No exemptions identified.

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

OPNAVINST 5530.14E CH-1
N4
19 Apr 2010

OPNAV INSTRUCTION 5530.14E CHANGE TRANSMITTAL 1

From: Chief of Naval Operations

Subj: NAVY PHYSICAL SECURITY AND LAW ENFORCEMENT PROGRAM

Encl: (1) Revised page 3-5; new pages 3-5a, 3-5b, and 3-5c; and revised page 3-6

1. Purpose. To provide policy regarding the possession of personal weapons on board Navy installations, specifically to include on-base Bachelor Quarters, on-base temporary lodging facilities, and on-base Navy housing areas (to include on-base Public-Private Venture (PPV) housing).

2. Action. Remove pages 3-5 and 3-6 of enclosure (1) of the basic instruction and replace with enclosure (1) of this change transmittal.

M. K. LOOSE
Vice Admiral, CEC, U.S. Navy
Deputy Chief of Naval Operations
(Fleet Readiness and Logistics)

Distribution:
Electronic only via Department of the Navy Issuances Web site
http://doni.daps.dla.mil

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO

OPNAVINST 5530.14E
N4
28 Jan 09

OPNAV INSTRUCTION 5530.14E

From: Chief of Naval Operations

Subj: NAVY PHYSICAL SECURITY AND LAW ENFORCEMENT PROGRAM

Ref: See Appendix C to Enclosure (1)

Encl: (1) Navy Physical Security and Law Enforcement Program Requirements

1. Purpose. The intent of this instruction is to identify responsibilities and provide guidance for the protection of people and assets throughout the Navy as directed in references (a) through (e). This instruction is a complete revision and must be reviewed in its entirety.

2. Cancellation. OPNAVINST 5530.14D and OPNAVINST 5530.15A.

3. Background

a. Three core lines of effort are necessary for protection: critical infrastructure protection, continuity of operations and Force Protection (FP). Antiterrorism (AT), Law Enforcement (LE) and Physical Security (PS) are pillars which complement, integrate with, and support the core lines of effort. While the prioritization of implementing the pillars must be based on each commander's risk management process, in general, the AT mission shall be treated as the effort of first importance as it ensures the availability of Navy assets for war-fighting missions.

b. Reference (a) provides over-arching Navy policy, guidance, information, procedures and responsibilities for the AT line of effort. Enclosure (1) to this instruction provides security and LE policy for safeguarding personnel, property, and material and enforcing rules and regulations at Navy installations, activities, and afloat/operational commands. Security measures that will deter, detect, delay, and defend against terrorist attack are addressed.

c. The policy framework in this instruction dictates man, train, and equip models and sets the operational posture for the Navy's program.

d. As the Navy's program adjusts and transforms over the near term, commanders must make every effort to rapidly conform to these new guidelines and eliminate duplicative efforts, wasteful or convenience behaviors that do not directly contribute to our security posture or align with directed priorities.

e. For the purpose of brevity in this instruction only, the short title for the Navy PS and LE Program will be "Navy Security Program."

4. Applicability

a. This instruction applies to all Navy military personnel, civilian employees, contractors, facilities, ships, aircraft, and non-Navy organizations physically located on or aligned to U.S. Navy-controlled installations worldwide.

b. Where this instruction conflicts with the Geographic Combatant Commander (GCC) PS or LE requirements, the GCC's requirements take precedence. Deviation from the policy and standards in this instruction must be documented in the appropriate planning and implementing guidance (e.g., protection plans, command guidance, etc.). Specific waiver/exceptions are not required, however the cognizant Navy Component Commander (NCC) will notify Deputy Chief of Naval Operations for Fleet Readiness and Logistics (CNO (N4)), in writing, of any deviation from Office of the Chief of Naval Operations (OPNAV) policy necessary to meet GCC requirements.

5. Exceptions. Navy Nuclear Security (e.g., weapons, Naval Nuclear Propulsion Program, and special nuclear material), Department of Defense high risk billet programs, personnel security program (security clearances, etc.), information systems and network security, industrial security or chemical agent security requirements and policy are addressed by the following instructions:

a. Reference (f) provides specific policy, planning guidance and requirements for Navy Security Force (NSF)

personnel, Harbor Security Boats (HSBs), and security-related equipment for waterfront restricted areas and nuclear weapons limited areas. The Strategic Weapons Facility (SWF) Commanding Officers (COs) have operational and tactical control of these security forces and patrol boats. Reference (g) provides guidance for the safeguarding of nuclear reactors and special nuclear material.

b. References (h) and (i) provide specific policy and guidelines for the Department of the Navy Information Systems and Security Programs.

c. Reference (j) establishes standards and guidance for personnel access to classified information and assignment to sensitive duties consistent with the interests of national security.

d. Reference (k) provides standards and responsibilities for safeguarding chemical agents.

6. Policy

a. The primary objective of the Navy Security Program is to safeguard personnel, property, facilities and materiel and to enforce laws, rules, and regulations at Navy installations, activities, and operational commands. Capability requirements and resourcing levels will be established using the approved Required Operational Capability (ROC) tiered methodology contained in reference (l). Figure 1-1 identifies the baseline security requirements for shore installations based on ROC levels.

FIGURE 1-1
ROC Baseline Functions

| ROC Baseline Functions* |
|---|
| ROC 1: Access control, mobile patrols, Intruder Detection System (IDS), Military Working Dog (MWD) teams, armed response teams, and all requirements mandated in NSPS-28, Nuclear Weapons Security Manual (S5210.41M), and SECNAVINST S8126.1, as applicable. |
| ROC 2: Access control, external Entry Control Points (ECPs), water barriers, HSBs, MWD teams, mobile patrols with back-up capability, ability to respond to simultaneous events, and internal ECPs. |

| |
|---|
| ROC 3: Access control, external ECPs, mobile patrols with back-up capability, and ability to respond to a single event. (Patrol/response may be provided by nearby installation as directed by the region commander.) |
| ROC 4: Access control (may be automated) and mobile patrol (may be provided by nearby installation/local LE as directed by the region commander.). |
| ALL: LE response capability with the ability to respond within 15 minutes. (This capability may be provided by a nearby installation or local LE as directed by the region commander.) Emergent, life-threatening calls require an immediate response, with due regard for safety and traffic conditions. |
| **Note: Specific security requirements will be based on type of assets assigned/supported* |

b. Operational commanders, region commanders, fleet commanders, Installation Commanding Officers (ICOs), and organizational COs shall implement this tiered approach to security capabilities and resources in reference (l) and this instruction.

c. ICOs shall establish and maintain a Navy Security Program that implements higher headquarters guidance and plans. Command and installation protection plans shall include all aspects of the protection framework, including PS, AT, and LE elements, as a part of an integrated family of capabilities.

d. COs shall use approved Navy Tactics, Techniques and Procedures (NTTPs) and Navy Tactical Reference Publications (NTRPs) (i.e., references (m), (n), and (o)) to carry out requirements set forth in this instruction. Any variance from the guidance and procedures outlined in appropriate NTTPs and NTRPs will be documented in local plans and instructions signed by the CO.

7. Roles and Responsibilities

a. Deputy Chief of Naval Operations for Operations, Plans and Strategy (CNO (N3/N5)) provides overarching AT policy and strategic oversight of the Navy Security Program and will annually assess the effectiveness of current policies and standards.

(1) As assessment sponsor, CNO (N3/N5) shall evaluate policy and proposed resources as well as provide an evaluation when the policy meets the overall AT requirements as set forth in references (a) and (b).

(2) Branch Head, Antiterrorism (OPNAV (N314)) under the Director, Operations and Plans (OPNAV (N31)) is the focal point for FP and security assessment matters as they relate to Navy afloat protection.

b. CNO (N4) has the primary responsibility for the formulation and dissemination of Navy Security Program policies and standards ashore.

(1) Branch Head, Protection (OPNAV (N46P)) under the Ashore Readiness Division (OPNAV (N46)) is the focal point for FP and security policy and program management as they relate to Navy ashore protection.

(2) OPNAV (N46) shall formulate policy on matters related to ashore AT, PS, LE.

(3) OPNAV (N46) shall ensure mission essential task standards, performance assessment tools, and FP drills and exercises are aligned with the metrics and capabilities required in enclosure (1) and contained in references (a) and (c).

(4) CNO (N4) serves as the Navy's resource sponsor for Navy security programs ashore.

c. Deputy Chief of Naval Operations for Integration of Capabilities and Resources (CNO (N8)) serves as the Navy's resource sponsor for Navy security programs afloat.

d. Director, Naval Criminal Investigative Service (NCIS), assists OPNAV (N46) with coordination and oversight for LE programs and shall provide assessment advice and assistance to ICOs to enable them to develop and maintain effective LE programs. Additionally, NCIS is responsible for managing and funding the Navy's Federal Bureau of Investigation National Academy quotas.

e. The Navy Inspector General ensures reviews are conducted as part of the Navy command inspection programs to determine compliance with the policies contained in this instruction.

f. Commander, U.S. Fleet Forces Command (USFF), is the Chief of Naval Operations' (CNO's) executive agent for FP, with tactical control over all NSF in the U.S. Northern Command Area of Responsibility (AOR). In this role, USFF shall:

(1) Establish and implement PS and LE standards and policies in the Continental United States (CONUS).

(2) Generate Navy-wide PS and LE requirements in addition to and in conjunction with AT requirements (reference (a)).

(3) Articulate authoritative fleet AT warfighting, readiness, and personnel capability requirements coordinated with other NCCs to the CNO.

(4) Provide a fleet kennel master to coordinate, identify and task MWD teams to directly support the United States Secret Service within the CONUS and global force management missions worldwide in accordance with references (p) through (s).

g. NCCs shall establish operational requirements in addition to the policies identified in enclosure (1) of this instruction for PS, LE, and AT for all Navy activities and facilities within their AOR.

h. Commander, Navy Expeditionary Combat Command, shall:

(1) Serve as the Master-at-Arms (MA)/Security Force subject matter expert concerning MA employment in support of combatant commander, NCC and Service requirements.

(2) Develop and coordinate MA training policy and execution.

(3) Serve as the MWD program manager.

i. Commander, Navy Education and Training Command, shall:

(1) Review Navy Security Program course curricula to ensure commonality and implement revised training as required by OPNAV or GCC changes in policy and operational requirements.

(2) Provide oversight and management of the Center for Security Forces to support the following:

(a) Develop and deliver Navy Security Program learning solutions in support of program requirements based on OPNAV policy and validated GCC and USFF/type commander individual training requirements. Ensure learning content is consistent with applicable AT, PS and LE doctrine and policy.

(b) Partner with Navy Security Program stakeholders to define individual human performance requirements and tasks to facilitate the delivery of the appropriate tools and opportunities to meet FP training requirements.

(c) Coordinate the requirement to establish and manage distance learning sites as required to meet OPNAV and GCC requirements.

j. The Commander, Naval Facilities Engineering Command, shall:

(1) Serve as the Navy's Physical Security Equipment (PSE) program manager and execution agent to perform the following:

(a) Participate in and/or lead program reviews as required.

(b) Function as the ashore PSE program technical authority and procurement contracting office.

(c) Responsible for budgeting and maintaining all PSE used for LE and PS on Navy ashore installations and facilities as directed by OPNAV (N46)/Commander, Navy Installations Command (CNIC).

(2) Coordinate with OPNAV, NCC, Budget Submitting Offices (BSOs), and end users to identify all projects for each program element every fiscal year.

(3) Implement and manage the technology insertion testing, procurement, installation, and evaluation processes when identified as applicable to the Navy Security Program.

(4) Establish and manage the Navy Security Program equipment and system project research, design, development, testing, evaluation, procurement, installation, and life-cycle support budget.

k. Region commanders shall:

(1) Report to their respective NCC for operational matters relating to the Navy Security Program.

(2) Report to CNIC for administrative matters relating to the Navy Security Program and resourcing.

(3) Establish and manage a regional security program, including the development of plans (AT, emergency management, etc.). Plans will be reviewed and updated as required, but at a minimum annually.

