Reduce the loss, theft, or diversion of, and damage to, Navy assets, thereby ensuring that warfighting capability is maintained.

b. During contingency operations, operations other than war, transition to war, etc., installation and activity commanding officers must provide for adequate protection of forces, personnel and property.

c. This instruction neither voids nor diminishes the authority or responsibility of commands to apply more stringent security standards appropriate for the asset, circumstances, and threat.

0104. SCOPE

a. This manual covers responsibilities for physical security and loss prevention. It classifies various security hazards, details management actions which must be employed to provide an acceptable physical security posture, and selectively sets minimum physical security requirements.

b. This manual applies to all Navy shore installations and activities.

c. This manual places specific emphasis on identification, analyses, and reduction of losses of government property. Physical security is essential to loss prevention.

d. This manual covers matters not covered by other, more specialized security programs.

(1) Protection of classified material, sensitive compartmented information, automated data processing systems, nuclear weapons, conventional arms, ammunition, and explosives, and nuclear reactors and special nuclear material are specifically addressed in references (a) through (f). Those instructions augment the basic guidance provided by this instruction.

(2) Antiterrorism and force protection are addressed in references (g) through (j). Security of Navy and other DoD personnel at U.S. Missions abroad is addressed in reference (k).

(3) Carrying of firearms and use of force, and weapons proficiency training are addressed in references (l) and (m).

e. The Physical Security Program addresses the protection of personnel and property (as such it is inseparably intertwined with antiterrorism and force protection programs). Such protection is accomplished by identifying the property requiring protection, determining jurisdiction and boundaries, assessing the threat, and committing resources to that end.

0105. PHYSICAL SECURITY PROGRAM

a. The physical security program is defined as that part of security concerned with active and passive measures designed

to prevent unauthorized access to personnel, equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. Physical security is a primary command responsibility.

b. Physical security programs provide the means to counter threats during peacetime transition to war, and in wartime. Physical security threats include the following:

(1) Foreign intelligence services.

(2) Paramilitary forces.

(3) Terrorists and saboteurs.

(4) Criminals.

(5) Protest groups.

(6) Disaffected persons.

0106. SECURITY RESPONSIBILITIES. Specific responsibilities are set forth in the following paragraphs.

0107. CHIEF OF NAVAL OPERATIONS (CNO)

a. The CNO is responsible for formulation and dissemination of Navy physical security policies.

b. The Special Assistant for Naval Investigative Matters and Security (CNO (N09N)) exercises this authority on behalf of the CNO for the Navy. CNO (N09N):

(1) Oversees implementation of Navy physical security and acts as program manager for CNO antiterrorism initiatives.

(2) Performs management, operation, and support functions for all research and engineering of shipboard and waterside security systems; anticompromise emergency destruct systems; explosive detection systems; and locking devices, security containers, and related delay systems. In order to effect appropriate coordination and reduce duplication of efforts, commanders should forward their research, development, test, and evaluation requirements for physical security equipment to CNO (N09N3). Requirements may be forwarded using Mission Need Statements or Operational Requirements documents.

c. Director, Antiterrorism and Force Protection (N34) under the Deputy Chief of Naval Operations (Plans, Policy and Operations (N3/N5) coordinates force protection matters as it relates to naval operations.

0108. Fleet Commanders in Chief (FLTCINCs)/ECHELON 2 COMMANDERS/OTHER ECHELONS OF COMMAND. FLTCINCs, Echelon 2

commanders, and other echelons of command will implement this instruction within their headquarters and subordinate activities, and oversee its implementation. This implementation will include where feasible and appropriate, consolidation and use of physical security resources on a regional basis.

a. The oversight function includes the following:

(1) Develop necessary procedures to meet specific needs, e.g., "campus security", Joint Reserve Bases, etc., for all bases and activities in their area of responsibility. These should be developed on a regional basis where appropriate and feasible.

(2) Coordinate and maintain liaison with the other Echelon 2 commands or Services having installations/activities in the same region(s) as its own, or which share other common interests and concerns.

(3) Develop specific physical security threat assessments, on a regional basis where appropriate and feasible, and keep them up to date.

(4) Oversee training and use of security forces, including consolidation and integration of security forces on a regional basis where appropriate and feasible.

(5) Ensure that all military construction projects are reviewed at the conceptual stage and throughout the process so that appropriate physical security, antiterrorist or force protective design features are incorporated into the design.

(6) Ensure that leases for their Navy activities resident within commercial facilities include provisions for positive physical security (including force protection measures) of Navy-occupied areas.

b. FLTCINCs and other Echelon 2 commands will formalize security procedures for joint response to terrorist incidents and other contingencies.

c. Commands involved with acquisition of major systems will establish internal procedures to ensure inclusion of appropriate security planning for these major systems, as discussed in chapter 2.

0109. <u>THE COMMANDING OFFICER</u>. The commanding officer of an activity is responsible for physical security of that activity and for establishing and maintaining a loss prevention program. The commanding officer will provide sufficient resources to implement, manage and execute an effective physical security and loss prevention program. Commanding officers of tenant activities who require armed security personnel to protect internal assets will coordinate these requirements with the host

installation (or region) commander. In addition to these same responsibilities, the commanding officer of an installation (or region) is also responsible for installation perimeter and area security, including coordination thereof with tenant activities.

0110. THE SECURITY OFFICER. The duties and responsibilities of Navy activity security officers are set out in appendix III.

a. The commanding officer of each Navy activity will appoint in writing a security officer. The security officer may act as security officer, force protection officer, and security manager concurrently. The basic function of the security officer is to assist the commanding officer by:

(1) Determining the adequacy of the command Physical Security and Antiterrorism Program.

(2) Identifying to the commanding officer those areas in which improved physical security and antiterrorism measures are required.

(3) Managing the program on behalf of the commanding officer.

(4) Specific duties expected of the position are outlined in appendix III.

b. The inherent importance of the duties dictates that the security officer must possess mature judgment, and should possess whenever possible:

(1) Appropriate grade/rank.

(2) Security experience appropriate for the mission and operating environment of the activity. Considerations include:

(a) Complexity of the physical security and loss prevention program and resources.

(b) Size of the command or activity.

(c) Size of the security organization.

(3) Occasionally, the security officer function may be a collateral duty, depending upon the size of the activity.

(4) The commanding officer is expected to provide the security officer with sufficient training, resources, staff assistance, and authority to manage and carry out an effective Physical Security and Loss Prevention Program.

(5) Consideration should be given to establishment of an assistant security officer position when the size of the security department exceeds about 100 persons.

0111. ORGANIZATIONAL RELATIONSHIPS. In the performance of assigned duties the security officer acts on behalf of the commanding officer. The security officer collaborates with officers or managers of other specialized security programs within the command concerning physical security needs, threats, requirements, and implementation. The security officer may also serve as the security manager, or manager of other specialized security programs.

0112. THE SECURITY PROBLEM. The security problem is influenced by:

a. The mission of the activity (e.g., combatant-oriented or training).

b. The size of the activity.

c. Who has jurisdiction (e.g., Joint Reserve Bases).

d. The nature of the property.

e. The geographic location (e.g., "heartland" or coastal).

f. The topography of the area.

g. The economic and political atmosphere (e.g., forward deployed or "campus").

h. Potential and presumed existing threats.

i. The degree of support provided by other organizations.

0113. THE SECURITY MANAGEMENT PHILOSOPHY

a. When planning for security, activities must prioritize assets and ensure that each is protected according to its value, vulnerability, and the role it plays in meeting the command's mission. Activity level planners must take basic program standards and requirements and build local procedures that will afford the appropriate degree of protection.

b. Management of security includes risk analysis, which provides the command with a method to rank the mission essential assets against the various threats. This process begins at the activity level, and encompasses the entire region. This analysis serves to:

(1) Identify assets in a priority order that are most critical for mission accomplishment.

(2) Analyze threats to those assets.

(3) Provide a baseline for managing and prioritizing resources to counter those threats.

0114. COMMAND PHYSICAL SECURITY REVIEW AND ASSESSMENT

a. The commanding officer of a Navy activity is expected to establish a continuing program of systematic physical security review and assessment.

b. During the physical security review and assessment process, the CNO shall be viewed as the "customer" who is being provided the physical security service by the activity.

(1) This manual constitutes the "customer's" standards.

(2) The end objective of the review and assessment processes discussed in this and following paragraphs is to provide physical security, including antiterrorism and force protection, in a manner that meets the pertaining standards at a cost that the "customer" can afford.

(3) Therefore, every activity must review its local processes, in conjunction with host installations, and other activities in the region, to come up with ways of providing physical security that meets the customer's standards in an efficient manner which the customer can afford.

(4) The following are some of the questions that facilitate a review and assessment process:

(a) What are the natures of the threats, and what are the likelihoods that threat events could occur?

(b) What is the activity's mission and what assets are critical to its accomplishment, and require what protection at what cost?

(c) How easily can assets be repaired or replaced?

(d) How does the activity physically protect its assets, and what are the alternatives?

(e) How does the activity link its manpower and financial planning with its security planning?

c. Imaginative thinking may well prove the greatest asset during the review and assessment process. In addition to identifying deficiencies, possible alternatives should be developed as solutions for consideration by the commanding officer.

d. This review and assessment process should include actively seeking local advice and assistance from within the activity regarding the following:

(1) Identifying and prioritizing the mission essential assets and developing vulnerability analyses and the activity threat assessment.

(2) Conducting self assessments of facility for antiterrorism readiness.

(3) Determining requirements for and evaluating security afforded to areas of the activity.

(4) Entry and visitor control procedures and establishment of restricted areas.

(5) Review of draft physical security plans or recommended changes prior to approval by the commanding officer.

(6) Review of command reports of significant missing, lost, stolen, and recovered government property, including loss trends analysis and breaches of security.

(7) Recommendations for improvements to physical security.

(8) Development of security education requirements and materials.

e. Appropriate local participants in such a <u>continuing</u> program of physical security review and assessment include representatives of the following functional areas:

(1) Security officer

(2) Comptroller

(3) Security manager, and officers or managers of other specialized security programs

(4) Public Works Officer or facilities manager

(5) Supply officer

(6) Legal officer or general counsel

(7) All major activity functional area managers <u>whose missions and operations are influenced and impacted by security requirements</u>

0115. INSTALLATION PHYSICAL SECURITY REVIEW AND ASSESSMENT

a. The commanding officer of a Navy installation is expected to establish a continuing program of systematic physical security and loss prevention review and assessment, with goals and purposes similar to that of the individual activity review and assessment programs (see preceding paragraph). But, here specific goals also include:

(1) Vulnerability analysis and assessment of the overall installation.

(2) Preparation of Terrorism Threat Assessment Plan.

(3) Identification of common as well as unique physical security interests and needs of the tenant activities which the host installation must be aware.

(4) Preparation of Physical Security/Force Protection Plan.

(5) Host/tenant coordination and agreements concerning efficient, not alike employment of mutually supportive physical security resources and procedures.

(6) Preparation of Terrorism Incident Response Plan

b. While a command's own individual review and assessment program looks to needs within its organization, the host installation program review and assessment program looks to the needs among the host and tenant organizations, and meeting those needs in an efficient manner. Appropriate participation includes representatives of each tenant activity located on the installation or outlying tenant activities for which physical security and law enforcement are the responsibility of the host command.

0116. REGIONAL PHYSICAL SECURITY REVIEW AND ASSESSMENT

a. The commanding officers of Navy installations within a geographic region are expected to establish a continuing program of systematic physical security review and assessment, with goals and purposes (e.g., terrorism threat assessment planning, force protection planning, and terrorism incident response planning) similar to that of the individual activity and host installation/tenant activity review and assessment programs discussed in the two preceding paragraphs.

b. Yet, specific goals here include identification of employment of specific physical security measures and related antiterrorism and force protection measures that efficiently meet all the security interests and needs of individual activities and installation (host/tenants), in a manner that avoids waste of resources.

c. Therefore, activities and installations must be accurately and completely up-to-date on what their security and force protection interests and needs are. Moreover, they must also have identified all the feasible options for meeting these security and force protection needs, and not become fixated on just one solution. This is a prerequisite for the required flexibility by each participating activity that is necessary for successful security implementation on a regional basis. Regionalization requires that each participating activity have the knowledge to be able to evaluate whether a given course of action could work for them, or to state what adjustments would make the course of action acceptable.

0117. PHYSICAL SECURITY SURVEYS

a. A physical security survey is not an inspection. Instead, it is an in-house formal assessment of an activity's physical security program; including loss prevention, antiterrorism, and force protection. It includes a complete study and analysis of each activity's property and operation, as well as the physical security measures in effect.

b. The intent of these surveys is to update the commanding officer on what needs protecting, what security measures are in effect, and what needs improvement. The survey is also intended to provide the commanding officer with a basis for determining priorities.

c. The results of physical security surveys are key to the activity/installation/regional physical security and loss prevention review and assessment programs described in previous paragraphs. Accordingly, the surveys need to be kept updated so that these review and assessment processes are based on current, complete, and accurate data.

0118. VULNERABILITY ASSESSMENTS

a. Echelon 2 commanders shall ensure physical security vulnerability assessments of facilities, installations, and operating areas within their purview are conducted by either a CNO (N34) or Joint Staff/Defense Threat Reduction Agency team every 3 years. Physical security vulnerability assessments will normally occur at the installation commander level (300 personnel or more) and above. These assessments should consider the range of identified and projected terrorism threats against a specific location or installation personnel, facilities, and other assets. The assessment should identify vulnerabilities and solutions for enhanced protection of DoD personnel and resources. The assessment will address the broad range of physical threats to the security of personnel and assets and shall be conducted at least once every three years.

b. For installations with fewer than 300 personnel, Echelon 2 commands will conduct vulnerability assessments using

CNO (N34) vulnerability assessment checklist every 3 years. Echelon 2 commands may request CNO (N09N) augmentation for guidance within their assessment teams, if needed.

0119. THREAT ASSESSMENTS

a. Liaison with Law Enforcement Agencies. All Naval Criminal Investigative Service (NAVCRIMINVSERV) components maintain close and effective liaison with local, State, and Federal law enforcement and intelligence agencies and disseminate, by the most effective means, known threat information affecting the security of a particular military installation. If a command detects or perceives threat information, the servicing NAVCRIMINVSERV component should be promptly notified. Follow-up action generally consists of the NAVCRIMINVSERV component attempting to obtain amplifying details/intelligence regarding the perceived threat.

b. Evaluation. Based on available information, the command must determine the active short, medium, and long-term threat. The NAVCRIMINVSERV can supply these threat evaluations on request. Threat information must be analyzed together with the existing physical security posture to determine if vulnerabilities exist. The possibility of attempts by terrorist groups, criminals, activists, or foreign intelligence operatives to penetrate the security of military installations continues to be a matter of serious concern. Accordingly, NAVCRIMINVSERV will provide, upon request, a comprehensive annual area threat assessment through the servicing NAVCRIMINVSERV office. Requests should be in writing at least 45 days in advance. The request should specify what threats are of particular concern (terrorism, foreign intelligence, activist and/or criminal), desired method of transmission of the finished report and any unique dissemination requirements.

0120. NEW CONSTRUCTION. All new construction shall comply with the requirements of this manual. Plans for new construction shall be reviewed by the security officer or designated representative during the design process and various review phases to ensure that physical security, loss prevention, antiterrorism, and force protection measures are adequately incorporated. Issues which cannot be resolved at the local level because of lack of necessary funding or other reasons outside the control of the local command (e.g., appropriate and adequate clear zones) will be resolved by the parent Echelon 2 command.

0121. FACILITY MODIFICATIONS. All facility modifications to existing buildings, facilities, sites, etc., shall comply with the requirements of this manual. Proposals for these modifications shall be reviewed by the security officer or designated representative during the design process and review stages to see that physical security, loss prevention, antiterrorism, and force protection measures are adequately incorporated. Issues which cannot be resolved at the local level

because of lack of necessary funding or other reasons outside the control of the local command (e.g., appropriate and adequate clear zones) will be resolved by the parent Echelon 2 command.

0122. NAVY MILITARY CONSTRUCTION PROJECTS. Navy military construction (MILCON) projects must be submitted via the chain of command through CNO (N09N3) to Commander, Naval Facilities Engineering Command. CNO (N09N3) review of physical security construction projects will include ensuring requirements in this manual are addressed (and protective design measures have been considered), and that equipment reliability and maintenance has been considered. Security and force protection can be enhanced by appropriate facility and environmental design. Examples include improved use of lighting and standoff distances.