(4) Evaluate the execution and effectiveness of the installation Navy security program and AT plans within their region to ensure compliance with this instruction and higher headquarters directives.

(5) Re-deploy installation NSF personnel within the region as needed to assist with a crisis event.

l. The ICO shall:

(1) Report to the assigned region commander for all operational matters relating to FP.

(2) Perform and coordinate all Navy Security Program requirements within the installation's AOR. Tenant activities are not authorized to establish a separate armed security and/or LE force without approval from CNO (N4) via the ICO, region commander, and NCC.

(3) Establish an installation Navy security program, including the development of a comprehensive protection plan that incorporates AT, PS, and LE. Each plan will be reviewed and updated as required, but at a minimum annually.

(4) Coordinate with their region commander to ensure sufficient funding to meet Navy Security Program support costs including maintenance availability.

(5) Ensure post orders are prepared and published.

m. Afloat/squadron COs shall:

(1) Report to the numbered fleet commander in the AOR in which they are operating for all PS and LE matters.

(2) Establish an afloat Navy security program, including the development of a comprehensive protection plan that incorporates AT, PS and LE. Each plan will be reviewed and updated as required, but at a minimum annually.

n. Tenant COs/officers in charge shall:

(1) Implement installation PS and LE policies and procedures as directed.

(2) Report to the ICO for all operational matters related to the Navy Security Program.

(3) Participate as an active member of the ICO's Navy Security Program.

(4) Coordinate all Navy Security Program issues with the ICO of the installation where they reside as well as their BSO.

o. In the case of a CO of any Navy activity not physically located on a Navy installation and not a tenant of an ICO, report to the region commander for operational matters related to Navy Security Program.

8. Action

a. NCCs/numbered fleet commanders and all echelon 2 operational commanders shall ensure subordinate activities comply with the requirements set forth in this instruction.

b. Echelon 2 commanders shall determine the manning, training, equipment, and material resourcing levels needed for activities under their cognizance to meet the requirements of this instruction and to document and prioritize all unfunded shortfalls. Where requirements cannot be funded, these Commanders will provide justification and proposed mitigations to their resource sponsor for approval.

c. OPNAV AT working groups and summits shall be leveraged by echelon 2 commanders to discuss initiatives and issue resolution related to PS and LE.

9. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed in accordance with reference (t).

10. Reports and Forms

a. Reporting requirements contained in this instruction are exempt from reports control by reference (u).

b. The following forms can be obtained via the Naval Forms Online Web site at https://navalforms.daps.dla.mil/web/public/home. Locally generated forms will not be used in lieu of official forms.

(1) OPNAV 5580/26 DON Command Investigator ID Card Stock Number (S/N) 0107-LF-984-6000

(2) OPNAV 5580/21 Field Interview Card S/N 0107-LF-984-0000

(3) OPNAV 5580/12 Department of the Navy Vehicle Report

(4) OPNAV 5527/17A DON Evidence Tag S/N 0107-LF-983-4000. Note: Once stocked quantity of OPNAV 5527/17A is depleted, the form number will change and be restocked as OPNAV 5580/17A.

(5) OPNAV 5580/17B DON Evidence Tag (Sticker) S/N 0107-LF-983-5200

(6) OPNAV 5580/22 Evidence Property Custody Receipt S/N 0107-LF-984-1200

M. R. MOOSE
Vice Admiral, CEC, U.S. Navy
Deputy Chief of Naval Operations
(Fleet Readiness and Logistics)

Distribution:
Electronic only, via Department of the Navy Issuances Web site
http://doni.daps.dla.mil

# NAVY

# PHYSICAL SECURITY AND LAW ENFORCEMENT REQUIREMENTS

# TABLE OF CONTENTS

PAGE

**CHAPTER 1 INTRODUCTION AND NAVY SECURITY GUIDANCE**

0100 GENERAL ..... 1-1
0101 PHYSICAL SECURITY AND LAW ENFORCEMENT PROGRAM ..... 1-1
0102 COMMANDER/COMMANDING OFFICER AUTHORITY ..... 1-1
0103 IMPLEMENTATION OUTSIDE THE CONTINENTAL UNITED STATES . 1-2

**CHAPTER 2 PHYSICAL SECURITY**

0200 GENERAL ..... 2-1
0201 PHYSICAL SECURITY SURVEYS ..... 2-1
0202 SECURITY CHECKS ..... 2-1
0203 SECURITY INSPECTIONS ..... 2-2
0204 VULNERABILITY ASSESSMENTS ..... 2-3
0205 THREAT ASSESSMENTS ..... 2-4
0206 RISK MANAGEMENT ..... 2-4
0207 PHYSICAL SECURITY OF ACTIVITIES NOT LOCATED ABOARD NAVY INSTALLATIONS ..... 2-4
0208 SECURITY EDUCATION PROGRAM ..... 2-5
0209 KEY SECURITY AND LOCK CONTROL ..... 2-5
0210 EXTERNAL ENTRY CONTROL AND RESTRICTED AREA ACCESS CONTROL ..... 2-6
0211 BARRIERS AND OPENINGS ..... 2-16
0212 PROTECTIVE LIGHTING ..... 2-16
0213 UNIFIED FACILITIES CRITERIA SECURITY REQUIREMENTS ... 2-17
0214 FLIGHTLINE AND AIRCRAFT SECURITY ..... 2-18
0215 WATERSIDE AND WATERFRONT SECURITY ..... 2-19
0216 HARBOR SECURITY BOATS ..... 2-21
0217 SECURITY OF MATERIAL ..... 2-22
0218 SECURITY OF COMMUNICATIONS SYSTEMS ..... 2-23
0219 PROTECTION OF BULK PETROLEUM PRODUCTS ..... 2-24
0220 WAIVERS AND EXCEPTIONS ..... 2-25

**CHAPTER 3 LAW ENFORCEMENT**

0300 GENERAL ..... 3-1
0301 CRIME PREVENTION ..... 3-1
0302 DISSEMINATION OF INFORMATION ..... 3-2
0303 POLICE RECORDS ..... 3-2
0304 SUPPORT TO CIVILIAN LAW ENFORCEMENT AGENCIES ..... 3-3
0305 APPREHENSION AND DETAINMENT ..... 3-4
0306 CONTROL AND ACCOUNTABILITY OF PERSONAL WEAPONS ..... 3-5
0307 INVESTIGATIONS ..... 3-6
0308 EVIDENCE HANDLING ..... 3-9
0309 LOST AND FOUND ..... 3-10

PAGE

0310 JUVENILES ..... 3-10
0311 DOMESTIC VIOLENCE ..... 3-11

**CHAPTER 4 PHYSICAL SECURITY AND LAW ENFORCEMENT PLANNING**
0400 GENERAL ..... 4-1
0401 REQUIREMENTS ..... 4-1

**CHAPTER 5 NAVY SECURITY FORCE**
0500 GENERAL ..... 5-1
0501 NAVY SECURITY FORCE PERSONNEL ..... 5-2
0502 STANDARDS OF CONDUCT ..... 5-6
0503 NCIS SECURITY TRAINING, ASSISTANCE, AND ASSESSMENT TEAMS ..... 5-6

**CHAPTER 6 SECURITY AND LAW ENFORCEMENT TRAINING**
0600 GENERAL ..... 6-1
0601 NSF APPRENTICE TRAINING REQUIREMENTS ..... 6-1
0602 ANNUAL SUSTAINMENT TRAINING REQUIREMENTS ..... 6-1
0603 NON-LETHAL WEAPONS (NLW) TRAINING ..... 6-3
0604 NSF SPECIAL DUTIES AND QUALIFICATIONS ..... 6-6

**CHAPTER 7 LEGAL ASPECTS**
0700 GENERAL ..... 7-1
0701 JURISDICTIONAL REQUIREMENTS ..... 7-1

**CHAPTER 8 USE OF FORCE AND WEAPONS POLICIES**
0800 GENERAL ..... 8-1
0801 ARMING REQUIREMENTS ..... 8-1
0802 NON-LETHAL WEAPONS ..... 8-2

**CHAPTER 9 EMERGENCY VEHICLES**
0900 GENERAL ..... 9-1
0901 EMERGENCY VEHICLE USE ..... 9-1

**CHAPTER 10 SECURITY FORCE COMMUNICATIONS SYSTEMS**
1000 GENERAL ..... 10-1
1001 REQUIREMENTS ..... 10-1
1002 COMMUNICATIONS EQUIPMENT ..... 10-2

**CHAPTER 11 INCIDENT REPORTING AND THE NAVY SECURITY NETWORK**
1100 GENERAL ..... 11-1
1101 REPORTING REQUIREMENTS ..... 11-1

**APPENDIX A POST VALIDATION MODEL AND STAFFING** ..... A-1
**APPENDIX B DEFINITIONS/ACRONYMS** ..... B-1
**APPENDIX C REFERENCES** ..... C-1

# CHAPTER 1

## INTRODUCTION AND NAVY SECURITY GUIDANCE

### 0100. GENERAL

a. The primary objective of the Navy Security Program is to safeguard personnel, property, facilities and materiel and to enforce laws, rules, and regulations at Navy installations, activities, and operational commands.

b. Throughout this instruction references will be made to the Navy Security Force (NSF) for both Physical Security (PS) and Law Enforcement (LE). While the use of contract personnel to perform inherently governmental LE functions is prohibited by statute, it is important to understand that the NSF is composed of a mix of active and reserve military personnel, government civilians, and contractor professionals as outlined in chapter 5 of this instruction.

### 0101. PHYSICAL SECURITY AND LAW ENFORCEMENT PROGRAM

a. PS and LE programs for an installation or ship are the responsibility of the host Installation Commanding Officer (ICO) or ship's Commanding Officer (CO), as applicable. The COs of tenant activities shall retain only those internal security functions intrinsic to their organizations and missions, which include PS of facilities, personnel security, information security, industrial security, and information assurance.

b. The Navy Security Program encompasses both LE and PS programs and includes all measures taken by a command, activity, ship, or installation to protect itself against all acts designed to, or which may, impair its effectiveness and/or readiness.

c. Navy installation security departments shall be responsible for providing PS and LE services to tenant commands. With the exception of Strategic Weapons Facilities (SWFs), tenant commands shall not establish a Security Department of their own.

### 0102. COMMANDER/COMMANDING OFFICER AUTHORITY

a. As outlined in references (a) and (d), COs of installations, ships and activities are responsible for issuing

necessary instructions for the protection and security of personnel, property or places under their command.

b. ICOs must conspicuously post and enforce the orders and regulations they issue. The statutory authority resides in section 797 of title 50, United States Code (U.S.C.) (section 21 of the "Internal Security Act of 1950"). This statute makes it a crime for an individual to violate certain regulations or orders promulgated or approved by a military commander designated by the Secretary of Defense. Those regulations or orders must enhance the protection or security of a military facility, property or places subject to Department of Defense (DoD) jurisdiction, or a military conveyance (including ingress or egress to such places).

**0103. IMPLEMENTATION OUTSIDE THE CONTINENTAL UNITED STATES.** Navy organizations located outside the continental United States that are unable to implement certain requirements of this or supporting instructions based on security requirements in host nation or Status of Forces Agreements (SOFAs) are required to address and request waivers and/or exceptions from this policy in their Antiterrorism (AT) plans. These commands shall also consider the need for mutual aid agreements and the use of bilingual security personnel to the fullest extent possible. In cases where the host nation prohibits the ICO from implementing requirements of this instruction, the region commander shall report to the Deputy Chief of Naval Operations for Fleet Readiness and Logistics (CNO (N4)) via their operational chain of command.

# CHAPTER 2

## PHYSICAL SECURITY

**0200. GENERAL.** PS is concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to installations, equipment, materiel, and documents; and to safeguard against espionage, sabotage, damage, and theft. PS involves the total spectrum of procedures, facilities, equipment, and personnel employed to provide a secure environment. The essence of PS on Navy installations at locations where military personnel reside and during in-transit operations involves the integration of policy, doctrine, personnel, materiel, training, intelligence, and planning.