0123. SECURITY OF LEASED FACILITIES. Terrorist activity worldwide against U. S. military and business concerns poses a clear and persistent danger to Navy interests. Many Navy activities are located within "leased space" facilities and are confronted with unique situations in addressing physical security issues.

a. Commanders shall use the guidance and policies contained in chapters 3 and 5, as applicable, in determining security and/or protective measures deemed essential for their particular spaces, areas and/or buildings. Commands should address physical security in all lease agreements.

b. Liaison with appropriate authorities, e.g., General Services Administration, building administrators, lessors, etc., is essential to delineate specific security responsibilities among the concerned parties regarding measures that are necessary for the protection of lives and property and which are tailored to the individual characteristics of the leased space.

(1) Physical security standards that cannot be met, either temporarily or permanently, must be identified and waiver or exception requests submitted, as appropriate, per paragraph 0124. Compensatory security measures implemented and/or planned must be identified in all such requests.

0124. ACTIVITY UPGRADE REQUIREMENTS/WAIVERS/EXCEPTIONS. All activities will review their existing security posture and determine modifications necessary to conform to this instruction. Basic principles, objectives, and processes must be achieved, and waivers or exceptions to them are not appropriate.

a. A 10 percent deviation from physical security requirements is authorized without need of waiver or exception. New construction, upgrade or modification to existing facilities must conform with standards contained in this manual. A plan of action and milestones will be developed to correct deficiencies.

b. Deficiencies which are not correctable within 12 months will be covered by an approved waiver or exception pending completion of the required upgrade effort. Compensatory security measures are required.

c. Effective with the publication of this manual:

(1) The only provisions authorized for waivers and exceptions to this manual are those outlined here. Any requests for waivers or exceptions to this manual will be submitted per appendix IV.

(2) All existing waivers and exceptions to earlier editions of this manual are cancelled because of extensive revisions here.

d. Blanket Waiver and Exceptions. Blanket waivers and exceptions are not authorized.

e. Waiver and Exception Cancellation. Waivers and long term exceptions are self-cancelling on the expiration dates stated in the approval letters, unless extensions are approved by CNO (N09N3). Cancellations do not require CNO approval.

CHAPTER 2

SECURITY PLANNING

0200. GENERAL

a. Each Navy activity/installation will develop and publish a physical security and loss prevention plan, in consonance with regional commanders and their security coordinators.

b. Tenant commands will develop and maintain a physical security plan for their activities that takes into account the host command's physical security plan. These plans will be coordinated with the host command security officer.

c. Security plans for tenant activities on a Navy installation will be integrated into the installation physical security plan. Tenant commands will comply with host activity physical security requirements. These integrated plans will incorporate requirements, policies, and procedures for facilities, equipment, regular and auxiliary security forces, employee training/education, and other elements of security essential to force protection and objectives set forth here.

d. Security planning will be integrated with terrorism threat assessment planning and terrorist incident response planning.

e. Tenant and host commands, as appropriate, will ensure that tenant/host and intra or inter-service support agreements outline complete and detailed physical security requirement responsibilities.

f. Where appropriate and feasible, similar integration and coordination of security planning and implementing of specific measures will be accomplished among Navy activities on a regional basis, and with local law enforcement/host nation security forces.

0201. PHYSICAL SECURITY PLAN CONTENT. The content of the plan is more important than its format. The format should be one that facilitates rather than hinders use of the plan. Higher echelons in the chain of command may prescribe for their subordinates a format that facilitates integration into the next higher echelon's plan.

a. The plan must be a "users" instruction clearly delineating how the command conducts day-to-day security and how it responds to security incidents. It should reflect the detailed implementation of the policy in this manual at the activity and installation level (and regional level, if appropriate and feasible).

b. It will cover all phases of the security operations of the activity/installation. It must also be current and reflect the routine needs of the command as well as unusual situations that require special security considerations/measures.

c. It will provide instruction relative to individual security responsibilities, authority, and procedures for handling and reporting incidents.

d. It will also establish systems for alerting and evacuation of personnel. A set of recognizable alarms should be developed for potential emergencies, each with their own set of reactions, with a means to immediately sound those alarms and frequent drill conducted that will familiarize all personnel with individual responsibilities.

e. Orders and contingency plans must consider recommended actions at various terrorist threat levels and conditions.

f. Contingency plans for major shore commands and their seniors in command exercising territorial authority shall contain provisions for reinforcement of security forces when necessary.

g. Specific matters that are appropriately addressed in most plans include, for example:

(1) Implementation of activity and installation (and regional, if appropriate and feasible) physical security review and assessment programs described in chapter 1.

(2) Protection for vulnerable points/assets within the activity.

(3) Restricted areas and access controls.

(4) Personnel screening/inspection criteria instructions.

(5) Personnel identification and control systems.

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

(7) Lock and key control program.

(8) Loss prevention reporting and analyses measures.

(9) Designation of Threat Conditions (THREATCONs) and implementation of associated measures.

(10) Security force organization and training.

(11) Coordination with other security agencies and local law enforcement.

(12) Security response.

(13) Jurisdiction

h. The Physical Security Plan and antiterrorism/force protection (AT/FP) plans (references (g) through (j)) are one and the same provided that they cover crisis management standard operating procedures (i.e., Incident Response Plan), THREATCON implementation plan including a barrier plan (barrier deployment locations, barrier storage locations, and barrier transportation), personnel alerting system, and command center establishment procedures and security.

0202. PLANNING PROCESS

a. Security planning is a continuing process carried out both in advance of operations and concurrently with them.

b. Every asset cannot be made invulnerable. Therefore, the objective of security planning is to identify what assets are to be protected, analyze the threat against them, and develop realistic countermeasures. Increasingly sophisticated methods used by conventional criminals, terrorists, conventional enemy agents, etc., make this an increasingly challenging task. Limited availability of personnel for security duties and money for other security measures exacerbate this challenge. Developing sound security plans to work hand in hand with other related planning (e.g., crisis, force protection, disaster, etc.) requires good decisions by the planning organization based on accurate information, experience, knowledge to orchestrate and integrate security personnel duties such as in-depth protection crime prevention through environmental design to provide in-depth protection.

c. Physical security planning includes the following:

(1) Using electronic security systems to reduce both vulnerability to the threat and reliance on fixed security forces.

(2) Integration of physical security and force protection measures into contingency, mobilization, and wartime plans, and testing of physical security procedures and measures during the exercise of these plans.

(3) Coordinating with installation operations security, crime prevention, information security, personnel security, communications security, automated information security and physical security programs to provide an integrated and coherent effort.

(4) Training security forces at facilities or sites in tactical defense against, and response to, attempted penetrations.

(5) Creating and sustaining physical security awareness.

(6) Identifying resource requirements to apply adequate measures.

0203. PLANNING CONSIDERATIONS. The following factors shall be considered in determination of security requirements and planning:

a. Overall importance/criticality of the command.

(1) Mission and sensitivity of the activity.

(2) Importance of the activity to the continuity of essential naval operations (e.g., combatant support vs. "campus").

b. Force protection.

(1) Terrorist Assessment Plan.

(2) Terrorist Incident Response Plan.

c. Overall susceptibility/vulnerability of the command to threats. Specifically:

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

(2) Ease of access to vital equipment and material.

(3) Location, size, deployment and vulnerability of facilities within the activity and the number of personnel involved.

(4) Need for tailoring security measures to mission critical operating constraints and other local considerations.

(5) Probable duration of operations.

(6) Geographic location (existence of natural barriers).

(7) Legal jurisdiction of real property.

(8) Mutual aid and assistance agreements.

(9) Local political climate.

(10) Adequacy of storage facilities for valuable or sensitive material, including precious metals, drugs, arms, ammunition, and explosives.

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

(12) Possible losses and their impact on command mission and readiness.

(13) Possibility or probability of expansion, curtailment or other changes in operations.

(14) Overall cost of security.

(15) Availability of personnel and material.

(16) Coordination of security forces.

(17) Calculated risk.

(18) Potential for increase in threat.

0204. PHYSICAL SECURITY PERFORMANCE GOAL, DOD THREAT MATRIX, AND DOD ASSETS PRIORITIZATION

a. Physical Security System Performance Goal

(1) The goal of the security system for an asset or facility is to deploy security resources to preclude or reduce the potential for sabotage, theft, trespass, terrorism, espionage, or other criminal activity. To achieve this goal, a security system provides the capability to detect, assess, communicate, delay, and respond to an unauthorized attempt at entry.

(2) The components of a security system each have a function and related measures which provide an integrated capability for the following:

(a) Detection, accomplished through human, animal, or electronic means, alerts security personnel to possible threats and attempts at unauthorized entry at or shortly after the time of occurrence;

(b) Assessment, through use of video subsystems, patrols, or fixed posts, assists in localizing and determining the size and intention of an unauthorized intrusion or activity;

(c) Command and control, through diverse and secure communications to ensure that all countermeasures contribute to preventing or containing sabotage, theft, or other criminal activity;

(d) Delay, through the use of active and passive security measures, including barriers, impedes intruders in their efforts to reach their objective;

(e) Response, through the use of designated, trained, and properly equipped security forces. Detection and delay must provide sufficient warning and protection to the asset until the response force can be expected to arrive at the scene.

b. Physical Security Threat Matrix. Figure 2-1 is a description of the DoD generic threat types developed for the physical security program. Using these threat types as a guide, commanders shall develop program, system, command, or installation threat statements which assess potential security threats to critical assets. Using both law enforcement and intelligence information, these assessments should categorize opportunity (when possible) and capabilities of potential adversaries. Physical security threat statements will be used for the development of security systems tailored to the protection of assets and items of security interest.

c. Prioritization of Assets. At figure 2-2 is a description of the DoD resource and asset prioritization scheme with examples of typical assets, a criticality definition, and an example of a typical security system for each level.

0205. THREAT ASSESSMENTS. Additional standards and direction concerning threat assessments are provided in reference (h).

0206. RISK MANAGEMENT. Risk management is the concept which dictates that when there are limited resources available for protection, possible loss or damage to some supplies or to a portion of the activity is risked in order to ensure a greater degree of security to the remaining supplies or portions of the activity. However, security controls shall not be relaxed to the degree that anything is left completely unprotected.

0207. CRISIS SITUATIONS. In evaluating the need for and extent of physical protection required, the possibility of injury to security force personnel must be considered. This is especially relevant when addressing security measures taken during crisis situations (e.g., bomb threats, fires, terrorist incidents or natural catastrophes) to protect government assets; to limit damage and provide emergency services for containment of the incident; and to restore the target activity to normal operation. Situations which present unique and growing physical security problems are: the handling of bomb threats and terrorist incidents as well as any change to higher threat conditions (THREATCONS) (references (g) through (j) pertain). Bomb threat situation planning should be coordinated and cross referenced with the command disaster preparedness plan and integrated with the terrorist incident response plan and should include preventive measures to reduce the opportunities for introduction of bombs; procedures for evaluating and handling

THREAT TYPE	THREAT DESCRIPTION	THREAT EXAMPLE
MAXIMUM	INDIVIDUALS IN ORGANIZED AND TRAINED GROUPS ALONE/WITH ASSISTANCE FROM AN INSIDER; SKILLED, ARMED AND EQUIPPED WITH PENETRATION AIDS	TERRORISTS AND SPECIAL PURPOSE FORCES; HIGHLY TRAINED INTELLIGENCE AGENTS
ADVANCED	INDIVIDUAL(S) WORKING ALONE/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/IN SMALL GROUPS; SOME KNOWLEDGE OR FAMILIARITY OF SECURITY SYSTEM	CAREER CRIMINALS; ORGANIZED CRIME; WHITE COLLAR CRIMINALS; ACTIVE DEMONSTRATORS; COVERT INTELLIGENCE COLLECTORS; SOME TERRORIST GROUPS
LOW	INDIVIDUAL(S) OR INSIDER(S) WORKING ALONE/IN A SMALL GROUP	CASUAL INTRUDERS; PILFERERS AND THIEVES; OVERT INTELLIGENCE COLLECTORS; PASSIVE DEMONSTRATORS

Figure 2-1. Physical Security Threat Matrix

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
A INTEGRATED ELECTRONIC SECURITY SYSTEMS, 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 AND 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

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
B ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD BE EXPECTED TO GRAVELY HARM THE OPERATIONAL CAPABILITY OF THE UNITED STATES	ALERT SYSTEMS, FORCES, AND FACILITIES ESSENTIAL COMMAND, CONTROL, AND COMMUNICATIONS FACILITIES AND SYSTEMS CATEGORY I ARMS, AMMUNITION, AND EXPLOSIVES RESEARCH, DEVELOPMENT AND TEST ASSETS

Figure 2-2. Resource and Asset Priorities

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
C ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIERS, SECURITY PATROLS, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD IMPACT UPON THE TACTICAL CAPABILITY OF THE UNITED STATES	NONALERT RESOURCES AND ASSETS PRECISION GUIDED MUNITIONS COMMAND, CONTROL, AND COMMUNICATIONS FACILITIES AND SYSTEMS CATEGORY II ARMS, AMMUNITION AND EXPLOSIVE POL/POWER/WATER/SUPPLY STORAGE FACILITIES RESEARCH, DEVELOPMENT AND TEST ASSETS

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
D ELECTRONIC SECURITY SYSTEMS, ACCESS CONTROL, BARRIERS, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD COMPROMISE THE DEFENSE INFRASTRUCTURE OF THE UNITED STATES	ARMS, AMMUNITION, AND EXPLOSIVES EXCHANGES AND COMMISSARIES, FUND ACTIVITIES CONTROLLED DRUGS AND PRECIOUS METALS TRAINING ASSETS RESEARCH, DEVELOPMENT AND TEST ASSETS

Figure 2-2 (Contd). Resource and Asset Priorities

threatening messages; policy on evacuation and safety of personnel; procedures for search; procedures for obtaining assistance and support of law enforcement and military explosive ordnance disposal (EOD) units; procedures in the event a bomb is found on the premises; and procedures to be followed in the event of an explosion or detonation.

0208. SABOTAGE. As a minimum measure, assigned personnel should be made aware of the nature of the threat posed by anti-military individuals and groups. Active liaison with the Naval Criminal Investigative Service or command intelligence personnel is a major factor in obtaining such information at the local level.

0209. TERRORISM. Acts of terrorism directed at Navy personnel, activities or installations have the potential to destroy critical facilities, injure or kill personnel, impair or delay accomplishment of mission and cause incalculable damage. Standards and guidance for planning for responding to terrorist acts are contained in references (g) through (j).

0210. THREAT CONDITIONS (THREATCONS) FOR Combating TERRORISM. Requirements and guidelines concerning THREATCONS are outlined in reference (g).

0211. COORDINATION. To provide for efficient coverage of security needs without wasteful duplication:

a. Physical security of separate activities and installations will be coordinated with other military activities/installations in the immediate geographic region or area and with local civilian law enforcement agencies or host government representatives. Opportunities to "partner" or share special capabilities among regional users will be fully explored and documented to ensure economy of effort.

b. Within the physical confines of the installation, the host activity shall coordinate physical security measures employed by tenant activities.

c. The physical security of all arms, ammunition and explosives, and other hazardous material held by tenant activities will be closely coordinated with the host activity.

d. All 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 from the outset to ensure that security considerations are included during initial planning.

CHAPTER 3

PART ONE

PHYSICAL SECURITY MEASURES

0300. SECURITY MEASURES

a. Physical security measures are necessary to establish or maintain an adequate command physical security posture. Where appropriate and feasible, physical security measures are to be coordinated and integrated on a regional basis.

b. Physical security measures are a combination of active or passive systems, devices, and security personnel used to protect a security interest from possible threats. These measures include:

(1) Security forces and owner or user personnel.

(2) Military working dogs.

(3) Physical barriers, facility hardening and active delay or denial systems.

(4) Secure locking systems, containers, and vaults.

(5) Intrusion detection systems.

(6) Assessment or surveillance systems (i.e., closed-circuit television or thermal imagers).

(7) Protective lighting.

(8) Badging systems, access control devices, material or asset tagging systems, and contraband detection equipment.

0301. ANTITERRORISM AND FORCE PROTECTION MEASURES. Antiterrorism and force protection standards and measures are addressed in references (g) through (j).

0302. SECURITY OF FUNDS. Unless more specific measures are prescribed by other authorities, funds including cash and readily negotiable instruments will be protected in a manner that is clearly appropriate for the amount of money involved. Commanding officers shall not send armed money escorts off base without approval from the local authorities and/or the regional coordinator.

0303. LOSS REPORTING. Requirements and guidelines for reporting of missing, lost, stolen, or recovered (MLSR) government property are outlined in reference (n).