**0201. PHYSICAL SECURITY SURVEYS**

a. ICOs shall ensure that PS surveys of their activities are conducted annually and the results addressed as a part of a command review and assessment program. Survey results are a local management tool and not normally disseminated up the chain of command. Surveys will serve to update the command on what needs protecting, what security measures are in effect, what needs improvement, and what the security priorities are.

b. Surveys must be conducted on all normally inhabited facilities as well as the following:

(1) Arms, Ammunition, and Explosives (AA&E) storage facilities in accordance with reference (b).

(2) Exchange and commissary facilities.

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

(4) Activities possessing restricted areas and facilities and mission-critical areas designated in writing by the ICO.

(5) The office, headquarters, or residence (if applicable) of the installation command staff and any local or regional senior leadership that regularly works or resides on the installation.

**0202. SECURITY CHECKS.** Installations shall establish a system for the daily after-hours checks of installation restricted

areas, facilities, containers, perimeter, building ingress and egress points to detect any deficiencies or violations of security standards. Tenants shall also establish a system for the daily after-hours checks of their restricted areas, facilities, containers, and barrier or building ingress and egress points to detect any deficiencies or violations of security standards. In accordance with reference (t), records of security violations detected by NSF personnel, including those identified during random spot checks of tenants, shall be maintained for a period of 3 years. The activity security officer must follow up each deficiency or violation and keep a record for a period of 3 years of all actions taken (structural, security, disciplinary, administrative, etc.) by the responsible department to resolve the present deficiency or violation and to prevent recurrence.

## 0203. SECURITY INSPECTIONS

a. Security inspections are required for all critical areas as described by reference (b). This includes AA&E storage facilities (and ready-for-issue storage areas), and other locations aboard Navy installations, ships, activities, and facilities as may be directed by the CO. Some units/facilities may be exempt from inspection due to their mission. These units/facilities will be inspected under the guidance of regulations and directives unique to those activities.

b. The CO shall ensure that required security inspections provide a recorded assessment of the PS procedures and measures implemented by the unit or activity being inspected to protect its assets. Security inspections will be reviewed, approved, and maintained on file by the CO and shall be made available for review by the Navy region commander, echelon 2/Navy Component Commanders (NCCs), and the Naval Inspector General (IG) upon request.

c. Security inspections on non-AA&E areas shall be conducted at least once every 2 years.

d. Security inspectors shall be granted access to Navy units, activities, records, and information on a "need-to-know" basis, consistent with the inspector's clearance for access to classified defense information and provisions of applicable DoD and Navy policy.

e. COs of the organizations inspected shall provide a report of corrective actions taken to their appropriate chain of command.

f. Findings noted on security inspection reports that represent vulnerabilities that cannot be corrected through the region commander due to lack of resources shall be recorded in the Core Vulnerability Assessment Management Program (CVAMP) and forwarded to the Budget Submitting Office (BSO) with recommendations and requests for resource assistance. Refer to section 0220 of this chapter for submission of waiver and exception requests.

g. If a vulnerability assessment is conducted (see section 0204 of this chapter) that meets the criteria described herein for a designated facility, the requirement for the security inspection is satisfied. Documentation to this effect will be identified within security inspection records.

## 0204. VULNERABILITY ASSESSMENTS

a. Region commanders shall ensure that vulnerability assessments of housing areas, facilities, and/or activities at installations meeting the requirements of reference (a) are conducted every 3 years. This requirement may be met by either a Chief of Naval Operations Integrated Vulnerability Assessment (CNOIVA) or a Joint Staff Integrated Vulnerability Assessment (JSIVA). CNOIVAs are conducted by the Naval Criminal Investigative Service (NCIS) Security Training Assistance and Assessment Team (STAAT) with a representative of the appropriate Navy echelon 2 command. JSIVAs are conducted by the Defense Threat Reduction Agency.

b. Region commanders shall ensure ICOs conduct an annual vulnerability assessment of all installations, facilities, and operating areas within their area of responsibility. These local assessments must include all activities and elements residing as tenants on installations or geographically separated but under the command of the local ICO for AT. The requirement for local assessments is satisfied if a higher headquarters vulnerability assessment is conducted at that location during the same calendar year.

c. All vulnerabilities identified through an integrated vulnerability assessment or self-assessments must be entered into the installation CVAMP account for consideration for

possible funding to eliminate/mitigate the noted vulnerability in accordance with reference (a).

**0205. THREAT ASSESSMENTS.** All NCIS components shall maintain close and effective liaison with local, state, and federal LE and intelligence agencies. NCIS shall disseminate, by the most effective means, threat information potentially affecting the security of a particular military installation, ship, and/or designated facility on or off base. If a command receives, detects, or perceives threat information, the servicing NCIS component shall be promptly notified. Comprehensive threat assessments shall be requested from NCIS when impending operations, official travel, or other circumstances require the development or update of a Force Protection (FP) plan (reference (a)). NCIS shall also provide, upon request, an installation-specific threat assessment through the servicing NCIS office. These threat assessments are available on the NCIS Web site.

**0206. RISK MANAGEMENT.** Commanders and COs shall establish a risk management process, as required by reference (d), using references (k), (m), and (v), to identify, assess, and control risks arising from criminal or terrorist activities and to assist in planning and conducting FP. The risk management process shall be embedded into unit organization, operations, systems, culture, and individual behaviors. Risk management efforts shall be identified in all AT plans.

**0207. PHYSICAL SECURITY OF ACTIVITIES NOT LOCATED ABOARD NAVY INSTALLATIONS.** At all Navy activities not located aboard a Navy installation, the CO shall establish a Navy security program and appoint a security officer in writing.

a. Activities located aboard other DoD service/agency sites shall coordinate PS requirements with the host. Navy organizations should establish Inter-Service Support Agreements (ISSAs)/Memoranda of Understanding (MOUs)/Memoranda of Agreement (MOAs) with the host service or nation via the chain of command. Topics that shall be addressed in these agreements include establishment and identification of property boundaries, intrusion detection system monitoring, available response forces, use of force (including deadly force) training and issues, PS support, etc. ICOs shall coordinate all such agreements through higher headquarters, including Staff Judge Advocate (SJA)/Office of Counsel/legal offices.

b. Security around Navy vessels located in private shipyards shall be negotiated in contracts using the standards

set forth in the latest revision of reference (w). AT plans for private shipyards shall be coordinated with Naval Sea Systems Command.

## 0208. SECURITY EDUCATION PROGRAM

a. Commanders and COs shall develop and implement a security education program for the purpose of keeping all personnel vigilant and concerned on a myriad of security matters. Security education programs will include, but are not limited to:

(1) General security safety and awareness.

(2) Theft prevention.

(3) Installation-specific security procedures.

b. All personnel shall receive initial security training to ensure that they understand the need for security, to help them be proficient in the security procedures applicable to the performance of their duties, and to help them understand the possible consequences of security lapses or breakdowns.

c. Refresher training shall be given to the extent necessary to ensure personnel remain mindful of and proficient in meeting their security responsibilities or as required by the guiding instructions.

## 0209. KEY SECURITY AND LOCK CONTROL

a. Key and Lock Control Program

(1) Commanders and COs shall designate a key control officer and 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 instruction. This requirement does not include keys, locks and padlocks used for convenience, privacy, administrative or personal use.

(2) Security requirements for sensitive locks and keys are covered in reference (n).

b. AA&E. Reference (b) governs control and security of keys and locks used to provide security of AA&E.

c. Frequency of Inventories. Inventories shall be conducted semiannually at a minimum.

d. Padlocks and Lock Cores. Where padlocks and removable lock cores are used, a program must be instituted to rotate these locks and cores annually. 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.

e. Lock Procurement. The activity security officer shall be involved in the lock procurement process so that only locks that are adequate for their intended application are procured.

f. Lockouts. All lockouts involving locks used to meet security objectives of this instruction shall be promptly examined by competent personnel to determine the cause of the lockout, and the security officer shall be notified of the determination. Lockouts will be reported as a security deficiency and recorded as such.

## 0210. EXTERNAL ENTRY CONTROL AND RESTRICTED AREA ACCESS CONTROL

a. General

(1) Region commanders and ICOs shall develop a system of personnel and vehicle movement control in accordance with the sensitivity, classification, value, and operational importance of the area and the requirements of this instruction. Reference (x) pertains.

(2) ICOs shall publish a process for removal of, or denying access to, persons who are not authorized or represent a criminal threat.

b. Installations and Restricted Area Access Control

(1) At Force Protection Conditions (FPCONs) Normal, Alpha, and Bravo:

(a) In addition to the Armed Sentry(ies) (AS), unarmed personnel may be assigned as identification checkers to maintain smooth traffic flow at all installation perimeter vehicle Entry Control Points (ECPs).

(b) The installation CO, ship and squadron CO, regional and numbered fleet commanders (or their designated representatives) will coordinate any additional security

augmentation requirements to be filled by ships and squadrons in accordance with the established supported/supporting relationship. For special events (i.e., scheduled ship tours, general public visiting, ship/squadron homecomings, etc.), regional and numbered fleet commanders (or their designated representatives) will coordinate all mutually agreed upon security augmentation requirements to be filled by ship/squadron personnel.

(2) DoD decals continue to be the minimum acceptable standard for basic vehicle access control or for permanent access to installation perimeters. All Navy-controlled entry points shall enforce this requirement (reference (y)). In cases where an installation shares a common, unguarded perimeter with another Service's installation, the ICO must coordinate with the other Service to minimize confusion over the Navy decal requirement. Reasonable measures must be employed to ensure all motor vehicle operators are aware that decals are needed on any Navy installation.

c. Automated Entry Control Systems (AECS). AECS-controlled ECP guidance is contained in reference (z).

d. Water Boundaries

(1) Water boundaries shall be protected by barriers and marked with appropriate signage. In addition to barriers, patrol craft shall be used at activities whose waterfronts contain critical assets as per section 0215 of this chapter. In inclement weather, such patrols may not be able to provide an adequate degree of protection and shall be supplemented by increased waterfront patrols, watchtowers, Military Working Dog (MWD) teams, and other appropriate waterside security systems.

(2) Limited waterway areas shall be protected as outlined in section 0215 of this chapter and references (n) and (aa).

e. Gate Runners. ICOs shall ensure that policy dealing with gate runners includes the following:

(1) Minimum force necessary shall be used to prevent unauthorized access to Navy activities.

(2) Whenever possible and consistent with actions in self-defense per reference (bb), use physical barriers (both fixed and rapidly deployable) rather than physical force (in

particular deadly force) to prevent unauthorized access to Navy installations (reference (aa)). Rapidly deployable barriers are not considered deadly force.

(3) Unless operating under Rules of Engagement (ROE) or standing rules for the use of force (reference (bb)) that state otherwise, no sentry shall engage a driver or vehicle with weapons fire unless the sentry determines that conditions of extreme necessity exist and they are justified in using deadly force in accordance with reference (aa).

f. Security Badges and the DoD Common Access Card (CAC)

(1) The DoD CAC shall be the principal card enabling access to buildings, facilities, installations, ships, and controlled spaces. COs shall direct acceptance of the CAC for access where existing access control systems use a picture badge and/or a badge with a magnetic stripe or other integral CAC technology.

(2) Upon full implementation of the CAC as the standard access control token, COs shall eliminate all locally used badges and associated equipment. Supplemental badging systems may continue to be used for the following:

(a) An additional level of access control security not presently afforded by the CAC (e.g., such as entrance into a Sensitive Compartmented Information Facility (SCIF) or other high-security space).

(b) AECSs incorporating technology that is not yet supported by the CAC (e.g., at ECPs using contactless chips that allow both short- and long-range read capabilities).

(c) Ancillary badges used for circulation control may also continue to be used; however, they shall not replicate or employ technology currently on the CAC.

(3) When purchasing upgrades to existing access control systems, the upgraded system must meet Federal Information Processing Standard 201 (including International Organization for Standardization 14443 contactless technology and ability to perform automated personal identity verification), include an emergency power source, and have the ability to provide rapid electronic authentication to Federal and DoD authoritative databases, including DoD personnel registered in the Defense Enrollment and Eligibility Reporting System per reference (e).

g. Restricted Areas

(1) Restricted areas shall be established in writing by the CO within his or her jurisdiction in accordance with reference (n) and section 797 of title 50, U.S.C. Designated restricted areas shall be a part of installation plans or local instructions for PS.