0304. KEY SECURITY AND LOCK CONTROL. Each Navy activity must establish a key and lock control program for all keys, locks, padlocks and locking devices used to meet security and loss prevention objectives of this manual. It is not intended to include keys, locks and padlocks used for convenience, privacy, administrative, or personal use.

a. Reference (e) governs controls and security of keys and locks used to provide security of arms, ammunition, and explosives.

b. Keys and locks cannot be adequately controlled without inventories. The frequency of inventories shall be appropriate for the local circumstances, especially circumstances that exacerbate problems of maintaining control.

c. No key and lock control program can assure that any given key has not been compromised over a period of time. Accordingly, where padlocks and removable lock cores are used, there must be a program to rotate these locks and cores. The intent is that anyone possessing a key without authorization eventually discovers that the location of the lock which the key fits is no longer known. If the rotation is done in conjunction with lock maintenance, the incremental impact on resources including manpower should be minimal. This approach is more cost effective than replacing all existing keys and replacing or rekeying all existing locks.

d. All locks and padlocks used to meet standards in this manual shall be adequate for the intended security of the protected asset. To this end, the activity security officer should be involved in the lock procurement process so that only locks that are adequate for their intended application are procured.

e. Lockouts. If a lock does not work properly, do not assume the reasons are innocent ones. Although the failure of a locking device could be the result of a product failure, it could alternately be a result of attempted or actual illegal penetration. Therefore, all lockouts involving locks used to meet security objectives of this manual will be promptly examined by competent personnel to determine the cause of the lockout and the security officer notified of the determination.

0305. SECURITY CHECKS. Each Navy activity must establish a system for the checking by occupants/users of restricted areas, facilities, containers, and barrier or building entry and departure points to detect any deficiencies or violations of security standards.

CHAPTER 3

PART TWO

SECURITY OF AIRCRAFT, SHIPS IN PORT, AND OTHER WEAPON SYSTEMS AND PLATFORMS ASHORE

0306. GENERAL. This part establishes policy and responsibility for security of aircraft, ships in port, and other weapon systems and platforms ashore.

0307. POLICY

a. Installation commanding officers are responsible for the security of assets whether assigned or transient while these assets are resident on their installations. Commanding officers shall develop security plans to meet this responsibility.

b. The priority for security placed on similar assets within the Echelon 2 command may vary due to differences in the following:

(1) Mission;

(2) Location and vulnerability;

(3) Operational readiness;

(4) Value, classification, and replacement costs.

c. Before operations commence, the command (or Service) owning the assets should request any special security support from the host installation, if necessary, as far in advance as possible. Economic and logistical considerations dictate that every reasonable effort be made by the host installation to provide the necessary security without resort to external support from the command owning the asset (aircraft, ship, etc.). The owning command should provide material and personnel for extraordinary security measures (extraordinary security measures are those that require heavy expenditures of funds, equipment, or manpower; or unique or unusual technology) to the host installation.

0308. AIRCRAFT SECURITY PLANNING. In general planning for aircraft security, an installation commander should consider the degree to which the installation provides a secure environment. Installation commanders should consider at least the following factors:

a. Whether the installation is open or closed to the public.

b. Whether the flightline or aircraft parking area is adequately fenced, lighted, and posted with signs.

c. Whether a controlled access policy or limited entry restriction is in effect at the flightline or aircraft parking area.

d. Whether, and to what degree, the flightline or aircraft parking area has security or law enforcement patrol coverage or surveillance provided by personnel working within or around the area.

e. Intrusion Detection Systems (IDS) should be used to augment other physical security procedures, devices, and equipment.

0309. TRANSIENT OR DEPLOYED AIRCRAFT

a. The installation commander will always provide a secure area for transient aircraft on the installation.

b. For administrative aircraft, this requirement may be met by parking aircraft in an area where normal personnel activity provides a reasonable degree of deterrence.

c. More critical aircraft require additional security measures as listed below. The host installation should make every reasonable effort to provide the same degree of security that the owning Service would provide under the same (transient or deployed) circumstances.

(1) Park the aircraft in a permanent restricted area with an IDS when possible.

(2) If it is not possible to park the aircraft in an established restricted area with IDS, park it in a hangar or encircle it with an elevated barrier, such as rope and stanchions. When a hangar is used, the walls constitute the restricted area boundary.

(3) Provide area lighting of sufficient intensity to allow the security force to detect and track intruders.

(4) Display restricted area signs so that personnel approaching the aircraft can see the signs.

(5) Provide circulation control. Entry must be limited to only those persons who have a need to enter.

(6) Require the senior security supervisor to give the aircraft commander a local threat assessment for the duration of ground time.

0310. OTHER SITUATIONS

a. Various aircraft assigned to the Services provide tactical support, logistical support, reconnaissance, and

refueling capability for worldwide American interests. Many of these aircraft, because of their large size or mission tasking, are an attractive target. This is particularly true at installations where their presence is unusual, they are on display, or are located at civilian or foreign airfields. Refer to the security requirements matrix (table 3-1) to determine the minimum security to be provided for nonalert aircraft. These requirements apply to aircraft on display or located at civilian or foreign airfields. Special or increased requirements for specific operational configuration must be identified in advance (when possible) to host security forces.

b. Security forces in support of aircraft must be notified before a visit to the aircraft is allowed to take place. Any change in security priorities based on operational status must be identified to the host installation.

c. The aircraft commander determines if security is adequate.

0311. EMERGENCY SITUATIONS

a. Initial security for aircraft that crash or are forced to land outside a military installation is the responsibility of the nearest military installation. The owning Service will respond and assume on-site security as soon as practical.

b. In the above emergency situations, security must:

(1) Ensure the safety of civilian sightseers.

(2) Prevent tampering with or pilfering from the aircraft.

(3) Preserve the accident scene for later investigation.

(4) Protect classified cargo or aircraft components.

0312. PIERSIDE PROTECTION OF SHIPS. Ships will normally be protected by a pier sentry controlling access, located at least 100 feet from ships in the continental U.S. (CONUS), and 400 feet from ships outside of the continental U.S. (OCONUS) when host country laws and/or customs permit.

0313. HARBOR SURVEILLANCE AND WATERSIDE/WATERWAY SECURITY. Commanding officers will ensure that these areas are adequately patrolled and/or that appropriate surveillance is maintained.

Aircraft Type	Security Priority	Entry Control Responsibility	SRT[1] Team	CBS[2]	Motorized Patrol
Tactical Aircraft (AV-8, F-14, F/A-18)	C	Aircrew	Yes	—	Yes
Airlift Aircraft (C-3, C-9, C-130, C-141)	C	Aircrew	Yes	—	Yes
Strategic Bomber Aircraft (B-1, FB-111)	C	Aircrew	Yes	—	Yes
Air Refueling Aircraft (KA-6, KC-10, KC-135)	C	Aircrew	Yes	—	Yes
Special Mission Aircraft (E-2, EA-6, EP-3, ES-3)	B	Security	Yes	Yes	—
Reconnaissance Aircraft (S-3, P-3)	B	Security	Yes	Yes	—
Advanced Technology Aircraft	B	Pilot carries detailed information for divert contigencies	—	—	—
Other DoD Aircraft	C	Aircrew	Yes	Yes	Yes

[1] Security Response Team (SRT). A team consisting of two security force members available to respond within 5 minutes. All priority aircraft require SRT support. SRTs may be area patrols not specifically dedicated to the visiting aircraft.

[2] Close Boundary Sentry (CBS). A security force member posted inside or outside the boundary to keep the boundary of the restricted area under surveillance.

CHAPTER 3

PART THREE

PROTECTION OF BULK PETROLEUM PRODUCTS

0314. GENERAL. This part prescribes general policies for security of Government-owned, Government-operated (GOGO) and Government-owned, Contractor-operated (GOCO) fuel support points, pipeline pumping stations, and piers.

0315. POLICY

a. Commanders of GOGO and GOCO fuel support points, pipeline pumping stations, and piers shall designate and post these installations as Restricted Areas. (This restricted area requirement does not apply to locations for issue (and incidental storage) of ground fuels for use in motor vehicles, material handling equipment, and stationary power and heating equipment. Commanding officers will determine the means to protect against loss or theft of fuel at these locations.)

b. Access to these facilities shall be controlled and only authorized personnel shall be permitted to enter. Commanders shall determine the means required to enforce access control (i.e., security forces, barriers, lighting, and security badges) based on the considerations in Chapter 2 of this Instruction.

0316. SECURITY PLAN AND LIAISON. Commanders shall take the following actions to protect their fuel facilities:

a. Establish liaison and coordinate contingency plans and inspection requirements with the nearest U.S. military installation to provide manpower and equipment resources to the facility in the event of emergencies and increased threat conditions.

b. Establish liaison with supporting law enforcement agencies and host nation officials; and support agreements, if appropriate.

0317. PHYSICAL SECURITY INSPECTIONS

a. Navy installations responsible for the security oversight of fuel facilities will conduct a physical security inspection of that facility at least once every 2 years.

b. Inspections should be formal, recorded assessments of crime prevention measures and other physical security measures, used to protect the facilities from loss, theft, destruction, sabotage, or compromise.

CHAPTER 3

PART FOUR

SECURITY OF COMMUNICATIONS SYSTEMS

0318. GENERAL

a. This part describes concepts for physical security of communications facilities located on and off Navy installations, to include mobile systems. Specific security support for facilities that require special security measures shall be coordinated between or among the concerned activities and installations.

b. Because of the difference in location, physical layout and equipment, security considerations must be thoroughly assessed for each communications system. The physical security program shall be tailored to that particular facility or system.

0319. POLICY

a. The protection provided to communication facilities and systems shall be sufficient to ensure continuity of operations of critical users and the facilities they support. These include nuclear weapon delivery units and storage facilities and primary command and control elements. The determinations on strategic importance, both to the United States and its allies, shall be based upon whether or not each mobile system or facility processes, transmits, or receives, telecommunications traffic considered crucial by the National Command Authorities, the Chairman, Joint Chiefs of Staff, or the Commanders in Chief of the Unified and Specified Commands. Commander, Naval Computer and Telecommunications Command shall be consulted on this issue.

b. Communications systems play a major role in support of each Navy activity's mission, providing operational communications in both peacetime and wartime. These are attractive targets due to limited staffing, isolated location and mission. Therefore, security for these systems must be an important part of each command's physical security program.

c. Parent Echelon 2 commands must review the host installation's implementation of physical security measures during inspections, oversight, and staff visits.

d. Access shall be controlled at all communications facilities; only authorized personnel shall be allowed to enter. Facilities should be designated and posted as Restricted Areas.

e. Depending on regional conditions, commanders should consider locating enough weapons and ammunition at communications facilities to arm designated onsite personnel. If arms are

stored at the facilities, appropriate security measures and procedures shall be employed following reference (e). Weapons will not be located at unmanned facilities.

f. Existing essential structures should be hardened against attacks. This includes large antenna support legs, antenna horns, operations building and cable trays. Future construction programs for critical communications facilities should include appropriate hardening of essential structures.

0320. RESPONSIBILITIES. Fleet Commanders in Chief and other Echelon 2 commands will:

a. Identify critical communications facilities and mobile systems within their commands.

b. Ensure that a security plan is developed for each communications facility and mobile system within their command. The plan shall include emergency security actions and procedures for emergency destruction of sensitive equipment and classified information. The plan may be an annex to an existing host installation security plan; only the applicable parts of the total plan shall be distributed to personnel at the facility or mobile system.

c. Arrange for security of off-installation facilities and mobile systems with the closest U.S. military installation. This includes contingency plans for manpower and equipment resources during emergencies. These arrangements can be made by establishing a formal agreement such as an interservice support agreement. Whether the facilities are located on or off the installation, or mobile, installation commanders are responsible for security of communications facilities for which they provide host support.

d. Because operations, maintenance, and communications personnel at the facility or mobile system are the most important factor in security, ensure implementation of a training program to ensure that assigned personnel understand their day-to-day security responsibilities, are familiar with the vulnerabilities of the facility, and are prepared to implement emergency security actions. The training program shall include the following:

(1) Security procedures and personal protection skills for assigned personnel.

(2) The use of weapons and communications equipment for protecting the facility or mobile system.

(3) Awareness of local terrorist threats and other activity in the area.

0321. MOBILE COMMUNICATIONS SYSTEMS. Per chapter 2 of this instruction, a security operational concept or standards shall be developed for mobile systems to describe the minimum level of security for the system in the expected operational environment.

CHAPTER 3

PART FIVE

SECURITY OF MATERIEL

0322. GENERAL. This part provides security policy and procedures for safeguarding controlled inventory items, including drugs, drug abuse items, (as identified under Code of Federal Regulations (CFR), 21 CFR 1301.71 through 1301.76 and P.L. 91-513), and precious metals. The following definitions describe sensitive items:

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

(2) Code "Q" Items. Drug or other controlled substances designated as Schedule III, IV, or V items, per 21 CFR 1308.

(3) Code "R" Items. Precious metals and drugs or other controlled substances designated as Schedule I or II items per 21 CFR 1308.

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

0323. POLICY

a. The security of controlled inventory items is of special concern to the DoD. Consequently, these items shall have characteristics so that they can be identified, accounted for, secured or segregated to ensure their protection and integrity.

b. Special attention shall be paid to the safeguarding of inventory items by judiciously implementing and monitoring physical security measures. This shall include analysis of loss rates through inventories, reports of surveys, and criminal incident reports, to establish whether repetitive losses indicate criminal or negligent activity.

0324. RESPONSIBILITIES

a. Commanding officers shall:

(1) Establish physical security measures to protect inventory items, and to reduce the incentive and opportunity for theft.

(2) Monitor the effective implementation of security requirements through scheduled inspections of and staff or oversight visits to affected activities.

(3) Ensure that adequate safety and health considerations are incorporated into the construction of a security area for controlled inventory items.

(4) Ensure that storage facilities and procedures for operation adequately safeguard controlled inventory items.

0325. Controlled Substances Inventory. Accountability and inventory of controlled substances shall be as prescribed in reference (o).

0326. SECURITY REQUIREMENTS FOR "R" CODED ITEMS AT BASE AND INSTALLATION SUPPLY LEVEL OR HIGHER

a. Storage in vaults or strongrooms (as defined in reference (a)) 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 Group One combination locks. Or they may be stored using any means which provide a degree of security equivalent to any of the preceding.

b. Unless not feasible, storage areas or containers will be protected with an installed intrusion detection system.

0327. SECURITY REQUIREMENTS FOR "Q" CODED ITEMS AT BASE AND INSTALLATION SUPPLY LEVEL OR HIGHER

a. The preferred storage for sensitive inventory items coded "Q" is in vaults or strongrooms (as defined in reference (a)).

b. Small quantities may be stored in security containers or other means approved for items coded "R."

0328. SECURITY REQUIREMENTS FOR "R" AND "Q" CODED ITEMS BELOW BASE AND INSTALLATION LEVEL (i.e., Small Unit/Individual Supplies)

a. Storage as described in paragraphs 0326 and 0327.

b. As an alternative, small stocks may be stored in a 750-pound or heavier GSA-approved security container. Smaller GSA-approved security containers are authorized, but must be securely anchored to the floor or wall. Also, any means which provides a degree of security equivalent to any of the preceding may be used. Security containers should also be located within a continuously manned space or be checked by a

security force member at least twice per 8-hour shift, barring any reason for the contrary.

0329. LOSS PREVENTION MEASURES. A loss prevention program is essential at every Navy activity. Losses of property may prevent timely accomplishment of mission requirements.

a. The mission is affected not only by direct loss of the property, but it is also affected by lost opportunities of procuring other goods and services to improve mission accomplishment because available funds must be diverted to loss replacement. A manager whose property must be continually bought over and over again to replace losses is robbing other managers of the opportunity of putting the same money to better use.

b. As a minimum, loss prevention measures will consist of the following:

(1) To identify trends and patterns of losses, there must be a continuing process of loss analysis. It should consider the types of material lost; geographic location; times and dates; proximity of specific personnel; proximity of doorways, passageways, loading docks and ramps, gates, parking facilities, piers and other activities adjacent to loss or gain locations; material movement paths; etc.

(2) It is intended that the results of analysis of loss and gain trends and patterns will be used to appropriately allocate resources available for crime prevention.

(3) Actions to prevent or reduce opportunities for losses of government property at supply centers, shipyards, shipping and receiving points, ordnance stock points, and other Navy activities, should be stressed.