(2) Tenant COs shall publish and inform the ICO and region commander, in writing, of all areas under their control that are designated as restricted areas. Particular attention will be paid to those areas that are vital to national security.

(3) ICOs shall publish a consolidated list of all restricted areas and mission essential/vulnerable areas not designated as restricted areas aboard the installation, including tenant command restricted areas. This list shall be contained in the installation AT plan, shall be reviewed annually, and shall specify which areas are vital to national security. This list should be limited to official use only.

(4) COs shall establish restricted areas around assets and facilities to protect mission-critical or sensitive assets or programs, security interests, classified material, nuclear material, conventional AA&E, biological select agents and toxins, drugs, precious metals or precious metal-bearing articles, articles or funds having high likelihood of theft, and certain unclassified chemicals.

(5) When the decision is made to designate an area as restricted, the CO shall further identify entry requirements, including:

(a) Personnel authorized access.

(b) Visitor control.

(c) Identification systems.

(d) Access control procedures.

(e) Security clearance requirements (including any requirement for maintenance and custodial personnel).

(6) In designating restricted areas, COs shall identify the level of restricted area to be established as described

herein. All restricted areas shall be posted simply as restricted areas so as not to single out or draw attention to the importance or criticality of an area.

(a) Level One

1. The least secure type of restricted area. It shall be established to provide an increased level of security over that afforded elsewhere aboard the activity to protect a security interest that, if lost, stolen, compromised, or sabotaged, would cause damage to the command mission or impact upon the tactical capability of the United States. It may also serve as a buffer zone for Level Three and Level Two restricted areas, thus providing administrative control, safety, and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement within it may or may not permit access to a security interest or asset.

2. At a minimum, Level One restricted areas shall be established around category III and IV AA&E storage facilities; defense infrastructure; petroleum, oil, and lubricants, power, and water supply and storage areas; pier facilities for amphibious, auxiliary, and Military Sealift Command (MSC) ships; Strategic Sealift Ships (SSS); prepositioned ships, mine warfare and coastal patrol ships; controlled drugs and precious metals; funds and negotiable instrument storage areas; NSF facilities; emergency dispatch centers; electronic security system monitoring spaces and MWD facilities; motor pools; and research, development, test, and evaluation centers; or other sites whose loss, theft, destruction, or misuse could compromise the defense infrastructure of the United States.

(b) Level Two

1. A Level Two restricted area may be inside a Level One area but shall not be inside a Level Three area. It shall be established to provide the degree of security necessary to protect against uncontrolled entry into, or unescorted movement within, an area that could permit access to a security interest that, if lost, stolen, compromised, or sabotaged, would cause damage to the command mission or harm the operational capability of the United States. Uncontrolled or unescorted movement could permit access to the security interest.

2. At a minimum, Level Two restricted areas shall be established around alert systems, forces, and

facilities; pier facilities for carriers, submarines, and large-deck amphibious ships (priority B); aircraft hangars, ramps, parking aprons, flight lines, runways, and aircraft rework areas; all risk category arms and category I and II AA&E storage facilities and processing areas (including ammunition supply points); essential command and control, communications, and computer facilities, systems, and antenna sites; critical assets power stations, transformers, master valve, and switch spaces; and assets whose loss, theft, destruction, or misuse could impact the operational or tactical capability of the United States.

(c) Level Three

1. The most secure type of restricted area, it may be within less secure types of restricted areas and shall be established to provide a degree of security where access into the restricted area constitutes, or is considered to constitute, actual access to a security interest that, if lost, stolen, compromised or sabotaged, would cause grave harm to the command mission or strategic capability of the United States. Access to the Level Three restricted area shall constitute actual access to the security interest or asset.

2. At a minimum, Level Three restricted areas shall be established around nuclear, biological, chemical and special/nuclear weapons research, testing, storage, and maintenance facilities; critical command and control, communications, and computer facilities, systems, and antenna sites; critical intelligence-gathering facilities and systems; nuclear reactors and category I and II special nuclear materials; permanent or temporary pier facilities for fleet Ballistic Missile Submarines (SSBNs) armed with nuclear weapons; and assets whose loss, theft, destruction, or misuse would result in grave harm to the strategic capability of the United States. Facilities identified by the Geographic Combatant Commander (GCC) as having strategic significance will be designated and protected as a Level Three restricted area.

(7) Decisions regarding designations of restricted areas, their levels, and criteria for access to each restricted area are at the discretion of the CO, except in cases:

(a) Where higher headquarters guidance has been provided for the protection of specific assets (e.g., classified material, sensitive compartmented information, automated data

processing systems, nuclear weapons, conventional AA&E, and nuclear reactors and special nuclear material).

(b) Where direction has been provided by the chain of command or in the Department of Defense, SECNAV, or Office of the Chief of Naval Operations (OPNAV) publications.

(8) ICOs shall ensure that the minimum security measures are employed for restricted areas to include a clearly defined protected perimeter, controlled access limited to those with appropriate clearance and "need-to-know," establishment of a personnel identification system, maintenance of access list and visit log documentation, performance of checks for unauthorized entry every 8 hours during normal working hours or every 4 hours after normal working hours, and designation of a response force.

(9) Each Navy activity shall establish a system to check restricted areas, facilities, containers, perimeter, or building entry and departure points by occupants/users in an attempt to detect any deficiencies or violations of security standards.

h. Limited Waterway Areas

(1) ICOs adjacent to waterways who decide to limit persons, vehicles, vessels, and objects within designated areas shall ensure the proper authority designates their waterfront and waterway areas as restricted areas. See table 2-1 of this chapter.

(a) 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, as provided in table 2-1 of this chapter.

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

2. The cognizant USACE local field office is the responsible agency for establishing restricted areas.

3. The USCG Captain of the Port (COTP) is responsible for establishing all other types of limited waterway areas.

(b) ICOs shall make their case for protection of adjacent waterway areas with the proper agency via the region commander. ICOs desiring adjacent waterway or waterfront access controls must provide a written request to the appropriate local office of USCG or USACE. Requests must 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 shall be provided to the Branch Head, Antiterrorism (OPNAV (N314)).

(2) ICOs shall make every effort to coordinate protection of adjacent waterway areas with the proper agency. ICOs shall review operations and AT plans to ensure areas of responsibility/jurisdiction are properly identified. The Installation Security Officer (ISO) shall make certain that a liaison is maintained between security personnel and local USCG officials to ensure designation of limited waterway areas and procedural aspects are kept current.

(3) Although public notification of designated limited waterway areas is the responsibility of the local USACE or USCG, as appropriate, the ICO shall ensure that the language of the associated notices conveys the commander's intent (e.g., that such notices explicitly ban swimmers or persons as well as boats if that is what is intended).

(4) ICOs shall ensure that areas designated are appropriately patrolled or observed to ensure protection of ships and operations.

(5) Such areas as described in this section, at a minimum, will be designated as a Level One restricted areas.

**TABLE 2-1**
**LIMITED WATERWAY ACCESS**

| Area | Restricted Area (Note 1) | Naval Vessel Protection Zone (NVPZ) | Security Zone (Note 1) | Restricted Waterfront Area (Note 1) |
|---|---|---|---|---|
| **Enforcement** | Enforcement may be delegated to the command. *No threat needed. Easy to obtain. Provides limited area jurisdiction for command. | USCG and Navy *An NVPZ exists around U.S. naval vessels greater than 100 feet in length overall at all times in the navigable waters of the United States, whether the large U.S. naval vessel is underway, anchored, moored, or within a floating dry dock, except when the large naval vessel is moored or anchored within a restricted area or within a naval defensive sea area. | USCG only. Navy may patrol under COTP (Note 2) authority. *Threat required. COTP controls access and movement of all vessels vehicles and persons (including their removal), and may take possession and control of any vessel. (see subpart 165.33 of title 33, Code of Federal Regulations (CFR)) | USCG only. COTP directed by COMDT (Note 3) *Threat required. Long-term limited access area. Any change must be directed by the COMDT. |
| **Penalties** | Misdemeanor | Violations of the NVPZ are a felony offense, punishable by up to 6 years in prison and/or up to $250,000 in fines. | Felony 10 years/$10,000 fine | Felony 10 years/$10,000 fine |
| **Limitations** | Only on inland waterways | Around U.S. naval vessels greater than 100 feet in length overall in the navigable waters of the United States. | Only within territorial limits of United States. No person or vessel may enter zone without permission from COTP. Can be placed overland. | Must be issued and directed by COMDT. COTP may be directed to enforce. Must be in regulations. Limits access of persons. |
| **Authority** | Part 207 of title 33, CFR | Sections 91 and 633 of title 14, U.S.C.; part 45 of title 49, CFR. Final Rule published in the Federal Register (FR) on May 13, 2002 (Page 31958 of Volume 67, FR) Atlantic, and June 4, 2002 (Page 38391 of Volume 67, FR) Pacific | MAGNUSON ACT (section 191 of title 50, U.S.C.) subpart 6.10-5 of title 33, CFR, part 165 of title 33, CFR | Magnuson Act (section 191 of title 50, U.S.C.) subpart 165.40 of title 33, CFR |
| **Agency** | USACE (Note 4) | USCG | USCG/COTP | USCG/COMDT |

**NOTES/ACRONYMS:**
1. Does not include airspace.
2. COTP - U.S. Coast Guard Captain of the Port
3. COMDT - Commandant of the Coast Guard
4. USACE - U.S. Army Corps of Engineers

i. Signs and Posting of Boundaries

(1) ICOs shall ensure that signs are posted as a part of establishing legal boundaries of the installation.

(2) 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.

j. Inspection of Vehicles

(1) Administrative Inspection of Vehicles

(a) All vehicles on Navy activities are subject to administrative inspection in accordance with procedures authorized by the ICO. ICOs shall issue instructions directing security personnel to administratively inspect vehicles entering and leaving the installation and restricted areas.

(b) No person or group, except as provided in subparagraph j(1)(c) below, may be exempted from, or singled out for, such inspections, and the instruction by COs regarding such inspections shall be coordinated in advance of implementation with local SJA or Regional Legal Service Office (RLSO) officials to ensure strict adherence to either mandatory inspection of all vehicles or a structured random inspection pattern that is impartial and unbiased.

(c) Federal agents (i.e., Federal Bureau of Investigation, U.S. Secret Service, NCIS, Central Intelligence Agency, Defense Intelligence Agency, Army Criminal Investigation Division, and Air Force Office of Special Investigations) when conducting official business, upon presentation of their special agent credentials when entering or leaving Navy activities, are exempt from administrative inspections. This exemption includes vehicles used by them in the course of official business and all occupants therein per reference (cc).

(d) Security force personnel must be instructed that persons and vehicles attempting to enter an activity 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 shall 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 subject to inspection while aboard the activity or within the restricted area.

(e) Actions carried out during an administrative vehicle inspection include the verification of occupant identity and in the case of commercial vehicles, the verification of delivery documents (e.g., bill of lading). These tasks may be satisfied by official access lists and other accepted documents.

(2) Intermediate Inspection of Vehicles. Just as in the case of administrative inspections, intermediate inspections must verify driver identity, cargo, and destination. Additionally, intermediate inspections are done with the purpose of observing the entire vehicle exterior portions in plain sight. This level of inspection is used as a part of AT spot checks.

(3) Complex Inspection of Vehicles. In addition to the requirements of the administrative and intermediate inspections, complex inspections are done for the purpose of observing all exterior and interior vehicle spaces normally accessible without the use of special tools or destruction of the vehicle infrastructure.

k. Special Precautions. Personnel responsible for the accomplishment or implementation of personnel and vehicle control procedures shall be watchful for the unauthorized introduction to or removal from the installation government property, especially weapons and AA&E materials. This responsibility includes all personnel and means of transportation, including government, private, and commercial vehicles, aircraft, railcars, and ships.