(4) Warehouses, storage buildings, office buildings, and other structures which contain high value, sensitive, or pilferable property, supplies, or office equipment are to be afforded security protection commensurate with the value and sensitivity of the contents.

(5) Shore activities that are tenants may need to include loss prevention support in host-tenant agreements or inter-service support agreements. Where feasible and appropriate, such support should be coordinated and integrated among Navy activities on a regional basis.

(6) Employees must be made continually aware of the need for loss prevention and local procedures for preventing property losses as well as their responsibility for the care and protection of government property.

CHAPTER 4

THE SECURITY FORCE

0400. GENERAL

a. The local Navy security force consists of designated persons specifically organized, trained, and equipped to provide physical security and law enforcement under the authority of a Navy commanding officer. (The mission is limited by both jurisdiction and authority to the protection of naval operations and forces.)

b. Security forces at Navy activities are composed of military and civilian personnel performing law enforcement or security functions for Navy installation/activity commanding officers. Military security forces include rated Master-at-Arms and Law Enforcement Specialists (Navy Enlisted Classification 9545), hereafter referred to as Navy Security Forces. Civilian security force personnel are either civil service employees who are locally hired (also referred to as Navy Security Forces) or contractor personnel. Whether composed of military, civil service, or contractor personnel, the commanding officer is expected to employ members of the security force in an overall coherent and integrated manner. Contractor personnel will not be assigned to perform law enforcement duties (reference (p) pertains).

c. To avoid unnecessary duplication of effort among host installations and their tenant activities and other installations/activities within the same geographical region, commanding officers are to integrate the efforts of their security forces whenever appropriate and feasible, and develop support agreements with local, state, and federal entities.

d. In overseas locations certain Navy activities are also protected by foreign nationals. In such cases, rules and policies governing these guards as part of the security force will be determined locally per applicable agreements.

0401. FUNCTIONS OF THE SECURITY FORCE. Security force functions fall into four general categories:

a. Provide force protection, e.g., deter and detect terrorism and criminal activity.

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

c. Protect life and property.

d. Enforce rules, regulations, and statutes.

0402. SIZE OF THE SECURITY FORCE. The size of the security force is dependent upon many factors including:

a. Size and location of the activity.

b. Assets to be protected.

c. Number of posts and the number of hours that each is manned.

d. Degree of supervision that is appropriate considering the training and experience of security force members.

e. Number, type, and size of restricted areas including the number of separate entry points.

f. Use of alternate security support measures and effectiveness of mechanical or electronic security measures.

g. Security force support provided by other agencies.

h. Total daily population of the installation or activity and its composition.

i. Regional coordination and integration of security force requirements and employment to avoid unnecessary duplication of effort.

0403. DETERMINATION OF POSTS

a. Guarding and security patrolling of areas must be commensurate with the importance of the area/assets being guarded and the threat. Since no two activities will present the same degree of risk or contain identical situations (e.g., combatant support vs. "campus"), it is impractical to set fixed rules to apply to all activities.

b. Commanding officers must ensure that an analysis of their command is performed to determine the number and type of posts required to provide optimum and cost-effective protection. Entry points will be limited to the minimum number required. Consideration should be given to employing alternate security measures such as electronic access control systems, electronic intrusion detection systems, closed circuit television, securing nonessential personnel and vehicle entry points, etc.

c. A general rule of thumb, but not a hard and fast rule, for estimating the number of personnel per post is that a post manned 24 hours a day, 7 days a week needs approximately six personnel. Such estimates and the general rule of thumb may be adjusted based on local experience and conditions.

d. See discussion in chapter 1 of required continuing review and assessment processes.

0404. SECURITY FORCE ORDERS. The commanding officer of each installation or activity will publish and maintain security force orders pertaining to each fixed and mobile post. These orders are the written and approved authority of the commanding officer for members of the security force to execute and enforce regulations. The concept of security force orders is as follows:

a. All security force orders will specify the limits of the post, the hours the post is to be manned and the special orders, duties, uniform, arms and equipment prescribed for members of the security force. Additionally, all orders will contain guidance in the use of force, as outlined in reference (l).

b. All security force orders will be brief, concise, specific and current. They shall be written in clear and simple language. Security force orders will be under constant review and updated as required. Manpower/funding constraints mandate continuing efficient use of available security force personnel. This makes it appropriate for the security officer to conduct a total detailed review of all security force orders at least semiannually.

c. Security force orders for military and civilian guards and police will be approved and signed by the commanding officer.

0405. ARMING

a. Authority to Arm Security Force Personnel. The authority to arm security personnel is vested in the commanding officer by reference (l), or, in overseas locations, as governed by Status of Forces Agreements, North Atlantic Treaty Organization, or local agreements. In the exercise of this authority, commanding officers will comply with reference (l).

b. Navy military and civilian personnel regularly engaged in law enforcement or security duties shall be armed.

(1) No person will be armed unless currently qualified in the use of assigned weapons. In order to qualify, Navy military and civilian personnel performing physical security/law enforcement functions must satisfactorily complete the firearms training outlined in reference (m).

(2) NO CONTRACT GUARD WILL BEAR FIREARMS ON BOARD A NAVY INSTALLATION OR ACTIVITY UNTIL WRITTEN CERTIFICATION OF QUALIFICATION MEETING NAVY STANDARDS (reference (m) pertains) IS PROVIDED BY THE CONTRACTOR, AND THE GUARD HAS SUCCESSFULLY COMPLETED TRAINING IN THE USE OF FORCE AND RULES OF ENGAGEMENT. In addition, contractors must comply with provisions prescribed by the state in which the contract is administered, including current licensing and permit requirements.

0406. USE OF FORCE INCLUDING DEADLY FORCE. Mandatory requirements and guidance concerning use of force including deadly force are outlined in reference (l).

0407. PRIVATELY-OWNED (PERSONAL) WEAPONS PROHIBITED

a. THE USE AND/OR POSSESSION OF PRIVATELY OWNED (PERSONAL) WEAPONS AND AMMUNITION BY MILITARY AND CIVILIAN PERSONNEL WHILE IN THE PERFORMANCE OF ASSIGNED DUTIES IS STRICTLY PROHIBITED.

b. Only Government-owned weapons and standard military ammunition officially issued for on-duty use in the performance of law enforcement/physical security functions may be carried by security force members.

c. Off-duty security force personnel are not authorized to keep government-owned weapons in private residences, either on or off the installation. Government-owned weapons will only be stored in approved security containers or armories per reference (e). Weapons must be returned to approved storage after completion of duty or training.

0408. COMPOSITE SECURITY FORCE

a. When a composite security force is in place, civil service, contract, and military assets will be employed in an overall integrated, coherent manner. Contractor personnel will not be assigned to perform law enforcement duties (reference (p) pertains).

b. Integration of Police and Fire Protection. The security officer may supervise both protection forces as separate functions. Except for consolidation of alarm monitoring and central dispatch of security, fire protection, and rescue forces, activities will not normally consolidate or integrate police or guard forces with fire protection forces. In any event:

(1) The capability must exist to accommodate urgent and simultaneous requirements for responses by fire/rescue and by security forces whether to related or unrelated emergencies.

(2) The need to perform one of these missions must not become the reason why the other mission cannot be timely and adequately performed.

(3) Each requires personnel who are specifically and adequately trained and equipped (including the ability to maintain simultaneous communications) for each mission.

0409. MARINE CORPS SECURITY FORCES (MCSF). MCSF are available to support Navy Security Forces under specifically validated situations to protect priority assets. Other mission, functions,

requirements, and guidelines concerning MCSFs are discussed in reference (q).

0410. CIVILIAN MEMBERS OF A COMMANDING OFFICER'S SECURITY FORCE.

a. General Requirements. In general, security force personnel should be physically agile, mentally alert, and possess good judgement.

b. Contracting for Guard Services

(1) Scope. This paragraph applies to the procurement of existing or new contractor guard service (as permitted by existing law) requirements within the Navy.

(2) Policy

(a) Contractor personnel will not be assigned to perform law enforcement duties (reference (p) pertains).

(b) All contract guard services will be obtained through the Naval Facilities Engineering Command (COMNAVFACENGCOM), except when COMNAVFACENGCOM advises that these services are to be obtained through the General Services Administration.

(c) The current edition of the joint Naval Criminal Investigative Service/COMNAVFACENGCOM Guard Services Contract Performance Work Statement (NOTAL) (reference (p)) will be used as the applicable statement of requirements. These requirements may be revised by COMNAVFACENGCOM to include any additional requirements for Navy contracts that may become appropriate or required per other authorities.

(d) Contract guard personnel performing guard services on board a Navy installation or activity within CONUS shall have a completed favorable National Agency Check prior to assignment.

c. Civilian Civil Service Members of Security Force. Minimum Civil Service qualifications of security force personnel are specified in Civil Service qualification standards. Positions will be classified based on duties actually performed.

0411. AUGMENTATION OF SECURITY FORCE FOR EMERGENCIES. As part of the crisis management portion of the Physical Security Plan, plans must be prepared for security force personnel to provide additional security, as required, during emergencies to include providing for augmentation by the Auxiliary Security Force (ASF) and other additional personnel and equipment. These plans should also provide for the essential training of augmentation personnel and rapid identification and acquisition of emergency equipment and supplies.

0412. ASF

a. General. All Navy installations (or regions) with a military population will form an ASF. The parent Echelon 2 command may approve alternate measures to this requirement. The ASF is used to augment the installation's permanent security force during increased threat conditions, or when directed by the host command. It will be responsive to the overall direction of the installation security officer.

b. The size of the ASF will depend largely on the size of the installation, criticality of assets to be protected and the number of personnel required to man additional security posts to protect mission essential assets. As a guide, the ASF should be sized to permit full manning of posts and patrols required in threat condition delta and sustain that security posture for at least 5 days.

c. Composition. The ASF will be composed of permanently assigned military personnel from the host and tenant activities. It should be organized into two watches and should include supervisory personnel as well as individual post standers. ASF personnel will meet Navy standards for weight and have passed the physical fitness test prior to assignment. Additionally, individuals will be mature, possess sound judgement, have no drug or alcohol dependency, and have no non-judicial punishment, nor civil (other than minor traffic violations) or courts-martial convictions in the previous 2 years.

d. Training

(1) Personnel assigned to the ASF will be trained in antiterrorism skills by Marine Cadre, or by Mobile Training Teams from the Marine Corps Security Force (MCSF) Battalion, or by Navy security personnel who are graduates of the cadre school.

(2) Following initial training and weapons qualification, ASF members should be assigned security duties 2 days a month as a means of continued training. Furthermore, the entire ASF should be employed in conjunction with a semiannual installation force protection exercise realistically tailored to prepare members for operational commitments or other incidents that may occur within their areas of responsibility. The intent is that ASF members use rather than lose the skills that they learn during training.

(3) All ASF personnel will be qualified with the type of weapon assigned and will periodically receive training in the use of force per chapter 9 of this manual.

(4) ASF training schedules are to be established and monitored by the security officer.

(5) Appendix V contains minimum training requirements for the ASF.

(6) ASF training records for military personnel shall accompany the member to his/her next duty station for the benefit of informing the gaining commanding officer of the ASF training already received by the member.

e. Weapons and Equipment. The host installation (or regional) command will provide ASF personnel with weapons and equipment necessary to perform the missions described here.

(1) Establishment of small arms/weapons allowances will be requested by the host installation or regional command per reference (r).

(2) Initial issue and replacement of small arms/weapons will be provided at no cost to the requesting activity per reference (r). All other security equipment and uniforms should be ordered through the Navy supply system.

CHAPTER 5

INSTALLATION ACCESS AND CIRCULATION CONTROL

0500. GENERAL

a. A system of personnel and vehicle movement control is a required basic security measure at Navy installations and activities. The degree of control must be in keeping with the sensitivity, classification, value or operational importance of the area. Visitor control relative to classified information will be in compliance with reference (a). Procedures will be coordinated among activities in the same geographical region when appropriate and feasible.

b. This chapter prescribes general policies for controlling entry into and exit from Navy installations. Access control is an integral part of the installation physical security program. Each installation or separate activity commanding officer must clearly define the access control measures (tailored to local conditions, e.g., Navy training "campuses") required to safeguard facilities and ensure accomplishment of the mission.

c. This chapter also prescribes general policies for establishment of restricted areas whether by host installations, tenant activities, or by separate activities.

0501. POLICY. It is DoD policy that procedures to control access to installations and separate activities shall be developed, established, and maintained, including the following:

a. Using a defense-in-depth concept to provide gradated levels of protection from the installation perimeter to critical assets.

b. Determining the degree of control required over personnel and equipment entering or leaving the installation.

c. Prescribing procedures for inspecting persons, their property and vehicles at entry and exit points of installations or at designated secure areas within an installation, and while on the installation.

(1) This shall include determination of whether inspections are randomly conducted or mandatory for all.

(2) All procedures shall be reviewed for legal sufficiency by the appropriate general counsel or legal advisor to the Navy installation/activity prior to issuance.

d. Enforcing the removal of, or denying access to, persons who are a threat to order, security, and the discipline of the installation.

e. Designating restricted areas to safeguard property or material for which the commander is responsible.

f. Using randomized antiterrorism measures within existing security operations to reduce patterns, change schedules and visibly enhance the security profile of an installation. This reduces the effectiveness of preoperational surveillance by hostile elements.

0502. INSTALLATION ACCESS. Installation/activity commanding officers shall:

a. Determine necessary access controls based on the results of review and assessment processes discussed in chapter 1 and considerations discussed in chapter 2. This will include the evaluation of automated entry control systems or access devices, where appropriate.

b. Allocate resources necessary to enforce the established controls. These controls will be monitored and evaluated to ensure adequate protection is maintained.

0503. ACCESS AUTHORIZATION AND CONTROL SYSTEM REQUIREMENT

a. The methods used to control personnel access at an activity will be included in written procedures in the Physical Security Plan, and will include the following:

(1) Designation of restricted areas.

(2) Description of access control methods in use.

(3) Method for establishing authorization for entering and leaving each area, as they apply to both personnel continually authorized access to the area and to visitors, including any special provisions concerning non-duty hours.

(4) Details of where, when, and how security badges will be displayed.

(5) Procedures to be followed in case of loss or damage to security badges.

(6) Procedures to recover issued security badges.

(7) Measures to deny illicit use of lost, stolen, sold, or other illegally acquired security badges.

0504. EMERGENCY PLANNING

a. Installation/activity commanding officers will plan for increasing vigilance and restricting access at installations/activities under the following situations:

(1) National emergency.

(2) Disaster.

(3) Terrorist threat conditions (see references (g) through (j) for further information).

(4) Significant criminal activity.

(5) Civil disturbance.

(6) Other contingencies that would seriously affect the ability of installation personnel to perform their mission.

b. Planning should include the following:

(1) Coordination with local, State, Federal, or host country officials to ensure integrity of restricted access to the installation and reduce the effect on surrounding civilian communities;

(2) Establishment of a system for positive identification of personnel and equipment authorized to enter and exit the installation;

(3) Maintenance of adequate physical barriers that will be installed to control access to the installation;

(4) Predesignation of posts to be manned, personnel, equipment, and other resources to enforce restricted access and respond to incidents;

(5) Exercising contingency plans to validate their effectiveness, including systems for alerting and evacuation of personnel.

0505. AREA PROTECTION AND CONTROL

a. Prior to making decisions to employ additional physical security measures for a specific area(s) within the installation or activity, a thorough risk and threat analysis must be performed to determine the degree of physical security required.

(1) The continuing review and assessment processes described earlier in chapter 1, and the planning considerations outlined in chapter 2 are to be used.

(2) Only after these factors are addressed can appropriate controls for specific areas be decided on and instituted.

b. Restricted Areas

(1) Restricted areas are designated in writing by a commanding officer who has jurisdiction over the area. These areas are established under DoD Directive 5200.8 of 25 April 1991 (enclosed in reference (s)), and Section 21, Internal Security Act of 1950; Ch. 1024, 64 stat. 1005; 50 U.S.C. 797).

(2) General policies and standards for restricted areas are outlined in appendix VI.

c. Enclave Security Concept. Essentially, enclaving is the provision of concentrated security measures at specific sites, usually designated as restricted areas, within an installation or activity, such as flightline areas and waterside areas or other large critical/essential assets for which a higher degree of protection is appropriate.

0506. WATER BOUNDARIES. Water boundaries present special security problems. Such areas should be protected by barriers, and posted. In addition to barriers, patrol craft should be used at activities or installations whose waterfronts contain critical assets, or which are otherwise essential to the mission of the installation or activity. In inclement weather, such patrols cannot provide an adequate degree of protection, and should be supplemented by increased waterfront patrols, watch towers, military working dog teams, and other appropriate waterside security systems.