**0211. BARRIERS AND OPENINGS**

a. Sufficient barriers shall be in place to control, deny, impede, delay, and discourage access by unauthorized persons.

b. Inspections shall be carried out at least weekly to ensure they continue to function as needed. Mechanical barriers shall be operationally tested on a daily basis.

**0212. PROTECTIVE LIGHTING.** COs shall ensure that lighting is provided to discourage or detect attempts to enter Navy installations, ships and other restricted areas and to reveal

the presence of unauthorized persons within such areas. Considerations for protective lighting are found in reference (n).

## 0213. UNIFIED FACILITIES CRITERIA SECURITY REQUIREMENTS

a. New Construction and Facility Modifications. All new construction shall comply with the requirements of this manual and approved Unified Facilities Criteria (UFC) publications. This requirement also applies to pertinent facility modifications to existing buildings, facilities, sites, etc. The ICO or designated representative shall review plans for new construction and facility modifications. The operational echelon 2 commander shall address issues that 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). All UFC waivers must be submitted during the facility project approval process, and the project packages must now contain an operational and physical risk mitigations assessment with detailed rationale for the exemption, including a technical review by Naval Facilities Engineering Command (NAVFAC), a current local threat assessment memorandum, and the ability to employ mitigation measures other than UFC requirements.

b. Navy Military Construction Projects. Commander, Naval Facilities Engineering Command (NAVFACENGCOM), is responsible for reviewing PS construction projects. This responsibility includes ensuring the requirements of this instruction are fully met or, if not, submitting an exception for the deviation. In fulfilling this responsibility, NAVFACENGCOM shall ensure that all protective design measures, equipment reliability, and maintenance have been considered.

c. Security Of Leased Facilities. PS standards that cannot be met, either temporarily or permanently, must be identified. Waiver or exception requests must be submitted as appropriate. Compensatory security measures implemented or planned must be identified in all such waiver or exception requests.

d. Activity Upgrade Requirements

(1) All new construction or significant upgrades or modifications to existing facilities must be in accordance with applicable UFCs. Any construction that poses a potential vulnerability (as identified during security surveys, inspections, or vulnerability assessments) must be addressed to

conform to standards contained in this instruction. A Plan of Action and Milestones (POA&M) shall be developed to correct deficiencies.

(2) Deficiencies that can be corrected within 12 months require the submission of a waiver pending completion of the required upgrade effort. Deficiencies that cannot be corrected in 12 months or are deemed permanent require the submission of an exception. Compensatory security measures are required in either case.

## 0214. FLIGHTLINE AND AIRCRAFT SECURITY

a. Flightlines will be protected in accordance with reference (n).

b. ECPs shall be equipped with gates, gatehouses, areas for processing personnel and vehicles into the flightline restricted area, communications equipment (two-way radio and telephone), and security lighting.

c. Off-Base Aircraft Mishaps

(1) Initial security for military 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. Reference (dd) pertains.

(2) The senior security supervisor on scene shall be responsible for coordinating with civilian LE.

e. Security of Navy Aircraft at Non-Navy Controlled Airfields

(1) Trained security personnel, composed of U.S. military security units, Navy Expeditionary Combat Command, host-nation security forces, private security personnel, or a combination of the above, must provide FP as appropriate for expeditionary air forces ashore. Such forces must be assigned to meet standards approved by the GCC for the airfield in question. Deployment orders should specifically identify the security forces performing this function.

(2) All aircraft require an Armed Response Team (ART), which may consist of an area patrol that is not dedicated to the

visiting aircraft. Close Boundary Sentries (CBS) are required per table 2-2 below and consist of NSF dedicated to keeping the restricted boundary under surveillance.

**TABLE 2-2**
**SECURITY REQUIREMENTS BY AIRCRAFT TYPE**

| Aircraft type | Entry control responsibility | ART | CBS | Motorized patrol |
|---|---|---|---|---|
| Tactical Aircraft (AV-8, F/A-18) | Aircrew | Yes | | Yes |
| Airlift Aircraft (C-5, C-9, C-17, C-130) | Aircrew | Yes | | Yes |
| Strategic Bomber Aircraft (B-52, B-1, B-2) | Aircrew | Yes | | Yes |
| Air Refueling Aircraft KC-10, KC-135) | Aircrew | Yes | | Yes |
| Special Mission Aircraft (E-2, EA-6, EP-3) | Security | Yes | Yes | |
| Reconnaissance Aircraft (P-3, P-8A) | Aircrew | Yes | | Yes |
| Advanced Technology Aircraft | Pilot carries detailed information for divert contingencies | | | |
| Other DoD Aircraft | Aircrew | Yes | Yes | Yes |

(3) When planning exercises or operations that involve Navy aircraft use of airfields without adequate U.S. military security forces, appropriate augmentation must be provided. Maritime expeditionary security squadrons are requested through the appropriate numbered fleet commander for such duties. Thoughtful consideration of the combination of local conditions and FPCON is required to determine specific augmentation requirements.

(4) Commander, Naval Air Forces, shall promulgate guidance for naval aircraft transiting in the United States (the Continental United States (CONUS), Alaska, and Hawaii).

## 0215. WATERSIDE AND WATERFRONT SECURITY

a. In Navy-controlled ports, the installation protection plans (see section 0400 of this instruction), the AT plan in particular, shall detail the port security posture. In CONUS, private shipyards, Naval Sea Systems Command, and applicable supervisor of shipbuilding shall ensure that contractors fulfill security requirements. Doctrinal information pertaining to waterside PS measures can be found in references (aa) and (ee).

b. Region commanders must ensure waterways adjacent to afloat assets in Navy-controlled ports are under appropriate

surveillance and adequately patrolled. ICOs are ultimately responsible for asset protection. In waterfront areas also covered by a COTP, overall port security is the responsibility of USCG.

c. Table 2-3 below provides a description of the security required to protect categorized Navy assets. Threat and vulnerability assessments must also be taken into consideration when visiting a port. Each level incorporates the measures from all the previous levels. The use of water barriers for priority C assets should be considered on case-by-case basis after evaluating the threat, vulnerability, asset, and whether co-located with A or B assets.

(1) While at anchorage inside installation restricted areas, all ships shall be provided protection.

(2) Piers where ships are moored will be protected by a pier ECP sentry controlling access at the foot of the pier or by a single ECP established separately from the brow when a unit is moored. No sentry is required for pedestrian-only ECPs controlled by an AECS when the entire perimeter of the restricted area is adequately secured unless there is an additional requirement to process visitors. One additional person shall augment the gate during periods of heavy traffic to support visitor control and maintain traffic flow. These duties shall be performed in accordance with reference (n).

(3) At fleet concentration areas and other installations with multiple piers with individual access control points, piers shall be enclaved to the maximum extent possible.

(4) Prior to a ship's arrival in a non-U.S. Navy controlled port, the ship's CO will develop an Inport Security Plan (ISP) using the most recent Port Integrated Vulnerability Assessments (PIVAs) and threat assessments. The ISP must be approved by the NCC/numbered fleet commander prior to entering port.

(5) Foreign naval ships visiting U.S. Navy installations shall be provided protection commensurate with similar, collocated United States Navy (USN) vessels.

**TABLE 2-3**
**SECURITY OF WATERFRONT ASSETS MATRIX IN U.S. NAVY CONTROLLED PORTS**

| Priority | Asset | Security measures (cumulative from low to high) |
|---|---|---|
| A (Highest) | SSBN | Per SECNAVINST S8126.1 and at non-home ports where cumulative asset in port time exceeds more than 120 days in a calendar year, use water barriers to stop small boat threat. |
| B (High) | Carriers, other submarines, and large-deck amphibious | – Electronic water/waterside security system (closed-circuit television, associated alarms, surface craft or swimmer detection, underwater detection).<br>– Use water barrier(s) to prevent direct unchallenged access from small boat attacks.<br>– Submarines and aircraft carriers shall receive an armed escort during ingress and egress. |
| C (Medium) | Surface combatants, other amphibious, auxiliary, MSC SSS, ammunition ships, mine warfare | – Establish security zone with the USCG, where possible.<br>– Use water barrier(s) where appropriate and/or practical, harbor patrol boat(s) with bullhorn, night vision device, spotlight, marine flares, and lethal and non-lethal weapons.<br>– Arrange patrol boat backup support from harbor operations, USCG, or other (tenant boat units, small craft from ships). |
| D (Low) | Patrol coastal, MSC SSS (reduced operational status), pier facilities | – Adjacent landside security (patrols, surveillance, pier access control), no special requirement in waterways.<br>– Identify restricted area waterway(s) with buoys and signs. |

## 0216. HARBOR SECURITY BOATS

a. Harbor Security Boat (HSB) requirements are driven by the criticality of the asset to be protected. Harbors with home-ported priority A, B, or C assets present shall have a minimum of two boats in the water and available 24 hours per day, 7 days per week.

b. Waterborne patrols are required 24 hours per day, 7 days per week. For installations with priority A assets, at least one patrol will be continuous. For installations with priority B and C assets, patrols may be random during FPCONs Normal and Alpha. However, security patrol craft must be in the water (crew nearby) and ready to get underway immediately. Commanders will determine the frequency of the random patrols at FPCON levels below Bravo. FPCONs Bravo and higher require continuous

patrols whenever priority A through C assets are present. Installations hosting priority A or B assets shall berth assets within barrier system (where installed) and have an HSB dedicated to those piers/areas berthing the high-value unit. Where high-value units are not contiguous, each area must have a dedicated HSB. For harbors without home-ported ships, specifically Naval Weapons Stations, waterborne patrols may be validated dependent on the number of days combatant ships are pierside.

c. Per reference (f), close-in waterside barriers, waterside perimeter barriers, and a brow security system shall be used in conjunction with HSBs to protect submarines armed with nuclear weapons.

d. SWF COs have operational and tactical control of their own NSF personnel and HSBs.

## 0217. SECURITY OF MATERIAL

a. Safeguard controlled-inventory items, including drugs, drug abuse items (as identified under subparts 1301.71 through 1301.76 of title 21, CFR, and Public Law 91-513), and precious metals.

b. Policy

(1) Controlled-inventory items shall have characteristics so that they can be identified, accounted for, secured, or segregated to ensure their protection and integrity.

(2) Special attention will be paid to the safeguarding of inventory items by judiciously implementing and monitoring PS measures, including analysis of loss rates through inventories, reports of surveys, and criminal Incident Reports (IRs) to establish whether repetitive losses indicate criminal or negligent activity.

c. Controlled-Substances Inventory. Accountability and inventory of controlled substances shall be as prescribed in reference (ff).

d. A loss-prevention program shall be carried out at every Navy activity.

## 0218. SECURITY OF COMMUNICATIONS SYSTEMS

a. General

(1) The protection provided to communication facilities and systems shall be sufficient to ensure continuity of operations for critical users and the facilities they support. This determination is based on strategic importance, both to the United States and its allies, and on whether or not each mobile system or facility processes, transmits, or receives telecommunications traffic considered crucial by the National Command Authorities, the Chairman of the Joint Chiefs of Staff, or the GCC. Commander, Naval Network Warfare Command, shall be consulted on this issue.

(2) Security for communications systems shall be a part of each command's security program. Security considerations will be thoroughly assessed for each communications system.

(3) Echelon 3 commands shall review their installation's implementation of PS measures for communication systems during inspections, oversight, and staff visits.

(4) Access shall be controlled to all communications facilities; only authorized personnel, including employees and authorized exceptions with escorts, will be allowed to enter. Facilities shall be designated and posted as restricted areas (see section 0210 of this chapter).

(5) Existing essential structures shall be hardened against attacks. This requirement includes large antenna support legs, antenna horns, operations buildings, and cable trays. Future construction programs for critical communications facilities shall include appropriate hardening of essential structures.

b. Echelon 3 commands and staffs shall:

(1) Identify critical communications facilities and mobile systems within their commands.

(2) 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 AT plan; only the applicable parts of the total plan shall be distributed to personnel at the facility or mobile system.

(3) Arrange for security of off-installation facilities and mobile systems with the closest U.S. military installation, including contingency plans for manpower and equipment resources during emergencies. These arrangements may be made by establishing a formal agreement, such as an ISSA. Whether the facilities are located on or off the installation or are mobile, ICOs are responsible for security of communications facilities for which they provide host support.

(4) Implement a training program to ensure that assigned personnel understand their day-to-day security responsibilities and are prepared to implement emergency security actions. The training program shall include the following:

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

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

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

c. Mobile Communications Systems. 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.

## 0219. PROTECTION OF BULK PETROLEUM PRODUCTS

a. General

(1) Commanders of government-owned, government-operated and government-owned, contractor-operated fuel support points, pipeline pumping stations, and piers shall designate and post these installations as restricted areas. This 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. Commanders shall determine the means to protect against loss or theft of fuel at these locations.

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

b. Commanders shall take the following actions to protect their fuel facilities:

(1) 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 as needed based on the threat assessment.

(2) Establish liaison with supporting LE agencies and host nation officials and support agreements, if appropriate.

c. Security Inspections

(1) Navy installations responsible for the security oversight of fuel facilities shall conduct a security inspection of that facility at least once every 2 years.

(2) Inspections will be formal, recorded assessments of crime-prevention measures and other PS measures used to protect the facilities from loss, theft, destruction, sabotage, or compromise.

(3) Commands shall draft a POA&M to correct discrepancies found.

## 0220. WAIVERS AND EXCEPTIONS

a. Wherever mandatory security requirements within this enclosure cannot be met, commands shall enter the discrepancy into CVAMP and request waivers or exceptions from CNO (N4) via the chain of command. Waivers and exceptions will be evaluated based on merit only. All units accepting a higher risk than established through Navy-prescribed AT standards (reference (a)), or the PS and LE standards contained herein, must implement a waiver and exception program. Additionally, for any waivers or exceptions to references (z), (aa), and (gg) through (ii), NAVFACENGCOM must endorse prior to submission to CNO (N4).

b. General

(1) Blanket waivers and exceptions are not authorized.

(2) Waivers and long-term exceptions are self-canceling on the expiration dates stated in the approval letters unless CNO (N4) approves extensions. Cancellations do not require Chief of Naval Operations approval.

(3) All existing permanent exceptions to earlier editions of this instruction are rescinded 3 years after the date of this instruction. Continuing security deficiencies will be reassessed in accordance with this instruction and appropriate waivers and exceptions requested.

c. Waiver and Exception Program. This program provides a management tool for commanders and COs as well as those in the chain of command to review and monitor corrective actions for standards that cannot readily be achieved. All waivers or exceptions must be submitted at a classification level appropriate to the vulnerability and in accordance with reference (i).

(1) Waivers (temporary). Commands must request a waiver when a prescribed Navy standard is not currently achieved but the condition is correctable within a considerable period of time (not to exceed 1 year). Temporary conditions requiring an approved waiver require the use of compensatory measures pending completion of standard achievement.

(2) Exceptions (permanent). Commands shall request a permanent exception when a prescribed Navy standard cannot be achieved or when a correctable security-threatening condition exists that will exceed 1 year to correct. Exceptions should also be submitted when correcting a problem would be cost-prohibitive. Conditions approved as permanent exceptions require compensatory measures. Exceptions can be permanent or approved for up to 36 months.

d. Waiver and exceptions will be routed per table 2-4 below and formatted in accordance with reference (n). Echelon 2 commands are delegated authority to approve initial waivers for subordinate commands and their own headquarters. No further delegation is authorized. The request for waiver must include a complete description of the problem and compensatory measures or alternative procedures, as appropriate. When a waiver request is based on a lack of resources rather than a commander's risk

decision, include appropriate resource allocation module or other resource related requests or action. 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 Branch Head, Protection (OPNAV (N46P)). Waiver extension requests will refer to previous correspondence approving initial and previous extensions, as appropriate.

**TABLE 2-4**
**WAIVER AND EXCEPTION APPROVAL AUTHORITY**

| Policy requirement | Waiver routing | Exception routing |
|---|---|---|
| OPNAV 5530.14E | Installation to region to BSO to echelon 2 (approval authority) | Installation to region to BSO to echelon 2 to OPNAV (N46P) is approval authority) |
| OPNAV 5530.13C | Installation to region to Naval Ordnance Safety and Security Activity to BSO to echelon 2 (approval authority) | Installation to region to Naval Ordnance Safety and Security Activity to BSO to echelon 2 to OPNAV (N46P) is approval authority) |

# CHAPTER 3

## LAW ENFORCEMENT

**0300. GENERAL.** LE operations support good order and discipline on Navy commands around the world. The NSF will operate with restraint and authority, within reasonable standards, and with a minimum use of force, making the NSF ideally suited as a response force for any situation. Wherever Navy installations are located, the NSF will protect and assist the military community. The NSF will preserve the law and help the commander ensure a high standard of order and discipline within the commander's units.

a. The CO is responsible for the good order and discipline of the command.

b. The NSF must have standardized policies and procedures to enforce the law, maintain good order and discipline, investigate offenses, safeguard the rights of all persons, and provide service to the community.

c. All accidents and criminal incidents that occur aboard the installation or ship will be reported to the NSF, which shall take action to cause an initial response to and investigation of the offense.

**0301. CRIME PREVENTION**

a. General

(1) COs shall ensure that their commands conduct crime prevention measures to reduce the risk of crime. These measures must include proactive methods.

(2) The ISO of the host activity will establish a crime prevention program at the installation providing assistance to tenant activities, if requested, including:

(a) Designating a crime prevention coordinator within the NSF.

(b) Publishing procedures for crime prevention.

(c) Maintaining an active liaison with NCIS, local LE, and other organizations to provide for an exchange of crime prevention-related information.

(d) Offering crime-prevention services, including crime-prevention briefings and surveys.

(e) Participating in crime-prevention campaigns to highlight specific crime problems for intensified public awareness efforts. When possible, Navy campaigns should coincide with national crime-prevention campaigns.

(f) Making crime-prevention practices a part of the daily operations of the NSF, involving all members of the unit.

(g) Using all available records and information to develop and maintain trends and analysis information.

b. Crime Prevention Assistance. NCIS STAAT will have personnel trained in crime prevention who can provide assistance in developing or improving NSF crime-prevention programs.

c. Surveys. The NSF shall conduct crime-prevention surveys for living quarters (both residential and barracks), at non-appropriated fund/retail activities, and at morale, welfare and recreational facilities on request. These surveys are designed to assess the vulnerability of the location as a target for crime and to provide recommendations to reduce vulnerability. The NSF should advise these activities of this service, keep a record of all crime-prevention surveys conducted, and follow up to see whether recommendations made have been completed.

**0302. DISSEMINATION OF INFORMATION.** Personnel shall treat the business of the NSF as "For Official Use Only." Information regarding official business will be shared only with those for whom it is intended under established NSF procedures. Examples include responding to information requests, including Freedom of Information Act; Privacy Act; juvenile records; media inquiries; the public affairs office; and requirements and Departmental policy for release of information (references (jj) and (kk) pertain).

**0303. POLICE RECORDS**

a. The ISO shall establish and maintain a police records system which provides for the proper preparation, distribution, reporting, and retention of all reports generated by the NSF. At a minimum, this system will include provisions for the administrative handling of the Department of the Navy Criminal Justice Information System (DONCJIS) Web-based reporting system.

b. Procedures for police reports/forms, records retention, release records, special case records, and distribution are contained in and shall be administered as described in reference (n).

## 0304. SUPPORT TO CIVILIAN LAW ENFORCEMENT AGENCIES

a. Any support provided to civilian LE agencies by NSF will be consistent with the provisions set forth in the current editions of references (ll) and (mm) and the limitations contained in the Posse Comitatus Act, at section 1385 of title 18, U.S.C. Such support may not constitute direct involvement in civilian LE activities. In CONUS, U.S. Fleet Forces Command is the NCC to U.S. Northern Command and provides Navy assistance to civilian authorities as directed.

b. Absent a specific statutory provision, the military will not be used to aid or assist civilian LE in performing the functions of searches, seizures, and/or arrests. However, providing information, advice, training, facilities, and equipment to support civilian LE entities are generally recognized as permissible activities that do not violate the Posse Comitatus Act.

c. The ISO should consult the local SJA before providing support to civilian authorities, even when the support does not violate Posse Comitatus restrictions or DoD and Navy policy. Examples of support that are acceptable include, but are not limited to:

(1) Using NSF to assist civil authorities in the search for missing children.

(2) The use of an MWD in the interest of safety or preservation of life.

(3) Conducting joint crime awareness education programs (i.e., Drug Abuse Resistance Education (D.A.R.E.) programs) at local schools, etc.

d. The ISO shall ensure that all requests meet approval authority and are processed, reported, and reimbursed when applicable.

## 0305. APPREHENSION AND DETAINMENT

a. Authority

(1) Rule 302(b)(1) of reference (nn) gives NSF the authority to apprehend individuals.

(2) NSF may apprehend any person subject to the Uniform Code of Military Justice (UCMJ) if they have a reasonable belief the person being apprehended has engaged or is engaging in criminal activity.

(3) NSF has limited authority to apprehend persons not subject to the UCMJ. In areas under military jurisdiction or control, NSF may take persons not subject to the UCMJ into custody:

(a) Who are found committing a felony or misdemeanor amounting to a breach of peace in areas under military jurisdiction or control. Such persons must be turned over to civil authority as soon as possible.

(b) Who are violating properly promulgated post regulations. These persons may be escorted to the entrance of the base and may be forbidden reentry by the ICO as necessary. If counterintelligence or terrorist-related activities are suspected, NCIS shall be immediately notified prior to release.

(c) In some cases, persons not subject to the UCMJ may be cited for violations of the Assimilative Crimes Act not amounting to felonies or breaches of the peace and referred to a U.S. magistrate.

b. Detainment of Civilians. Title 18, U.S.C., and the U.S. Constitution authorize the detention of civilians for offenses committed on a military installation. Since civilians are not normally subject to the UCMJ, refer civilian violators to a U.S. magistrate for judicial disposition or to the local civil authorities having jurisdiction.

c. Miranda Rights and the UCMJ. Both UCMJ Article 31 (for military personnel) and the Fifth Amendment to the U.S. Constitution (for civilian and military personnel) protect against self-incrimination.

(1) A person subject to the UCMJ who is required to give warnings under Article 31 may not interrogate or request any

statement from a suspect or a person suspected of an offense without first advising individuals' of their rights. However, asking questions without such warnings shall be permissible up to the point at which an individual is suspected of an offense.

(2) Civilian personnel suspected of an offense should be provided with a Miranda warning prior to questioning if they are in custody or otherwise deprived of freedom of action in any significant way. The point at which a civilian is suspected of an offense is the same as military personnel. The warning must be given by LE or investigations personnel.

(3) In exigent circumstances (e.g., a case where the suspect possesses information that could result in serious bodily harm if not immediately divulged), a Miranda warning is not required.

(4) A civilian warning must be given to a juvenile in terms that the juvenile can understand. The warning should be given in the presence of a parent, guardian, or adult advocate in accordance with applicable laws.

d. Foreign Countries

(1) In foreign countries where the United States maintains military facilities, foreign nationals (citizens of that country or another foreign country) who commit an offense against the property of the United States or against the person or property of members of the Armed Forces located at the activity are not subject to the laws of the United States.

(2) Foreign nationals should be warned or advised in accordance with the procedures that control such advice in the country where the base is located. Such situations are extremely sensitive, and specific guidance shall be obtained from the local SJA before any process of apprehension occurs. SOFAs also apply.

(3) Do not question non-English-speaking persons or foreign visitors until their level of understanding of their rights can be fully ascertained. Call the SJA for guidance in any cases where there are questions.