0507. ENFORCEMENT OF MOVEMENT CONTROL

a. Enforcement of movement control systems for restricted areas rests primarily with the activity personnel who normally work in the areas.

(1) If this control is based on personal recognition, all personnel in restricted areas will be instructed to consider each unrecognized individual as a person whose authorization to be in the area is in doubt, and to maintain observation of and report them to their supervisor, the security officer, or other appropriate authority.

(2) If security badges are used, all personnel will be similarly instructed to consider each unbadged or an apparently improperly security badged individual as a person whose authorization to be in the area is in doubt, and to similarly report their presence.

b. Written procedures will be incorporated into the local Physical Security Plan to cover these requirements.

c. Consideration may be given to the use of CNO-approved, commercially available access control systems to enhance enforcement of movement controls within a facility. These

systems facilitate access control, while reducing the number of personnel required.

0508. SIGNS AND POSTING OF BOUNDARIES. Signs and posting of boundaries are addressed in appendix VII.

0509. VEHICLE MOVEMENT CONTROL. Vehicles will be controlled as necessary to:

a. Control movement of the personnel associated with the vehicles.

b. To manage risk of using vehicles for unauthorized removal of government property or bringing aboard unauthorized items.

c. To manage risk of vehicle bombs. To mitigate the effectiveness of a vehicle bomb attack, commanders shall be continually vigilant against allowing vehicle parking near high-density, soft target buildings. Every attempt should be made to establish a minimum of a 50-foot stand-off where possible. Parking regulations should be strictly enforced. During THREATCON Bravo, commanders will achieve a 100-foot or more vehicle stand-off from high density soft targets. AT THREATCON Charlie or Delta, a 400-foot stand-off should be achieved. Centralized or remote parking should be instituted at THREATCON Charlie or higher. Traffic patterns shall be a consideration in AT/FP plans.

0510. PARKING OF PRIVATELY OWNED VEHICLES

a. Privately owned vehicles should not be parked in any restricted area, as such parking exacerbates the risks and increases resources required to maintain appropriate access control.

b. Privately owned vehicles should not be parked near doorways leading into or from buildings primarily used for the manufacture, repair, rework, storage, handling, packaging or shipping of government material and supplies.

c. Parking decisions should also consider means of minimizing danger in the event of vehicular fire or explosion.

0511. ADMINISTRATIVE INSPECTION OF VEHICLES

a. All vehicles on Navy installations are to be subject to administrative inspection according to procedures authorized by the commanding officer. As ordered and directed by the commanding officer, authorized security personnel will administratively inspect vehicles entering or leaving the installation. Such inspections are deemed reasonably necessary to protect the premises, material and utilities from loss, damage or destruction.

b. To be effective, these administrative inspections must be conducted frequently enough so that personnel remain mindful that the inspections are a real possibility, and that they could be inspected at any time they enter or leave the area.

c. It is better to frequently conduct inspections of a few vehicles at any one time than to infrequently inspect a lot of vehicles at any one time.

d. No person or group may be exempted from, or singled out for, such inspections, and the instruction by commanding officers regarding such inspections shall be coordinated in advance of implementation with local Judge Advocate General (JAG) or Naval Legal Service Office officials to ensure strict adherence to either mandatory inspection of all vehicles or a structured random inspection pattern that is impartial and unbiased.

e. Naval Criminal Investigative Service. Naval Criminal Investigative Service (NAVCRIMINVSERV) personnel, upon presentation of their special agent credentials when entering or leaving Navy installations, vehicles used by them in the course of official business, and all occupants therein are exempt from administrative inspections, per reference (t).

0512. SPECIAL PRECAUTIONS. Personnel responsible for the accomplishment or implementation of personnel and vehicle control procedures shall at all times be watchful for the unauthorized introduction to or removal from the installation of government property, especially weapons, ammunition and explosive materials. This includes all personnel and means of transportation, including government, private and commercial vehicles, aircraft, railcars, and ships.

0513. CONTROL AND ACCOUNTABILITY OF PERSONAL WEAPONS

a. All personal weapons brought aboard a Navy installation or activity must be registered with the security department. Weapons which must be registered shall include:

(1) Pistols/revolvers.

(2) Crossbows.

(3) Rifles.

(4) Shotguns.

(5) Other instruments designed to expel a potentially lethal projectile, as designated by the commanding officer.

b. All Navy installations and activities shall implement procedures for the strict control and accountability of

personal weapons on board. Procedures shall include, but are not limited to:

(1) Registration, inventory, and deregistration of personal weapons.

(2) Identification of all personal weapons. Firearms will be identified by manufacturer, caliber, model and serial number.

(3) Semiannual sight inventories by serial number of personal weapons stored in armories or weapons containers.

(4) Storage of personal weapons.

c. Registration Requirements

(1) Weapons shall be registered within 72 hours after being introduced aboard.

(2) Weapons are not required to be brought in to be registered.

(3) Registrant must present proof of ownership.

d. Storage. Personal weapons introduced into an installation or activity will be stored in an approved armory or weapons container. Personal weapons shall not be kept or stored in barracks, bachelor officer quarters, bachelor enlisted quarters, evidence lockers (unless the weapon is controlled as actual evidence), or with security force in-service storage areas/containers.

(1) Host commands should provide storage for tenant command personal weapons, particularly those tenant commands without approved armories or available storage containers.

(2) Personnel residing in family housing may store their (registered) weapon(s) in their quarters at the discretion of the installation (host) commanding officer.

e. Lost, Sold or Stolen Personal Weapons

(1) The loss or sale of personal weapons will be promptly reported to the security officer.

(2) Discovery of stolen personal weapons will be immediately reported to the security officer.

f. Concealed Weapons. Personal weapons shall not be carried concealed aboard a Navy installation or activity.

CHAPTER 6

BARRIERS AND OPENINGS

0600. THE PURPOSE OF PHYSICAL BARRIERS. Physical barriers control, deny, impede, delay and discourage access by unauthorized persons. They accomplish this by:

a. Defining the perimeter of restricted areas.

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

c. Optimizing use of security forces, by separating the innocent from the suspicious.

d. Enhancing detection and apprehension opportunities.

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

0601. TYPES OF BARRIERS. Major types of physical barriers are:

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

b. Structural - fences, walls, doors, gates, roadblocks, vehicle barriers, etc.

0602. GENERAL CONSIDERATIONS. Physical barriers delay, but cannot be depended upon alone to stop a determined intruder. Therefore, to be effective, such barriers must be augmented by security force personnel or other means of protection and assessment. In determining the type of barrier required, the following will be considered:

a. Physical barriers will be established along the designated perimeter of all restricted areas. The barrier or combination of barriers used must afford a minimally acceptable equal degree of continuous protection along the entire perimeter of the restricted area.

b. In establishing any perimeter barrier, consideration must be given to providing emergency entrances and exits in case of fire. However, openings will be kept to a minimum consistent with the efficient and safe operation of the facility, to minimize the degree of resources required for security.

0603. FENCES

a. Federal standards and specifications for chain link fencing, gates, and accessories are outlined in references (u) through (y). To economize the use of security force personnel and increase detection by all parties in the area of any suspicious activity, mesh openings will not normally be covered, blocked, or laced with material which would prevent a clear view of personnel, vehicles, or material in the outer or inner vicinity of the fence line.

(1) Measures will be taken to prevent the effective height of the fence from being lowered by pulling down on the top of the fence fabric. Similarly, measures will be taken to prevent enough room being made to surreptitiously crawl under the fence by pulling up on the bottom of the fence fabric.

(2) The bottom of the fence fabric must be close enough to firm soil or buried sufficiently to prevent surreptitious entry under the fence.

(3) Culverts under or through a fence shall be secured to prevent their use for surreptitious entry.

(4) No fence will be located so that the features of the land (its topography) or structures (buildings, utility tunnels, light and telephone poles, fire escapes, trees, vines, ladders, etc.) aid passage over, around, or under the fence, without taking of compensatory measures. These measures will be documented in the physical security plan.

0604. WALLS. Walls may be used as barriers in lieu of fences. The protection afforded by walls shall be equivalent to that provided by chain link fencing. Walls, floors, and roofs of buildings may also serve as perimeter barriers.

0605. TEMPORARY BARRIERS. In some instances, the temporary nature of a restricted area does not justify the construction of permanent perimeter barriers. This will be compensated for by additional security forces, patrols and other temporary security measures during the period the restricted area is established.

0606. CLEAR ZONES

a. Where fences are used as restricted area perimeter barriers, an unobstructed area or clear zone should be maintained on both sides of the restricted area fence. Similarly, where exterior walls of buildings form part of restricted area barriers, an unobstructed area or clear zone should be maintained on the exterior side of the building wall. The purpose of such areas is defeated if vegetation is high enough to provide concealment of a person lying prone on the ground. Vegetation or topographical features which must be retained in clear zones for

erosion control or for legal reasons shall be trimmed or pruned to eliminate concealment or be checked by security patrols at irregular intervals.

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

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

d. Obstacles which are within exterior and interior clear zones and represent no aid to circumvention of the perimeter barrier or do not provide concealment (nor provide a plausible reason to appear innocently loitering) to an intruder do not violate the clear zones considerations.

e. In those activities where space on government land is available, but the fence does not meet clear zone guidelines 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, etc., to compensate for the close proximity of aids to concealment or access. All fencing should be kept clear of visual obstructions such as vines, shrubs, tree limbs, etc., which could provide concealment for an intruder.

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

0607. INSPECTION OF BARRIERS. Security force personnel should check restricted area perimeter barriers at least weekly for defects that would facilitate unauthorized entry and report such defects to supervisory personnel. Personnel must be alert to the following:

a. Damaged areas.

b. Deterioration.

c. Erosion of soil (intent here applies mostly to instances where a fence is used as the perimeter barrier).

d. Growth in the clear zones that would afford cover for possible intruders, and concurrently hinder effectiveness of any protective lighting, assessment systems, etc. If not removed, the growth described here and the obstructions described in the paragraph below could result in requiring more manpower to patrol the affected areas than would be the case if there were no such growth or obstructions.

e. Obstructions which would afford concealment or aid entry/exit for an intruder, or provide a plausible excuse to openly loiter without need for hiding (e.g., a bus stop next to the fence line).

f. Signs of illegal or improper intrusion or attempted intrusion.

0608. RESTRICTED AREA PERIMETER OPENINGS. Openings in the perimeter barrier will be kept to the minimum necessary for the safe and efficient operation of the activity. Access through such openings must either be controlled, or the openings must be secured against surreptitious entry, or other compensatory measures taken as a minimum. If the perimeter barrier is designed to protect against forced entry, then any openings in the barrier must afford protection against forced entry or other compensatory measures taken. These openings will be frequently inspected by security patrols.

0609. 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 (references (z) and (aa) pertain). For new construction at outside continental United States facilities, review reference (z) for appropriate stand-off distances. An interim buffer of at least 400 feet is recommended for high occupancy facilities.

CHAPTER 7

PROTECTIVE LIGHTING

700. GENERAL. Protective (or security) lighting increases the effectiveness of security forces performing their duties, has considerable value as a deterrent to thieves and vandals and increases the risk or uncertainty for a terrorist. As with ordinary sunlight during the day, protective lighting at night is useful for the ability of detection by security forces, or risky for the intruder only to the extent the intruder can be seen. Protective lighting serves little purpose if there are no clear zones requiring that intruders be exposed to sight rather than remain hidden from view. Requirements for protective lighting at an activity will depend upon the situation and the areas to be protected. In the interest of finding the best possible mix between energy conservation 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.

0701. GENERAL PRINCIPLES AND GUIDELINES. Reference (ab) provides general principles and guidelines for exterior protective (security) lighting. When protective lighting is installed and used, the following basic principles, in addition to those provided in reference (ab), should also be applied:

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

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

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

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

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

the system should be located to provide maximum protection against intentional damage.

f. Meet requirements of blackout and coastal dim-out areas.

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

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

i. When considering the above, do not overlook possible applications of on demand infrared lighting.

0702. PROTECTIVE LIGHTING PARAMETERS. It is not the intent of this instruction to prescribe specific protective lighting requirements. The commanding officer must decide what areas or assets to illuminate and how to do it. This decision must be based upon the following:

a. Relative value of items being protected.

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

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

d. Availability of clear zones so that any intruders, with no place to hide, must risk being seen because of the light.

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

f. Energy conservation.

0703. EMERGENCY POWER. Restricted areas provided with protective lighting should have an emergency power source located within the restricted area. Emergency power systems shall be tested periodically lest it be discovered when it is most needed that it does not work.

0704. WIRING SYSTEM. Multiple circuits may be used to advantage in protective lighting systems. The circuits should be so arranged that the failure of any one lamp will not darken

a long section of a critical or vulnerable area. The restricted area protective lighting system should be independent of other lighting systems.

0705. PROTECTION - CONTROLS AND SWITCHES. Controls and switches for restricted area protective lighting systems should be inside the protected area or otherwise secure so that they cannot be turned off by unauthorized persons to facilitate their concealment. High impact plastic shields may be installed over lights to prevent destruction.

CHAPTER 8

ELECTRONIC SECURITY SYSTEMS (ESS)

0800. PURPOSE. ESS are used to accomplish the following:

a. 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.

b. Provide additional controls at critical areas or points.

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

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

0801. ESS DETERMINATION FACTORS. The following factors must be considered to determine the feasibility and necessity of installing ESS equipment:

a. Mission.

b. Criticality.

c. Threat.

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

e. Accessibility to intruders.

f. Availability of other forms of protection.

g. Life cycle cost of the system.

h. Construction of the building or facility.

i. Hours of operation.

j. Availability of a security force and expected response time to an alarm condition.

0802. INTRUSION DETECTION SYSTEM POLICY (IDS)

a. IDS are designed to detect, not prevent, actual or attempted penetrations. Therefore, IDS are useless unless supported by near-real-time assessment systems and prompt security force response when the systems are activated.

b. If a computerized IDS is used, it must be safeguarded against tamper.

c. Exterior or interior IDS will be standardized commercial equipment approved by CNO (N09N3). Presently installed IDS, not meeting the standards of this instruction, may continue to be used until replacement is necessary. Waivers/exceptions to use presently installed IDS are not required. Industry standards, including Underwriters Laboratory 611, 681, 1076, and 2050 should be met.

d. The data/signal transmission subsystem links sensors with control and monitoring consoles.

(1) Alarm transmission lines between the protected area and monitoring units will be protected by electronic line supervision systems to detect any signal cutting, shorting, tampering, splicing, or substitution on the sensor signal data transmission network, or by physical measures to prevent these actions.

(2) All sensors, transmitters, transponders, control units and other IDS components associated with a protected zone will be physically located within the protected area or, if not practical because of design or safety constraints, will alternatively be located within enclosures that are resistant to physical attack and are protected by sensors that will detect unauthorized opening or tamper.

e. Emergency Backup Power. IDS shall have an emergency power source to ensure the system's continuous operation. Emergency backup power sources usually consist of rechargeable batteries, emergency generator, or both.

f. Keyswitches, controllers, or other mechanisms used to activate and deactivate the IDS will be installed inside the protected area. Alarm activation delay devices are available which will allow sufficient time for personnel to exit the protected area after the system is activated.

g. IDS equipment whose housing can be opened will be fitted with anti-tamper devices which will initiate an alarm signal. The anti-tamper system will be in continuous operation regardless of the IDS mode of operation (access/secure/day/night).

h. Central Alarm Stations. Where practical, alarm consoles and central dispatching should be consolidated. These alarm stations should be in controlled access areas and properly protected. New construction should include ballistic protection. Consoles should not be visible to the exterior of the facility.

i. Alarm Response. The metric for response by the first law enforcement patrol is for priority A assets and life

threatening situations: 5 minutes. For all others: 15 - 45 minutes.

0803. MAINTENANCE

a. Requirements. Proper maintenance of an IDS is imperative.

b. IDS Functional Testing. Must be tested frequently enough to ensure system reliability.

(1) Consider recommendations of equipment manufacturers and installers.

(2) Consider actual experience.

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

(4) Keep records of when components are functionally tested. When components are found to be inoperable, records will indicate the date of discovery and the date the component was last positively verified to be working.

c. IDS Preventive Maintenance

(1) Commanding officers will:

(a) Establish an IDS preventive maintenance schedule based on industry standards and actual experience with the system.

(b) Keep records of their preventive maintenance and unscheduled component/system outages to include identification of component/system element which caused each outage, consequential costs, and manpower impact including compensatory measures.

0804. CLOSED CIRCUIT TELEVISION. Closed circuit television (CCTV) is very useful in physical security operations and is frequently used to complement an IDS or with Video Motion Detection. Closed circuit television may be used at entry points that are not manned continuously in conjunction with electronic access control systems. Closed circuit television also has application in the video detection and assessment of alarms. In this configuration, the CCTV can be triggered automatically or by personnel at the alarm control center and can be used to determine whether response forces should be dispatched. CCTV can minimize the number of security personnel normally needed for checking identification at gates, or for patrol or observation posts.

0805. ELECTRONIC ACCESS CONTROL SYSTEMS USING MAGNETIC STRIPES. All new acquisitions of electronic access control components involving use of magnetic stripes will adhere to specifications in reference (ac).

CHAPTER 9

PART ONE

SECURITY EDUCATION AND TRAINING

0900. SECURITY EDUCATION PROGRAM

a. General

(1) The security responsibility of every member of the Navy and every civilian employee of the Navy must be stressed in a continuous, vigorous security education program.

(2) To be effective, a security program including antiterrorism and force protection must be supported by a security education program for all hands. Security force personnel cannot go it alone without the active interest and support of everyone.

(3) Strive to get everyone vigilant and concerned about security, antiterrorism, and force protection. One of the greatest challenges involves heightening their awareness and instilling a "feeling of ownership". History shows time and again instances where loss, damage and theft were wholly or in part attributable to a lack of care, concern, or awareness. Consequently, commanders and supervisors can make a significant contribution to security, antiterrorism, and force protection by developing an awareness and conscious concern for security within their organizations.

b. Requirement

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

(2) The Security Education Program will include all pertinent aspects of physical security, law enforcement, and loss prevention programs including those specifically related to force protection and antiterrorism. Many aspects of these programs have a direct personal application to activity personnel.

(3) Initial security instruction. All personnel, military and civilian, shall receive initial security instruction.

(4) Refresher security training shall be given to the extent necessary to ensure personnel remain mindful of and proficient in meeting their security responsibilities (see discussion in chapter 1 of continuing security review and assessment process).

c. Objectives

(1) To involve individually and collectively all military and civilian personnel in the protection of installation assets.

(2) To instruct each individual and keep him/her proficient in the security procedures applicable to the performance of his/her duty.

(3) To ensure that all personnel understand the need for security, as well as the possible consequences to their co-workers of security lapses or breakdowns.

(4) To ensure that general security measures in effect and the reasons for them are fully understood by all personnel. If they do not understand why, they are less likely to comply.

CHAPTER 9

PART TWO

SECURITY FORCE TRAINING

0901. GENERAL

a. This chapter addresses education and training requirements for the security force.

b. Minimum training standards are essential to enable security force personnel to perform their duties in a professional manner, including representing the Navy while in contact with visitors to Navy installations and activities.

0902. DUTIES AND RESPONSIBILITIES

a. CNO (N09N3) as the program manager for Navy physical security, law enforcement and antiterrorism matters will:

(1) Provide technical assistance and guidance to individual commands.

(2) Review physical security, law enforcement, and antiterrorism course curricula for changes to course curricula prior to implementation to ensure commonality.

b. Commanding officers will ensure that adequate physical security and antiterrorism (including force protection) training is conducted for all security force personnel, per this instruction and other applicable directives, instructions and regulations (e.g., references (g) through (j)).

0903. TRAINING REQUIREMENTS

a. Basic training required for military Navy Security Forces (both Master-at-Arms and Navy Enlisted Classification 9545, Navy Law Enforcement Specialist) is conducted at the Joint Law Enforcement Training Center, Naval Technical Training Center Detachment, Lackland Air Force Base, San Antonio, TX.

b. Basic training for new hire Civil Service Navy Security Forces will, at a minimum, consist of Phase I and other specific training equivalent to that afforded Masters-at-Arms and NEC 9545 personnel at the Joint Law Enforcement Training Center, Lackland AFB. Completion of the basic law enforcement course at the Federal Law Enforcement Training Center, Glynco, GA, is encouraged for new hires in the GS-083 series.

c. All personnel assigned full time physical security/law enforcement functions must successfully complete Phase I (basic) training as stipulated in appendix VIII. Personnel temporarily assigned to security duties for only a short period (e.g., 6

months or less) need not complete all of Phase I, but only those portions specifically applicable to the duties to which they are temporarily assigned, with a degree of supervision appropriate to their general lack of experience and training.

d. Contract guard personnel will receive training as outlined in appendix VIII and any additional training required by the State or local jurisdiction(s). Such training is the responsibility of the contractor. All contract security personnel will be trained within 30 days of commencement of the contract or employment. Contract security personnel will be qualified per appendix VIII, with the appropriate weapon prior to being armed.

0904. IN-SERVICE TRAINING PROGRAM

a. Minimum maintenance of training standards is essential to enable security force personnel to perform their duties in a professional manner.

b. Phase II Training Course. Each activity will conduct Phase II training course annually for all security force personnel. The course of instruction is outlined in appendix IX.

c. Periodic review of instructional material and instructors' presentations shall be conducted to determine how effectively they meet the security force training requirements specified herein.

0905. SPECIALIZED AND ADVANCED TRAINING. Specialized and advanced training necessary for efficient and effective operation of a modern security force should be provided. This training includes, but is not limited to, advanced investigative training, intrusion detection systems application training, antiterrorism training, loss prevention training, and advanced physical security/law enforcement training.

0906. FIREARMS PROFICIENCY TRAINING

a. Use of Force Instruction. Security force personnel will not be armed until detailed instructions governing the use of force, including use of deadly force, in the performance of duties are received (reference (l) pertains). Specific instructions governing the use of force will be given quarterly (including in connection with firearms qualifications or training sessions when conducted). A system will be instituted for security force personnel to officially acknowledge an understanding of the rules governing the use of force.

b. Training and Qualification

(1) The objective of firearms training is to ensure that security force personnel are competent and confident in employing firearms with accuracy and speed, and without hazard to

self, coworkers or other innocent parties. To this end, adequate instruction is to be provided concerning policies, procedures and regulations governing the carrying, use, and safety practices relating to firearms. A program of firearms qualification and training is required.

(2) Firearms Instruction and Qualification. All security force personnel (including the Auxiliary Security Force (ASF)) authorized to carry firearms shall be given instruction in the policy, regulations, and safety practices set forth in this instruction and references (l) and (m). Before a firearm is issued, assigned security personnel shall qualify on the Navy Qualification Courses (see references (l) and (m)) using the type of firearm assigned to them in the performance of physical security/law enforcement duties. Personnel will also receive classroom instruction in safety, liability, and use of deadly force (reference (l) pertains).

(3) Annual Firearms Qualification. After initial qualification, security force personnel authorized to carry firearms shall be required to requalify annually with the type of firearm assigned to them in the performance of physical security/ law enforcement duties. Requalification will be completed as outlined in reference (m). Prior to each firearms qualification/requalification session, all security force personnel shall be thoroughly briefed concerning safety procedures, and security department and Navy policies and regulations concerning the carrying and use of firearms, with particular emphasis on the use of deadly force (references (l) and (m) pertain).

(4) Failure to Qualify/Requalify. Should an individual fail to qualify/requalify within the authorized time frame, authorization to carry firearms shall be revoked and a written notice of this revocation shall be made by the security officer and filed in the member's training record/civilian personnel record. The security officer will determine if the individual should continue to receive remedial instruction to qualify/requalify.

0907. CONTRACT GUARD TRAINING.

a. A formal training program shall be provided at contractor expense prior to assigning a contractor employee to perform duties. In addition to other training which may be required, each contract guard shall receive training equal to the basic standards outlined in appendix VIII of this instruction.

b. If armed contract guards are required at Navy installations/activities, the contract will so stipulate, and minimum training standards equivalent to those contained in references (l) and (m) will be prescribed.

CHAPTER 10

SECURITY FORCE COMMUNICATIONS

1000. GENERAL. The activity security force needs sufficient equipment to maintain continuous two-way voice communications among all elements of the security force. Alternate communications systems are needed for use in emergencies to provide for increased communications requirements and to maintain sure and rapid communications throughout the emergency.

1001. GENERAL REQUIREMENTS

a. Permanent fixed posts will be provided with at least two means to communicate. Mobile patrols will be provided a multiple frequency radio or radio and mobile telephone.

b. A duress code (changed frequently, immediately if compromised) to alert all security forces of duress situations.

c. The provisions of reference (d) take precedence, where applicable.

d. Operational tests of all communication circuits will be conducted to ensure they are operating properly. Maintenance inspections of all communications equipment will be conducted periodically by electronics personnel.

1002. COMMUNICATIONS EQUIPMENT. If activities have not already done so, they should consider upgrading their Navy security force communications equipment and systems to include Data Encryption Standard (DES) equipment. Current state-of-the art DES equipment is compatible with older systems and allows time-phase upgrade to a full DES communications system.

CHAPTER 11

SECURITY DEVICES AND EQUIPMENT

1100. GENERAL. This chapter contains information helpful in satisfying specific security equipment requirements and in determining their need. It explains general and specific Navy policies on certain devices and equipment not covered in the preceding chapters and describes their basic characteristics, purposes, and limitations.

1101. SECURITY/LAW ENFORCEMENT VEHICLES

a. Discussion

(1) Standard authorized security/law enforcement vehicles are identified in Federal Standard 122 (as annually amended).

(2) Security/law enforcement vehicles which will be used in or will transit proprietary or concurrent jurisdiction areas on or off station should conform to local and state requirements for the equipping and certification of law enforcement emergency vehicles.

(3) Leasing is usually more practical than procurement because of rapid accumulation of mileage and extensive wear. Requirements for base security/law enforcement vehicles will be filled through leasing except when procurement would be more practical or cost effective. Vehicles should be leased off the General Service Administration's (GSA) Centralized Leasing Program for Surveillance and Law Enforcement Vehicles.

(4) Security/law enforcement vehicle requirements should be coordinated between the security department and the public works transportation department. Requests for all security/law enforcement vehicles will be processed through normal vehicle procurement procedures established by COMNAVFACENGCOM. In the event of a dispute concerning types or quantities of vehicles, the matter will be forwarded to the Echelon 2 command for resolution.

(5) The security force shall be furnished with sufficient vehicles to maintain required patrol standards, respond to alarms and emergencies, and to maintain supervision. Commands should consider leasing costs and fuel economy when determining their security/law enforcement vehicle needs. The following guidance is provided:

(a) Large pursuit sedans are equipped with an eight cylinder engine, are more expensive to lease, and incur greater operating expense. They should be used primarily for traffic enforcement and exclusive law enforcement purposes such

as prisoner transports absent a designated transport vehicle, i.e., patrol wagon.

(b) Midsize patrol sedans are equipped with a six cylinder engine, are more economical to lease, and have lower operating costs. They are recommended for use as patrol vehicles and can generally accommodate prisoner shields, shotgun mounts, and communication consoles.

(c) Security departments may use compact or subcompact vehicles or other means of transportation in lieu of standard security/law enforcement vehicles, e.g., bicycles and patrol craft, where appropriate.

(6) Nonstandard or special use vehicles include vans, patrol wagons specifically designed for prisoner transport, motorcycles, all-terrain-vehicles.

(a) Use of motorcycles and all-terrain-vehicles is hazardous even to well trained operators of those vehicles, and authorization of their use by security force members is strongly discouraged.

(b) Public works departments will provide nonstandard or special use vehicles only when authorized by the Echelon 2 command. Requests for authorization must provide complete justification for nonstandard vehicles and also address safety issues.

(7) Security/law enforcement vehicles will be used by security force personnel solely for the performance of assigned security/law enforcement duties.

b. Vehicle Markings

(1) Various operational endeavors place the security/law enforcement vehicle and security force personnel in hazardous positions requiring immediate identification and visibility. Therefore, these vehicles must be distinctively marked. Distinctively marked security/law enforcement vehicles patrolling throughout an installation, including housing areas, parking lots, restricted areas and roadways, contribute significantly to reducing crime.

(2) Echelon 2 commands will determine that security/law enforcement vehicles used within their commands are adequately marked for the purposes for which the vehicles are used. Vehicles shall be painted the manufacturer's standard gloss white. The word "Police" in 4-inch reflectorized blue letters shall be centered on the rearward facing vertical portion of the trunk lid and to the top front vertical side of both front fenders. A command or regional security department logo of either magnetic or decal manufacture may be applied to the front doors of the vehicle. If these are used, their designs will be

approved by Echelon 2 commands. Echelon 2 commands, when practical and cost effective, should streamline the marking process by such methods as centralizing contract purchases of reflectorized decals for issuance to and application by local security departments.

(3) Whenever possible, all markings or decals on leased vehicles should be removable without damage to the vehicles.

(4) Requests to exempt security/law enforcement vehicles from standard security/law enforcement markings and/or standard Navy markings and identification shall be forwarded to Echelon 2 commands for approval. Approval authorities shall ensure that use of such vehicles is limited to performance of authorized security/law enforcement functions.

c. Related Equipment

(1) Procurement and installation of related equipment such as exterior emergency lights, alley lights, spot lights, sirens, grill lights, dash mounted lights, etc., will generally be the responsibility of the command unless the leasing contract specifies otherwise.

(2) Echelon 2 commands will determine that security/law enforcement vehicles used within their commands are adequately equipped and maintained for the purposes for which the vehicles are used.

(3) Any vehicle which is used to transport detainees will be equipped to safely do so. This will be looked at from both the viewpoint of safety of detainees and the viewpoint of safety of members of the security force.

(4) Security/law enforcement vehicles must be equipped to provide for rapid access by security force members to all their assigned weapons (e.g., shotguns) in a manner that does not require them to unnecessarily expose themselves to danger in order to get to their weapons. Simultaneously and no less importantly, access to the weapons and their use by others (e.g., detainees) must be prevented. To this end, an electronically operated shotgun mount with a concealed release should be used when shotguns are carried in the vehicle's interior.

(5) Before deciding not to support the costs of installing vehicle-mounted spot lights, alley lights, etc., Echelon 2 commands will consider the hazards involved if security force members have only handheld lights to use (e.g., intruders/assailants aiming their blows or weapons at the vicinity of the light held in the hand of the security force member).

(6) In all instances, related equipment will conform, as a minimum, to local state codes. Security/law enforcement vehicles in foreign locations, absent local requirements, shall use flashing red, blue, or a combination of red and blue emergency lights.

d. Vehicle Replacement Standard

(1) Time is of the essence in the performance of security/law enforcement duties. Loss of life or property are the risks of untimely security/law enforcement response or presence due to unreliable vehicles.

(2) Also, as stated above operational endeavors place the security/law enforcement vehicle and security force personnel in hazardous positions which results in placing great dependence for their safety on the reliability of their vehicle.

(3) Therefore, vehicles are to be replaced when they are no longer adequately reliable for the performance of security/law enforcement functions.

e. Overseas activities may deviate from the above vehicle standards when unable to comply because of non-availability of vehicles and/or equipment or restrictions imposed by local Status of Forces Agreements or North Atlantic Treaty Organization agreements if the deviation is approved by their Echelon 2 command.

1102. FIREARMS AND AMMUNITION FOR SECURITY FORCES. The basic weapons issued to civilian/military security force personnel will be the 9mm pistol and the 12 gauge shotgun. THE USE OF PRIVATELY OWNED WEAPONS WHILE ON DUTY IS PROHIBITED. Service rifles are permitted for specific guard duties which require long range shooting such as guard towers. A squad automatic weapon is permitted for use on security patrol boats if the commanding officer has determined that need for such a weapon justifies the additional logistics and training requirements. The security officer and supervisory personnel will annually review firearm and ammunition requirements to ensure that the number of weapons and amount of ammunition available are appropriate.

a. Firearms Allowance List. Command procurement of firearms from other than Navy sources and not included on the Shore Based Allowance List contained in reference (r) is prohibited. Requests for changes in or establishment of firearms allowance will be submitted per reference (r).

b. Firearms allowance is based on the following guidelines. The allowance for security force handguns is normally based on 100 percent of manning. The allowance for Auxiliary Security Force (ASF) handguns is normally based on 50 percent of the size of the ASF. The allowance for shotguns is

normally based on 20 percent of the total security force and ASF membership.

c. The only ammunition authorized will be government-owned, officially procured, and issued for use in the specific weapon carried.

d. The required round for the 12-gauge shotgun issued for security force use is the standard commercial or military manufactured 00 buck. The minimum on-duty issue quantity of shotgun rounds is the number required to load the shotgun initially plus one full reload of the magazine.