**0306. PERSONAL FIREARMS SAFETY, CONTROL, AND ACCOUNTABILITY**

a. Unless otherwise authorized by applicable law or regulation, personal firearms shall not be possessed, used, introduced, transported, or stored on board a Navy installation, to include a joint base where the Navy is the lead Service, on-base Bachelor Quarters, on-base temporary lodging facilities, and on-base military housing areas (including on-base Public-Private Venture (PPV) housing), without first obtaining prior written approval of the installation commanding officer (ICO). Personal firearms overseas are also governed by applicable Status of Forces Agreements and host nation laws. Section 0306 is founded on a military necessity to maintain good order and discipline and security on board Navy installations. The provisions of this section do not apply to personnel residing in off-base Navy family housing, including off-base family PPV housing.

b. The term "firearms" includes, but is not limited to:

(1) Handguns: pistols, semi-automatic handguns, machine pistols, revolvers, and derringers.

(2) Long Guns: rifles, assault rifles, and shot guns, whether operated by bolt, pump, or lever.

(3) Other Guns: pellet, BB guns and/or any weapon which launches a projectile via explosive or compressed means/ processes which can kill, injure, or maim.

c. The written approval of the ICO shall be obtained by registering the weapon with the nearest Navy armory or NSF designated to process personal firearms registration.

d. All personal firearms approved by the ICO for transport on a Navy installation shall:

(1) Be transported only after installation NSF has been notified.

(2) Be unloaded and transported in the trunk of the vehicle or, if the vehicle has no trunk, be disassembled or

secured with an approved individual trigger or chamber-style lock. The firearm must then be stored in a locked container.

(3) Ammunition will be transported in a separate compartment from the one in which the firearm is stored (e.g., a glove box or secure interior storage box in the passenger compartment).

(4) In all cases, individuals will comply with all federal, state, and local laws and regulations concerning firearm transportation.

e. The ICO may authorize the storage of properly registered personal firearms in on-base Navy or military family housing, including on-base family PPV housing, and in existing Navy armories or weapons containers. Personal firearms storage in other locations on-base is NOT authorized (e.g., Bachelor Quarters, automobiles, and work centers).

(1) Personal firearms must be stored in either a locked container or locked gun rack, or secured with an approved individual trigger or chamber-style gun lock that prevents loading or firing. Ammunition must be stored in a separate locked container.

(2) Individuals storing privately owned firearms and ammunition in family housing (to include on-base PPV housing) will ensure firearms and ammunition are inaccessible to unauthorized persons and minors.

(3) In all cases, individuals will comply with all federal, state, and local laws and regulations concerning firearm ownership, possession, registration and use.

f. Minimum registration and accountability requirements: The ICO shall establish a process for the strict control and accountability of personal firearms authorized on board Navy installations. This process shall include, at a minimum:

(1) Registration, inventory, receipt and de-registration of personal firearms. A locally developed

receipt will be provided to the owner of the personal firearm when turned into the storage facility and retrieved when the firearm is signed out. As part of the registration process, the registering official shall conduct appropriate checks to verify compliance with the Lautenberg Amendment (section 922 of title 18, U.S Code). The registering official shall also obtain a copy of any required state or local registration documentation, as well as verify that any required Navy personal firearm's training has been completed.

(2) Identification of all personal firearms. Personal firearms will be identified by manufacturer, caliber, model, and serial number. This information will be included on the registration.

(3) Semi-annual sight inventories by serial number of personal firearms stored in Navy armories or weapons containers.

(4) Documentation of each time the owner of a personal firearm removes and returns the personal firearm to storage in Navy armories or weapons containers.

(5) Personal firearms approved for storage in an existing installation armory or magazine shall not be stored in the same container or weapons rack with Government arms, ammunition, and explosives.

(6) Personal firearms brought onto an installation after normal duty hours shall be stored at the region or installation security department ready-for-issue facility until the next duty day. Accountability procedures as identified above apply.

(7) Development of procedures for individuals to possess, introduce, transport, and or use properly registered personal firearms onboard a Navy installation for authorized purposes (e.g., target practice at Navy/Morale Welfare and Recreation ranges or hunting, where permitted).

(8) Identification of all prohibited/illegal firearms.

g. Concealed or loaded handguns: Individual state licenses or permits that authorize individuals to carry concealed handguns are not recognized or valid on Navy installations. Under no circumstances will the transportation of loaded or concealed handguns, shotguns, or rifles be permitted on Navy installations except by duly authorized law enforcement personnel or by military personnel in the performance of their official duties.

h. Violations of section 0306 of this Instruction by military personnel may subject them to appropriate administrative and/or disciplinary action under the Uniform Code of Military Justice. Civilian employees may be subject to disciplinary action or administrative action under applicable civilian personnel instructions.

**0307. INVESTIGATIONS**

a. Criminal and traffic investigations are official inquiries into incidents involving the military community. An investigation is the process of searching, collecting, preparing, identifying, and presenting evidence to .prove the truth or falsity of an issue of law. Investigators conduct systematic and impartial investigations to uncover the truth. They seek to determine whether a crime was committed and to discover evidence of who committed it. Investigators' efforts are focused on finding, protecting, collecting, and preserving evidence discovered at the crime scene, or elsewhere, and presenting the information in a logical manner. For investigations to be successful, the investigator must understand the general rules of evidence, provisions and restrictions contained in reference (nn).

b. Regional Investigations Coordinator (RIC)

(1) NCIS shall assign experienced special agents in a nonsupervisory role, on a full- or part-time basis, as the RIC based on factors such as operational tempo, case volume/type, and geographic boundaries. The RIC shall provide direct guidance and support to command investigators. The primary mission of the RIC is to ensure command criminal investigators

(CCIs) produce their own high-quality investigations by providing NCIS special agents to work directly with CCIs, offering guidance, mentorship, and expertise in investigative methods. RIC oversight includes, but is not limited to, training, investigative procedures, case management, investigator screening/selection, and investigative standardization. The region commander and area NCIS Special Agent-in-Charge (SAC) will determine the RIC office location. RIC oversight and responsibilities will encompass all Navy investigators within the region. For the purposes of this chapter, RICs will be used to delineate the organizational relationship between NCIS and CCIs.

(2) Commands that are geographically or remotely separated from their assigned RIC will have a local NCIS special agent identified to assist the CCI staff. The respective NCIS offices will identify a special agent to assist the CCI staff in all investigative matters, which will include oversight, liaison, and training roles.

(3) The ISO and RIC will have approval authority for all investigations initiated by CCIs. In the event an issue arises concerning the initiation, assumption and/or referral of an investigation by CCI personnel, the ISO and RIC will work in concert to resolve the matter. RIC personnel will operate in conjunction with appropriate Regional Security Officer (RSO)/ ISOs to ensure investigative standardization. This cooperation will be accomplished by developing a notification matrix, uniform investigative protocols, professional career development, and the inclusion of CCIs into NCIS criminal investigations.

(4) RIC personnel do not function in a supervisory capacity for command investigators; however, input will be provided with regards to evaluations, fitness reports, performance appraisals, and award recommendations. In some circumstances, the RIC could engage in the direct supervision of the lead CCI. In the event this supervisory relationship exists, the ICO and NCIS SAC must concur, and a written MOU must delineate the roles, responsibilities, and obligations of each party.

c. CCI

(1) Scope. CCIs are primarily tasked to conduct criminal investigations involving UCMJ violations and other criminal acts that are not pursued by NCIS. CCI shall be either

military (MA with Navy Enlisted Classification (NEC) 2002) or civilian personnel (job classification codes of 1801, 1810, 1811).

(2) Jurisdiction. CCIs assigned to ashore and afloat billets will fall under the operational and administrative control of the security officer and will not simultaneously be assigned to another branch in the security department. CCIs receive their authority from the CO and, regardless of rank, will have positional authority to conduct investigations pursuant to the UCMJ. CCIs are limited to the same jurisdictional authority granted other NSF members. Casework with NCIS special agents does not convey special agent authority and jurisdiction to the CCI. During the conduct of some investigations, the CCI may be required to perform official duties off base and in the civilian community. CCIs may also be assigned to conduct industrial accident investigations that may result in claims against the Navy, which shall be coordinated with the Naval Safety Center. The security officer will be briefed on all off-base investigative activities. In the event a CCI is unable to perform an off-base investigative lead or assignment, the RIC will coordinate with the area NCIS office for assistance. Where appropriate, CCIs are encouraged to assist NCIS special agents in the conduct of their investigations. This investigative assistance will broaden and expand the CCI's level of expertise with regard to investigative methods, tactics, and procedures.

(3) Screening/Selection. The RIC, or appropriate NCIS office, and the ISO shall engage in the screening and selection process for prospective civil service personnel holding a job classification of 1801, 1810, or 1811, and work in concert to ensure they select the best candidate available. MAs will go through a screening/selection process when negotiating NEC 2002 investigator orders or course quota fill through their detailer and RIC program manager at NCIS Headquarters. Upon successful screening and selection, member will attend Military Police Investigator course at Ft. Leonard Wood, MO, and receive 2002 NEC upon successful completion. All MAs filling an investigator billet will have the NEC 2002. The selection of CCIs will be based on professional appearance and conduct, eligibility to obtain and maintain a security clearance, as well as demonstrated professional capabilities which should include a thorough knowledge of basic police/patrol procedures, ability to present information in reports and briefs in a clear, logical manner; knowledge of criminal law and procedures, namely the UCMJ; ability to interface with members of the public, both

military and civilians; and knowledge of investigative theory and procedure. In those instances where workload exceeds onboard NEC or job classification coded CCIs, rated MA and civilian 0083 coded personnel may be screened and selected using the same process and criteria to temporarily augment CCIs.

(4) CCIs assigned afloat will utilize the NCIS afloat special agent assigned to the respective carrier/carrier strike group for all investigative matters.

(5) Credentials. The security officer shall issue OPNAV 5580/26 DON Command Investigator ID Card upon assumption of duties. The bearer shall maintain these credentials during the tenure of the CCI assignment. Security officers and RIC personnel shall work in concert in issuing credentials, which should only be performed upon successful completion of the screening/selection and training process. Upon incurring a permanent change of station transfer, termination, or reassignment, the CCI will return the credentials.

(6) Civilian Clothing. The wearing of civilian clothing by duly appointed investigators is authorized for shore-based military CCIs while engaging in investigative activity. The standard for civilian attire should be in keeping with current business and professional protocols, or within the operational needs of an ongoing investigation. Refer to this paragraph when requesting civilian clothing allowance.

## 0308. EVIDENCE HANDLING

a. NSF personnel shall take every precaution to preserve the integrity of evidence in its original condition. NSF personnel must enter evidence into the evidence custody system as soon as possible after its collection, seizure, or surrender.

b. Host activities shall receive and store evidence received from tenant activities in accordance with reference (n). Tenant activities shall not operate their own evidence lockers unless they have the capacity to do so, including suitable storage containers that comply with appropriate standards and a formal agreement with the host activity.

c. An unbroken chain of custody shall be maintained and documented for all evidence in accordance with reference (n).

d. Evidence shall be maintained until it is no longer needed and permission is granted to dispose of it by the proper adjudicating authority or SJA.

**0309. LOST AND FOUND**

a. NSF members who recover property will tag the items with an OPNAV 5527/17A DON Evidence Tag (Index) or OPNAV 5580/17B DON Evidence Tag (Sticker), and complete the OPNAV 5580/22 Evidence Property Custody Receipt. The property will then be relinquished to the lost and found custodian.

b. The lost and found custodian shall maintain a logbook that contains the recovery date, description of item, and final disposition, including date. Quarterly inventories will be conducted by a senior enlisted (E-6 or above) or an officer who is not directly involved in the lost and found process. Records of inventories will be recorded in the lost and found log book.

c. Lost and found property will be stored in a secure area, separate from evidence.

d. Property that is found will be retained for 120 days after attempts to notify the owner have been made. If there is no indication or ownership, the 120 days will commence following the completion of departmental procedures (e.g., posting of notices, advertisements, etc.).

e. Lost and found property will be disposed of in accordance with the evidence disposal procedures in reference (n). For those items that could be used by an installation charitable organization (bicycles, tricycles, etc.), the ISO must coordinate transfer with the SJA.

**0310. JUVENILES**

a. General

(1) The age limits for classifying persons as juveniles vary according to the laws of the particular state. Federal law defines a juvenile as "any person who has not attained his/her 18th birthday."

(2) Active duty military personnel under the age of 18 are subject to the UCMJ and are not affected by juvenile laws.