1103. CAMOUFLAGE UTILITY UNIFORM AND PROTECTIVE EQUIPMENT

a. Camouflage Utility Uniform. Navy policy concerning the camouflage utility uniform is outlined in reference (ad).

b. Protective Equipment. Body armor and protective masks should be available for issue to security force members.

1104. MILITARY WORKING DOGS (MWD). MWD requirements and guidelines are discussed in reference (ae).

1105. SECURITY BADGES. To assist activities in evaluating strengths and vulnerabilities of security badges, and the manner of their application, the following is provided for information and use as appropriate. Echelon 2 commands will approve adequacy of security badges and their manner of use by their subordinate activities.

a. Security badges are used to both:

(1) Control physical access to an area for security purposes.

(2) Alert other personnel in the area to the presence of unauthorized persons, because such persons are not wearing a badge or are wearing a questionable badge.

b. All new acquisitions of security badge-related components involving use of magnetic stripes will comply with paragraph 0805.

c. Badges should have expiration dates and serial numbers.

d. The following statements should be on security badges:

(1) "U. S. Government Property."

(2) "Loss of this card must be reported at once."

(3) "If found, drop in nearest U. S. mail box."

(a) "Postmaster: Postage Guaranteed. Return to Commanding Officer, (address of the issuing activity indicated on face of security badge)."

(b) "Warning - issued for official use of the holder designated hereon. Use or possession by any other person is unlawful and will make the offender liable to penalty - 18 U.S.C. 499, 506, 701." (Reference should be made to Status of Forces Agreements for overseas activities only).

APPENDIX I

REFERENCES

(a) OPNAVINST 5510.1H, Subj: Department of the Navy Information and Personnel Security Program Regulation

(b) OPNAVINST S5460.4C, Subj: Control of Special Access Programs Within the Department of the Navy (U) (NOTAL)

(c) OPNAVINST 5239.1A, Subj: Department of the Navy Automatic Data Processing Security Program

(d) OPNAVINST C8126.1A, Subj: Navy Nuclear Weapon Security (U) (NOTAL)

(e) OPNAVINST 5530.13B, Subj: Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition, and Explosives (AA&E)

(f) OPNAVINST 5210.16, Subj: Security of Nuclear Reactors and Special Nuclear Material

(g) SECNAVINST 3300.2, Subj: Combatting Terrorism Program

(h) SECNAVINST 3300.3, Subj: Combatting Terrorism Program Standards

(i) OPNAVINST 3300.53, Subj: Navy Combatting Terrorism Program

(j) OPNAVINST 3300.54, Subj: Protection of Navy Personnel and Activities Against Acts of Terrorism and Political Turbulence

(k) SECNAVINST 5500.34, Subj: Security of DoD Personnel at U.S. Missions Abroad

(l) SECNAVINST 5500.29B, Subj: Use of Deadly Force and the Carrying of Firearms by Personnel of The Department of the Navy in Connection with Law Enforcement, Security Duties, and Personal Protection

(m) OPNAVINST 3591.1C, Subj: Small Arms Training and Qualification

(n) SECNAVINST 5500.4G, Subj: Reporting of Missing, Lost, Stolen, or Recovered (MLSR) Government Property

(o) NAVMEDCOMINST 6710.9, Subj: Guidelines for Controlled Substances Inventory (NOTAL)

(p) Naval Criminal Investigative Service/COMNAVFACENGCOM Guard Services Contract Performance Work Statement (NOTAL)

(q) SECNAVINST 5530.4B, Subj: Naval Security Forces Ashore and Afloat

(r) NAVSEAINST 8370.2, Subj: Small Arms and Weapons Management Policy and Guidance Manual (NOTAL)

(s) SECNAVINST 5511.36A, Subj: Authority of Military Commanders Under the Internal Security Act of 1950 to Issue Security Orders and Regulations for the Protection or Security of Property or Places Under Their Command

(t) SECNAVINST 5520.3B, Subj: Criminal and Security Investigations and Related Activities Within The Department of the Navy

(u) FEDERAL SPECIFICATION RR-F-191K/GEN, 14 May 1990, Subj: Fencing, Wire and Post Metal (And Gates, Chain-Link Fence Fabric, And Accessories) (General Specification) (NOTAL)

(v) FEDERAL SPECIFICATION SHEET RR-F-191K/1D, 14 May 1990, Subj: Fencing, Wire and Post Metal (Chain-Link Fence Fabric) (Detail Specification) (NOTAL)

(w) FEDERAL SPECIFICATION SHEET RR-F-191K/2D, 14 May 1990, Subj: Fencing, Wire and Post Metal (Chain-Link Fence Gates) (Detail Specification) (NOTAL)

(x) FEDERAL SPECIFICATION SHEET RR-F-191K/3D, 14 May 1990, Subj: Fencing, Wire and Post Metal (Chain-Link Fence Posts, Top Rails, and Braces) (Detail Specification) (NOTAL)

(y) FEDERAL SPECIFICATION SHEET RR-F-191K/4D, 14 May 1990, Subj: Fencing, Wire and Post Metal (Chain-Link Accessories) Detail Specification) (NOTAL)

(z) User's Guide On Protection Against Terrorist Vehicle Bombs, UG-2031-SHR, May 1998, Naval Facilities Engineering Services Center, Port Hueneme, CA (NOTAL)

(aa) NAVFAC MIL-HDBK-1013/14, Subj: Military Handbook - Selection and Application of Vehicle Barriers (NOTAL)

(ab) NAVFAC MIL-HDBK-1013/1A, Subj: Military Handbook - Design Guidelines for Physical Security of Facilities (NOTAL)

(ac) DoD Security Equipment Working Group Specification 012, Prime Item Product Specification for Magnetic Stripe Credentials, 18 Feb 94 (NOTAL)

(ad) OPNAVINST 1020.4D, Subj: Standards for Wearing the Camouflage Utility Uniform by Naval Personnel

(ae) OPNAVINST 5585.2B, Subj: Department of the Navy Military Working Dog (MWD) Program

APPENDIX II

DEFINITIONS

1. For the purpose of this instruction, 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 to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

c. Antiterrorism/Force Protection Plan. Specific measures taken to establish and maintain an antiterrorism/force protection program.

d. Antiterrorism/Force Protection Program. Seeks to reduce the likelihood that Navy-affiliated personnel, their families, facilities, and materiel will be subject to a terrorism attack, and to mitigate the effects of such attacks should they occur.

e. Armed Guard. A person equipped with a firearm and ammunition whose primary function is to protect property and who has qualified with the firearm in an approved weapons qualification course.

f. Auxiliary Security Force (ASF). An armed force composed of local, non-deploying military assets derived from host and tenant commands under the operational control of the host command's security department. The ASF is used to augment the installation's permanent security force during increased threat conditions or when directed by the host command.

g. Critical Communications Facility. A communications facility that is essential to the continuity of operations of the National Command Authority during national emergencies, and other nodal points or elements designated as crucial to mission accomplishment.

h. Commanding Officer. The term "commanding officer" as used throughout this manual includes commanders, directors, officers in charge, etc.

i. Electronic Security Systems. That part of physical security concerned with the safeguarding of personnel and property by use of electronic systems. These systems include,

but are no limited to, intrusion detection systems, automated entry control systems, and video assessment systems.

j. Exception. A written, approved long-term (36 months or longer) or permanent deviation from a specific provision of this instruction. Exceptions require compensatory or equivalent security measures.

k. Facility. A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land.

l. Force Protection. Security programs designed to protect Navy 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, personnel protective services, and supported by intelligence, counterintelligence, and other security programs.

m. Incident Response Plan. A set of procedures in place for dealing with the effects of an incident.

n. Installations. Real Department of Defense properties including bases, stations, forts, depots, arsenals, plants (both contractor and government-operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

o. 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 government property, including documents and computer media, and developing trend analyses to plan and implement reactive and proactive loss prevention measures.

p. Navy Activity. Any unit of the Navy shore establishment or operating forces under a commander, commanding officer, or an officer in charge.

q. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage and theft.

r. Physical Security Inspection. An examination of the physical security and loss prevention programs of an activity to determine compliance with physical security policy. A physical security inspection is normally conducted by a representative of an immediate superior in command. Follow-up action to correct noted deficiencies is required.

s. Physical Security Survey. A specific on-site internal examination/evaluation of physical security and loss prevention programs of an activity to determine the activity's vulnerabilities and compliance with physical security policies. They are used primarily as a management tool by the surveyed command and program manager.

t. Property. All assets including real property; facilities; funds and negotiable instruments; arms, ammunition and explosives; tools and equipment; material and supplies; communications equipment; computer hardware and software; and information in the form of documents and other media; whether the property be categorized as routine or special, unclassified or classified, non-sensitive or sensitive, conventional or nuclear, critical, valuable, or precious.

u. Restricted Area. An area to which entry is subject to special restrictions or control for security reasons, or to safeguard property or material. This does not include those designated areas restricting or prohibiting overflight by aircraft. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity properly posted, and shall employ physical security measures.

v. Security Force. That portion of a security organization at a Navy installation/activity comprised of active duty military, civilian police/guard, or contract guard personnel, tasked to provide physical security and/or law enforcement. The size and composition of the security force will depend on the size of the installation/activity, geographic location, criticality of assets, vulnerability and accessibility, as determined by the installation/activity commanding officer.

w. Survivability. The ability to withstand or repel attack, or other hostile action, to the extent that essential functions can continue or be resumed after onset of hostile action.

x. Systems Security Engineering (SSE). An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. SSE uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats.

y. Threat Assessment Plan. The process used to conduct a threat analysis and to develop a threat assessment.

z. Waiver. A written temporary relief, normally for a period of 1 year, from specific standards imposed by this instruction, pending actions or accomplishment of actions which will result in conformance with the standards. Interim compensatory security measures are required.

APPENDIX III

DUTIES OF SECURITY OFFICER

1. The security officer will (not all inclusive):

a. Determine adequacy of the command's physical security, antiterrorism, force protection and loss prevention programs; identify those areas in which improvements are required; and provide recommendations for such improvements to the commanding officer.

b. Where applicable, coordinate security requirements (including those related to force protection and antiterrorism) of tenant activities (or, as appropriate, command security requirements with the host activity) and ensure that those requirements are entered in applicable host-tenant agreements and inter/intra-service support agreements. Where feasible and appropriate, similar coordination and actions are to be done among all Navy activities on a regional basis.

c. Maintain contact with and solicit advice from the cognizant staff judge advocate concerning the legal aspects of physical security.

d. Determine, in coordination with the staff legal officer and facilities engineer, the type of jurisdiction of all areas, and maintain a map depicting precise jurisdictional boundaries when more than one type of jurisdiction is involved.

e. Establish and maintain liaison and working relationships and agreements with the local Naval Criminal Investigative Service Office.

f. Assess the threat to the installation/activity.

g. Conduct physical security surveys, vulnerability assessments, inspections and audits.

h. Establish and provide for maintenance of records relating to losses of government and personal property and violations and breaches of physical security measures and procedures.

i. Identify the personnel, real property, structures, and assets to be protected and recommend priorities.

j. Recognize constraints in resource application.

k. Identify and recommend the necessary resources to implement effective Physical Security, Antiterrorism, and Force Protection Programs.

l. Identify and recommend physical security, antiterrorism, force protection procedures, equipment, and security upgrades that will detect, delay, deter, and/or prevent wrongful removal, damage, destruction, or compromise of protected property and/or endanger personnel.

m. Recommend points of entry and exit and determine appropriate barriers.

n. Develop and maintain the personnel identification and access control system(s), as required.

o. Recommend establishment of restricted areas and ensure such areas are properly designated by the commanding officer.

p. Determine boundaries and establish perimeters of restricted areas.

q. Identify and recommend other physical security, antiterrorism, and force protection measures and procedures necessary to accomplish the command's mission.

r. Plan, manage, coordinate, implement, and direct the command's physical security, law enforcement, antiterrorism, force protection, and loss prevention programs, to include developing and maintaining local instructions. Where appropriate and feasible, this will be done in an integrated manner with other Navy activities on a regional basis.

s. Develop and maintain a current command Physical Security Plan in conjunction with the command's Terrorist Threat Assessment Plan and Terrorist Incident Response Plan.

t. Participate in planning of new construction and modifications to existing facilities to ensure that all physical security, antiterrorism, force protection, and loss prevention concerns are adequately addressed.

u. Organize and train the security force.

v. Validate the number of posts, fixed and mobile, and identify the manning required to sufficiently protect personnel and property, and react to and confront situations and circumstances which threaten those assets.

w. Prepare post orders, standard operating procedures, and a training plan for the security force and auxiliary security force. The plan should include policy guidance/procedures, jurisdiction, use of force, apprehension and temporary detention of intruders and violators, antiterrorism, force protection, and other appropriate topics.

x. Develop written security orders/directives to cover all phases of security and related antiterrorism and force protection operations.

y. Provide technical assistance on all security and related antiterrorism and force protection matters.

z. Ensure liaison concerning mutual security, antiterrorism, and force protection responsibilities is maintained with Federal and civil agencies, host country officials, or military activities.

aa. Develop security and antiterrorism plans including force protection aspects of crisis management. Participate in the planning (e.g., threat assessment planning and incident response planning), direction, coordination and implementation of procedures for crisis management of situations (including hostage situations) which pose a threat to the physical security of the command. Advise the commanding officer during any security-related crisis.

ab. Coordinate and monitor physical security waivers and exceptions.

ac. Develop, maintain, and administer an ongoing security education program encompassing security, crime prevention, loss prevention, antiterrorism, force protection, and local threat conditions.

ad. Develop and maintain a command Loss Prevention Program and supporting loss prevention plan which:

(1) Identifies and prioritizes, by attractive nature and likelihood of loss, assigned property susceptible to theft and pilferage.

(2) Identifies command property accountability, inventory, causative research and inspection procedures in effect. Makes recommendations to the commanding officer, as appropriate.

(3) Establishes procedures for adequate internal and external investigative measures, and for the review and trend analysis of losses.

(4) Establishes command functional areas and designates personnel to be active in and responsible for loss reporting, review, trend analysis, and investigative requests and liaison.

ae. Support the security manager in protecting classified material.

af. Provide terrorist threat awareness training and briefings to all personnel and family members as appropriate for local situations.

2. Although security officers are not part of the military intelligence community in a formal sense, their overall security and force protection responsibilities place them in positions through which quantities of information of potential interest or concern to the intelligence and law enforcement communities pass on a recurring basis. Therefore, in addition to having a key role in developing and executing the terrorism threat assessment plan, security officers shall:

a. Report all actual or suspected terrorist incidents or activities to their immediate commander, supporting security office, other supported activities, local intelligence field office, and local military criminal investigative office.

b. Conduct regular liaison visits with the supporting security office, intelligence field office, and local criminal investigation office.

APPENDIX IV

WAIVERS AND EXCEPTIONS

1. Requests for waivers or exceptions will be submitted as set forth below.

a. Waivers. Requests for waivers of specific requirements will be submitted via the chain of command to Echelon 2 commands. Echelon 2 commands are delegated authority to approve initial waivers for subordinate commands and their own headquarters. No further delegation is authorized. Waiver extension requests must be forwarded to CNO (N09N3). The request for waiver must include a complete description of the problem and compensatory measures/ alternative procedures, as appropriate. Approved waivers will normally be for a period of 12 months. Extension of the waiver (normally for 12 months) must be requested via the chain of command and approved by CNO (N09N3). Waiver extension requests shall refer to previous correspondence approving initial and previous extensions, as appropriate.

b. Exceptions. Requests for exceptions to specific requirements due to permanent or long term (36 months or longer) inability to meet a specific security requirement must be forwarded via the chain of command to CNO (N09N3) for consideration. Each exception request will include a description of the problem and compensatory measures and procedures to be employed. Exception requests will be reviewed and endorsed by each echelon in the chain. If an endorser does not recommend approval of the request, the endorser should return the request to the originator. The same applies to any requests for extension of previously approved long term exceptions. Correspondence that requests extension of previously approved long term exceptions, should include a reference to the initial CNO approving correspondence.

c. Waivers and exceptions to security criteria contained in references (a) through (f) fulfill the waiver and exception requirements of this instruction.

d. In other countries the host nation may have ultimate responsibility for certain aspects of security, such as perimeter security for Navy activities located there, and Navy authorities may not be able to implement certain requirements set forth in this instruction. In those instances, formal exceptions are not required. However, the parent Echelon 2 command must review the situation and determine what, if any, measures are appropriate to take to compensate for measures not allowed by the host nation.

e. Waiver and Exception Requests. The initiating command will assign a waiver or exception number per subparagraphs f and g below. All information requested below must be provided in waiver, waiver extension, and exception (permanent and long-term)

requests. Requests will be in letter format, and all elements of subparagraphs g, h, or i will be specifically addressed. Nonapplicable elements shall be noted as "N/A".

f. Waiver and Exception Identification. This paragraph provides guidance for the assignment of waiver or exception numbers. Any request for extension of a previously approved waiver or exception will use the same number assigned to the original waiver or exception approval. The basic objective is to provide a ready unique identification of any given waiver or exception with respect to the activity involved and the initial year of the request. Each waiver or exception must be identified as follows:

(1) The first six digits, beginning with the letter "N" for Navy represent the Unit Identification Code (UIC) of the activity initiating the request.

(2) The next digit is either "W" for waiver or "E" for exception.

(3) The next two digits represent the serial number of the request, beginning annually on 1 January with 01. Waiver and exception numbers will run sequentially together, e.g., W01-88 followed by E02-88, then E03-88, W04-88, etc.

Note: This is important so that activities in the reviewing chain of command can exercise their discretion to change an exception request to a waiver request, and vice versa, without having to re-coordinate the number with the requesting activity.

(4) Extensions. Original numbers assigned long term exceptions and waivers will be used when requesting exception or waiver extensions.

(5) The last two digits identify the calendar year of the request.

(6) Example:

N01234-W01-96
N = Navy activity
UIC= 01234 (Navy UIC)
W = Waiver ("E" for exception)
01 = 1st waiver (or exception) request of calendar year
96 = 1996 (year initial waiver/exception requested)

g. Waiver Format. The following format is prescribed for requests for waivers:

(1) Line 1 - Waiver number.

(2) Line 2 - Statement of waiver requirement and references to chapter, section, and paragraph in this manual which cite standards which cannot be met.

(3) Line 3 - Specific description of condition(s) which caused the need for the waiver and reason(s) why applicable standards in this manual cannot be met.

(4) Line 4 - Description of the physical location of affected facilities or areas. Identify structures individually by building number.

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

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

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

(8) Line 8 - Identify actions initiated or planned (local capability or other) to eliminate the waiver and estimated time to complete.

(9) Line 9 - Provide point of contact to include name, rank/grade, DSN and commercial phone numbers.

h. Long-Term Exception Format. The following format is prescribed for requests for long-term exceptions:

(1) Line 1 - Exception number.

(2) Line 2 - Statement of long-term exception requirement and references to chapter, section, and paragraph in this manual which cite standards which cannot be met.

(3) Line 3 - Specific description of condition(s) which caused the need for the long-term exception and reason(s) why applicable standards in this manual cannot be met.

(4) Line 4 - Description of the physical location of affected facilities or areas. Identify structures individually by building number.

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

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

(7) Line 7 - Identify resources, including estimated cost, to eliminate the long-term exception.

(8) Line 8 - Identify actions initiated or planned (local capability or other) to eliminate the long-term exception and estimated time to complete.

(9) Line 9 - Provide point of contact to include name, rank/grade, DSN and commercial phone numbers.

i. Permanent Exception Format. The following format is prescribed for requests for permanent exceptions:

(1) Line 1 - Exception number.

(2) Line 2 - Statement of the exception requirement and reference to the chapter, section, and paragraph in this instruction which cite the standard which cannot be met.

(3) Line 3 - Specific description of condition(s) which caused the need for the permanent exception and reason(s) why applicable standards in this manual cannot be met.

(4) Line 4 - Description of physical location of affected facilities or areas. Identify structures individually by building number.

(5) Line 5 - Identify, in detail, compensatory security measures which are being applied.

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

(7) Line 7 - Provide point of contact to include name, rank/grade, DSN and commercial phone numbers.

APPENDIX V

AUXILIARY SECURITY FORCE (ASF) MINIMUM TRAINING REQUIREMENTS

1. The following is a list of subjects that is established as minimum training requirements for the Navy ASF. Subject areas that should be taught by the Marine Corps Cadre or Marine Mobile Training Teams are identified as well as those subjects that should be taught by existing security department personnel or locally available assets such as NAVCRIMINVSERV, medical, JAG, explosive ordnance disposal, etc.

MARINE CORPS CADRE/MOBILE TRAINING TEAMS

SUBJECT

Weapons
- Safety
- Basic Level of Proficiency/Qualification
- Pistol/Revolver
- Shotgun

Use of Force
- DON Policy
- Rules of Engagement

Physical Training

Unarmed Self Defense (Defensive Tactics)

Security Watch Standing (Interior Guard)
- General Orders
- Special Orders
- Challenging Procedures/Response

Search Techniques
- Personnel
- Vehicle
- Building
- Area

Communications
- Equipment
- Procedures

Antiterrorism Awareness
- Personal Protection
- Surveillance Detection
- Threat Types

Individual Tactics
- Cover
- Concealment
- Movement

LOCAL SECURITY DEPARTMENTS

Security Department
- Organization (Duties and Functions)
- Jurisdiction and Authority

Search and Seizure

Uniform Code of Military Justice

Apprehension and Restraint

Crowd Control

Basic First Aid

Community Relations

Crime Prevention

Protection of Crime Scene

Disaster & Emergency Plans

APPENDIX VI

RESTRICTED AREAS AND LIMITED WATERWAY AREAS

1. Restricted Areas

a. There are several valid reasons to establish restricted areas (e.g., mission sensitivity; protection of certain unclassified chemicals, precious metals or precious metal-bearing articles; conventional arms, ammunition and explosives; funds; drugs; nuclear material; sensitive or critical assets; or articles having high likelihood of theft) to protect security interests.

b. As a matter of policy, three different levels of restricted areas are established. The intent is to simplify and standardize the appropriate application of varying degrees or levels of restrictions, controls, and protective measures that are appropriate for different circumstances and/or assets as discussed in the preceding paragraph.

(1) Level One. The least secure type of restricted area. Its appropriate application is to situations judged to warrant establishment of a restricted area, but less than a Level Three or Level Two restricted area.

(2) Level Two. The second most secure type of restricted area. The most appropriate application is to situations where uncontrolled entry into the area, or unescorted movement within the area could permit access to what is being protected.

(3) Level Three. The most secure type of restricted area. The most appropriate application is to situations where access into the restricted area constitutes, or is considered to constitute, actual access to what is being protected.

(4) The general rule is that decisions regarding designations of restricted areas, their levels, and criteria for access to each restricted area are at the discretion of the commanding officer (see discussion of review and assessment processes in chapter 1). These decisions usually flow from the reasons that led to the conclusions to establishment of the restricted area in the first place. Exceptions to the general rule are:

(a) Direction provided for protection of specific assets (e.g., references (a) through (f)).

(b) Direction provided by the parent chain of command.

(c) Direction provided elsewhere in this manual concerning specific circumstances.

c. Minimum Security Measures Appropriate for Restricted Areas, i.e., Level 1.

(1) A clearly defined protected perimeter. This 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.

(2) Admission only to persons whose duties require access and who have been granted appropriate authorization. Persons not cleared for access to the security interest contained within a restricted area may, with appropriate approval, be admitted, but they must be escorted so that the security interest itself is still protected from unauthorized access.

(3) A personnel identification and control system.

(4) Entry and departure controlled.

(a) An electronic control system with the capability of recording entry and departure may be used to accomplish this.

(b) It is intended to permit use of electronic access control systems and CCTV to economize the number of personnel that are necessary to control access to restricted areas. Use of electronic measures can allow appropriately cleared and trained personnel to control access as intended, but in a manner that does not necessitate their physical presence at each and every control point.

(c) If a computer access control or logging system is used, it must be safeguarded against tampering.

(5) Secured during non-working hours.

(6) Checks are often made for signs of attempted or successful unauthorized entry, and for other activity which could degrade the security of the restricted area.

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

(1) The same measures specified for Level One, and,

(2) During normal duty hours, use of an access list and entry and departure log is suggested but not required. After normal duty hours, all personnel must be logged in and out. (An electronic control system with the capability of recording entry and departure may be used to accomplish this).

(3) When secured, checked at least twice per 8-hour shift or at least once per 8-hour shift if adequately equipped with an operational IDS. This is intended as a benchmark guide and not as a hard and fast rule.

e. The following minimum security measures are appropriate for Level Three restricted areas:

(1) The same measures specified for Levels One and Two, except as follows:

(a) Personnel identification and control system includes an access list and entry and departure log. After normal duty hours, all personnel will be logged in and out. Only visitors need be logged in and out during normal duty hours.

Note: This is based on the premise that other records (e.g., time and attendance, travel, etc.) will be available to call upon to establish whether regularly assigned/employed personnel were present in the restricted area on any given work day during normal duty hours. However, these other records would not normally establish whether a person would have been in a restricted area after normal duty hours.

f. Personnel and Vehicle Administrative Inspections.

(1) All instructions designating restricted areas shall include procedures for conducting inspections on a random basis of persons and vehicles entering and leaving such areas. The purpose is to detect and deter the introduction of prohibited items (firearms, explosives, drugs, etc.) and to detect and deter the unauthorized removal of government property and material. To be effective, administrative vehicle and personnel inspections must be conducted frequently enough so that personnel remain mindful that the inspections are a real possibility, and that they could be inspected at any time they enter or leave the area. It is better to frequently conduct random inspections of a few people or vehicles at any one time than to inspect a lot of people only infrequently. Procedures will be coordinated with the cognizant Staff Judge Advocate or Naval Legal Service Office and approved by the activity commanding officer or designated representative. Accredited Naval Criminal Investigative Service personnel, upon presentation of badge and/or credential, are exempt from such inspections aboard Navy installations.

(2) Security force personnel must be instructed that incoming persons and vehicles may not be inspected over the objection of the individual. However, those who refuse to permit inspection will not be allowed to enter. Persons who enter should be advised in advance (a properly worded sign to this effect prominently displayed in front of the entry point will suffice) that they and their vehicles are liable to inspection while in the restricted area.

2. Limited Waterway Areas. Commanding officers of installations/activities adjacent to waterways who decide to limit persons, vehicles, vessels, and objects within designated areas have several options.

a. Described here are the different types of limited waterway areas available. The U.S. Coast Guard (USCG) and the 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.

(1) Installation/activity commanding officers shall ensure their waterfront and waterway areas are designated by the proper authority.

(a) The USCG and USACE are the authority for implementing control mechanisms under the Ports and Waterway Act of 1972 (PWSA) (33 U.S.C. 1221 et seq), the Magnuson Act of 1950 (50 U.S.C. 191), the Outer Continental Shelf Lands Act (OCSLA) (43 U.S.C. 1331 et seq), and the Deepwater Port Act (33 U.S.C. 1501 et seq).

(b) The cognizant USACE local field office is the responsible agency for establishing restricted areas.

(c) The Coast Guard Captain of the Port is responsible for establishing all other types of Limited Waterway Areas.

(2) Installation/activity commanding officers shall make their case for protection of adjacent waterway areas with the proper agency. 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 all requests and subsequent correspondence/designation will be provided CNO (N09N3).

(3) 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.

(4) Although public notification of designated Limited Waterway Areas is the responsibility of the local USACE or USCG, as appropriate, installation/activity commanding officers shall ensure that the language of the associated notices convey the commanding officer's intent (e.g., that such notices explicitly ban swimmers or persons as well as boats if that is what is intended).

(5) Commanding officers shall ensure that areas designated are appropriately patrolled or observed to ensure protection of ships and operations.

APPENDIX VII

SIGNS AND POSTING OF BOUNDARIES

1. General

a. Signs will be posted as prescribed below unless alternate means are used to more effectively and efficiently provide the same information to the same intended audience.

b. Signs will read essentially as stated below (deviations will be approved by local supporting legal officer).

c. Size, placement, and use of any language in addition to English should be appropriate for the stated purpose.

2. Restricted Areas

a. Restricted areas will be posted at regularly used points of entry with signs that read essentially as follows:

WARNING
RESTRICTED AREA - KEEP OUT
AUTHORIZED PERSONNEL ONLY

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

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

b. The intent is that any reasonable person would conclude that everyone entering a restricted area through a regularly used entry point would have been informed of the above information.

c. Perimeter boundaries of restricted areas that are composed of barriers such as fences or walls not closed off by a roof or ceiling will be posted at intervals with signs that read essentially as follows:

WARNING
RESTRICTED AREA
KEEP OUT

Authorized
Personnel Only

(1) The intent is that any reasonable person would conclude that everyone crossing the boundary fence, etc., into the restricted area would have been informed of the above information.

(2) These signs do not have to be posted along restricted areas boundaries where the walls form an enclosed box with true floor and true ceiling.

d. Restricted signs will not indicate whether the area is a Level One, Two, or Three restricted area.

3. Navy Installations

a. All regularly used points of entry at Navy installations and separate activities will be posted at regularly used points of entry with signs that read essentially as follows:

WARNING
U. S. NAVY 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

b. The intent is that any reasonable person would conclude that everyone entering a Navy installation or separate activity through a regularly used entry point would have been informed of the above information.

c. The issue of whether to post perimeter boundaries of Navy installations and separate activities will be governed by trespass laws applicable to the jurisdiction in which the installation/activity is located.

APPENDIX VIII

PHYSICAL SECURITY/LAW ENFORCEMENT
PHASE I (BASIC) MINIMUM TRAINING STANDARDS
NAVY SECURITY FORCE

1. Subject Elements

a. Administrative

#(1) Overview/Orientation
#(2) Security Department Duties and Functions
#(3) Standards of Conduct
#(4) Forms and Reports/Report Writing
#(5) Area Familiarization/On-Job-Training

b. Physical Security

#(1) Vehicle and Personnel Movement Control
(2) Loss Prevention/MLSR Program
#(3) Threat Levels
#(4) Physical Security Safeguards

c. Legal Subjects

#(1) Jurisdiction and Authority
#(2) Rules of Evidence
#(3) Search and Seizure
(4) Uniform Code of Military Justice
(5) Self-Incrimination/Admissions and Confessions
#(6) Apprehension and Arrest

d. Traffic Laws and Enforcement

*(1) Traffic Control
*(2) Accident Investigation
*(3) Driving Under The Influence

e. Patrol

*(1) Military Working Dog
#(2) Crime Scenes/Preservation of Evidence
#(3) Crime Prevention
#(4) Crimes in Progress
(5) Juvenile Matters
#(6) Communications
#(7) Drugs of Abuse Identification, Prevention and Control
*(8) Patrol Procedures
(9) Vehicle Stops/Search of Vehicles

f. Unusual Incidents

#(1) Crowd Control

#(2) Terrorism
#(3) Bomb Threats, Wrongful Destruction and Sabotage

g. Professional Skills

(1) Weapons Proficiency Training
(2) Use of Force
(3) Defense Tactics

Legend:
Mandatory Training Requirements for Contract Guards.
* Required for all security force personnel whose duties require those skills.

APPENDIX IX

ANNUAL PHASE II (IN-SERVICE) TRAINING PROGRAM

1. The completion of Phase II training is mandatory for all security personnel on an annual basis. The required training is available via the Phase II Exportable Training Package and includes the material necessary for annual training (except firearms). This exportable package is available to installation security departments by contacting NAVCRIMINVSERV.

2. Listed subject matter in addition to weapons training is required for all security force personnel annually.

3. Commands must determine the length of time to be devoted to individual subject elements. This determination should be based on subject matter as it applies to overall command needs (see discussion in chapter 1 of continuing review and assessment process). Commands will ensure that adequate time is devoted to provide security force personnel sufficient knowledge of each subject.

4. Subject areas highlighted by the pound symbol are mandatory Phase II training for contract guard personnel. Commanding officers of user activities may require training in additional subject areas as appropriate to satisfy contract guard mission and duties as outlined in guard contracts.

LAW ENFORCEMENT/PHYSICAL SECURITY ANNUAL PHASE II (IN-SERVICE) TRAINING

Subjects

Jurisdiction#

Law and the Uniform Code of Military Justice

Use of Force#

Crime Scenes

Search and Seizure#

Interview and Interrogation Techniques

Reports and Forms#

Crisis Intervention

Juvenile Offenses

Crime Prevention Program

Selective Enforcement#

Public Relations/Citizens Interaction#

Information Security

Restricted Areas

Perimeter Security

Arms, Ammunition, and Explosives Storage Site Security

Disaster and Emergency Plans#

Local Instructions and Procedures#

Legend:
Mandatory Training Requirements for Contract Guards.