(3) The security officer of each installation will become familiar with host-state juvenile statutes and prepare Rules, Regulations, and Procedures (RRP), complementary to reference (n), defining actions to be taken with juvenile offenders aboard installation property.

b. Records

(1) The age of an offender has no effect on the need for detailed and accurate records of any incident or complaint. An IR will be prepared on each situation that fits the criteria for that form.

(2) Security units shall establish a separate file for the retention of records concerning juvenile offenders. This file will be in a distinctly different location from adult files to lessen the chance that a juvenile record will be placed in the adult IR files and shall be kept secured to prevent unauthorized disclosure. Access to this file will be restricted to individuals specified by the security officer as having a "need-to-know."

## 0311. DOMESTIC VIOLENCE

a. The role of LE in domestic incidents has become a coordinated community response that includes police, medical, family advocacy, and the military or civilian court system. RRP should be published by each LE agency, detailing the response to the scene and subsequent coordination with the SJA, family advocacy officer, family service center, and NCIS.

b. The NSF shall:

(1) Receive, report, and identify domestic violence incidents. For off-base incidents, the local LE agency shall have jurisdiction and shall be notified immediately.

(2) Complete an on-scene investigation and initiate follow-up investigation within NSF jurisdiction. Witnesses shall be interviewed, evidence seized, and photographs taken of the crime scene and the victim's injuries.

(3) Complete an IR, including a lethality assessment.

(4) Make appropriate notifications.

(5) Aid in the issuance of military protective orders.

(6) Enforce civilian and military protective orders. Orders violations should be investigated and a report forwarded to the command.

(7) Refer any victims of domestic violence to appropriate assistance programs such as the Family Advocacy Program, Victim and Witness Assistance Program, or Sexual Assault Victim Intervention Program.

c. Gun Control Act of 1968. All NSF personnel shall be screened to ensure they are in compliance with reference (k). The Gun Control Act (as amended by the Lautenberg Amendment of 1996) makes it a felony for a person to ship, transport, possess, or receive firearms or ammunition if that person has been convicted in any court of law for domestic violence. No exception is granted for LE, security, and counterintelligence personnel. LE or security personnel who have qualifying convictions or are the respondent to a protective order whether temporary, or permanent, or a restraining order:

(1) May not possess any firearm or ammunition.

(2) Must immediately return any government-issued firearm or ammunition to their supervisor.

# CHAPTER 4

## PHYSICAL SECURITY AND LAW ENFORCEMENT PLANNING

**0400. GENERAL.** A multitude of plans exist that affect PS and LE in the Navy. Since programs such as AT, PS, and LE are all means of FP operations (reference (oo)), each should reinforce the other at every applicable intersection to ensure a more solid FP posture is achieved. For the purpose of this instruction, a protection plan will be any plan that incorporates two or more programs directly associated with FP. This is not to be confused with an FP plan, which would encompass all programs that make up FP.

**0401. REQUIREMENTS**

a. PS and LE plans must complement the AT plan. AT plans will be written in accordance with reference (c) and must be considered when planning PS and LE measures. The planning process requires the identification of special considerations and factors of PS and LE to connect wherever possible to AT measures. This will provide a more comprehensive protection plan. Commanders and COs are encouraged to use a protection plan approach vice maintaining a multitude of separate plans.

b. ICOs shall be provided an LE response capability (which may be provided by nearby installations or MOAs/MOUs with local LE). Patrols should be able to respond to calls for service within 15 minutes. Emergent life-threatening calls will be answered as soon as possible with due regard for safety and traffic conditions.

c. Protection plans shall be reviewed as a part of existing FP-related working group meetings.

# CHAPTER 5

## NAVY SECURITY FORCE

### 0500. GENERAL

a. The NSF employs a combination of active duty and reserve military officer and enlisted, government civilian, and contract personnel who are organized, trained, and equipped to protect Navy personnel and resources under the authority of a Navy commander or CO. It is essential to the Navy's mission readiness that sufficient NSF personnel are fully resourced, trained, qualified, and assigned to Navy activities to meet the requirements of this instruction and all higher headquarter guidance. BSOs have the overall authority and responsibility to identify the appropriate staffing and skill level of NSF personnel required to meet the Navy's security mission (reference (pp)).

b. To maximize efficiency and effectiveness, region commanders/numbered fleet commanders should implement the following to the fullest extent possible:

(1) Common procedures and equipment for all security organizations under their cognizance.

(2) Prioritization of critical situations and coordinated, flexible command and control for all security forces.

(3) Regional programs, where feasible, for security functions such as training, investigations, harbor security protection, and MWD programs (including contract detection dogs.)

(4) Consolidated AT planning and exercises.

(5) Ensure that NSF personnel throughout the force understand the primacy of the AT task. In support of that priority, when negotiating contracts with union bargaining units and contractors, ensure that appropriate increased emphasis is placed on the AT mission and the associated tasks, duties and skills required.

## 0501. NAVY SECURITY FORCE PERSONNEL

a. The NSF is a composite force which consists of the following types of personnel, whose duties involve AT, PS, LE, NSF training and sustainment, and regional, installation, and afloat program management:

(1) Permanently assigned active duty officer and enlisted Navy personnel.

(2) Government civilian personnel (including Department of the Navy (DON) police, PS specialists, and other administrative support specialists). Minimum civil service qualifications for security force personnel are specified in reference (qq) and are set forth by the U.S. Army as the executive agent for civilian security guards and police. Positions will be classified based on duties actually performed in concert with the authorized grade levels for the position. Uniform allowances, where appropriate, will be funded by resource sponsors in accordance with levels set forth by the Office of Personnel Management.

(3) Government civilian personnel who are part of an A-76 service provider support and are responsible to the security department for non-guard services. While these personnel are not considered NSF, they are required to wear a distinctive uniform, as outlined in the Non-Guard Services Performance Work Statement.

(4) Host-nation local-hire personnel at overseas locations. In overseas locations, civilian foreign national personnel are also used as part of the NSF. In such cases, rules and policies governing these guards as part of the security force will be determined locally per applicable agreements.

(5) Contract personnel. Federal law, including section 2456a of title 42, U.S.C., and the National Defense Authorization Act, addresses the legality of using contracted personnel. When determining whether the use of contract personnel is appropriate, ICOs should first consult with their SJA or office of general counsel attorney. Contractor personnel will not be assigned to perform LE duties.

(6) Auxiliary Security Force (ASF) personnel. The ASF is used to augment the installation's permanent security forces

during increased FPCONs or when directed by the ICO. The ASF is under the operational control of the ICO and ISO of the installation to which assigned.

(7) Ship's Self-Defense Force (SSDF). SSDFs shall be established in accordance with reference (rr). The SSDF provides the CO with a capability to immediately augment the afloat/ashore NSF with armed, trained, and equipped response force. The SSDF is organized and trained by the ship's security officer as a surge capability for the NSF forces. During increased FPCON, the SSDF may augment the deck watches. The SSDF may also be activated during various operations, such as non-combatant evacuation operations, refugee embarkation operations and mass casualty operations.

(8) Navy Reserve (NR) NSF personnel. NR personnel are assigned to NR NSF units established at each installation and are intended to meet additional NSF manning requirements resulting from prolonged increased FPCONs, normally 30 to 35 days, and as directed by the ICO. The NR NSF unit CO/officer in charge will be the primary point of contact for the ICO for all NR NSF issues. Region commanders have the authority to reassign NR NSF personnel within the region as needed.

(a) Installation/NR NSF Integration. The NR NSF unit will be integrated into the installation's security team through regular drill periods conducted at the installation being supported. In those cases where the NR NSF unit is not collocated with the supported installation, the BSO will ensure that travel and per diem funding is available to support on-site drill periods.

(b) Resourcing the NR NSF. The supported installation is responsible for training, equipping, outfitting, and documenting the qualifications of the assigned NR NSF unit and shall provide the resources to include organizational clothing and adequate training ammunition/range time to achieve and maintain weapon operations proficiency.

(c) NR NSF Assignments. Each ICO will fully identify in the installation AT plan how the NR NSF will be manned, trained, equipped and utilized to meet increased FPCON.

b. NSF Occupations. Jobs, positions and collateral duties within the NSF include:

(1) Sentry. A sentry may be assigned to positions where primary duties involve manning a stationary/static guard position, a walking post or a security patrol.

(2) Patrol Officer. Patrol Officers are assigned to positions where primary duties involve LE. The patrol officer may be assigned collateral duties, such as Field Training Officer (FTO), customs inspector, AA&E custodian, or reaction force member/leader. Contract personnel will not be assigned to patrol positions.

(3) HSB Coxswain. The HSB Coxswain will normally be in charge of the security boat and its mission, unless another person is specially assigned, such as a boat officer.

(4) HSB Crew Member/Gunner. An HSB crewmember/gunner may be assigned to positions where the primary duties include working as a member of a security boat team, or manning a crew-served weapon to provide protective fire during security boat operations.

(5) MWD Handler

(a) Where assigned to installation security departments, MWD handler shall be assigned to specific watch sections, under the control of an assigned watch commander, and perform duties commensurate with their pay grade and level of post qualification.

(b) Where assigned to a deployable kennel or expeditionary security unit, the MWD handler will be assigned specific team assignments commensurate with their pay grade and level of mission qualification.

(6) Kennel Master

(a) Normally assigned to a region or NCC staff, and may be assigned to installations where there are seven or more teams assigned.

(b) Where assigned to an installation and not the operations officer, assistant operations officer, or training officer, performs duties in the training section or as a special staff assistant and is not in operational control of the assigned MWD teams.

(c) MWD specific duties and responsibilities are provided in reference (ss).

(7) Reaction Force Members. The duties of the reaction force members are normally assigned to patrol units on the base. During period of heightened threat, additional reaction units may be formed to support the base protective operations. Special duties and training are discussed in chapter 6 of this instruction and reference (n) and are based on the level required for the function performed.

(8) Watch Commander. Responsible for supervising all watch section responsibilities, to include patrol, sentries, harbor security, and the armory and reaction force.

(9) Patrol Supervisor. The patrol supervisor, where assigned, is responsible for mobile supervision of patrols and sentries, and acts as backup relief for the watch commander. The patrol supervisor may also act as the incident command post leader during high-risk incidents.

(10) Investigations/Protective Service Specialist. Investigator/protective service specialist conducts interviews and interrogations; conducts crime scene analysis; collects, analyzes, processes and stores evidence. Supports NCIS to manage and utilize confidential informants; submits evidence for forensic test; conducts surveillance and counter surveillance operations; conducts plain clothes operations; plans and performs investigative raids; protects assigned personnel; and inspects buildings and travel routes.

(11) Training/Planner. Manages the command security and AT training, FTO and Personnel Qualification System (PQS) programs; plans, conducts, and assesses security force drills; coordinates training and security planning with other services and agencies; trains security forces; reviews, plans, and analyzes command security and crises management capabilities; schedules and participates in higher headquarters assessments; operates budget; develops security requirements for new construction; develops standard operating procedures, post orders, and MOAs. Jobs, positions and collateral duties include PS/crime prevention coordinator, weapons/tactics instructor, and security force trainer.

(12) Corrections Specialist. Corrections specialist processes awardees and prisoners; processes and manages enemy prisoners of war; counsels awardees/prisoners; manages prisoner

work details; plans and conducts security drills; tests and monitors security systems; operates control center; and manages PS programs. Jobs, positions and collateral duties include prisoner escort, key custodian, training supervisor, and receiving and release supervisor.

## 0502. STANDARDS OF CONDUCT

a. NSF personnel shall take all reasonable and legal actions within their authority and area of jurisdiction to enforce laws and to ensure the security of the installation.

b. All NSF personnel shall adhere to traditionally established and uniformly accepted standards of conduct and ethics generally applied to all Sailors and LE officials.

c. NSF personnel shall not carry, display, or otherwise use their official position, credentials, badges, or authority:

(1) For personal or financial gain.

(2) For obtaining special privileges not otherwise available.

(3) For avoiding the consequences of illegal acts.

(4) To obtain information outside their scope of duties when it is not otherwise available.

d. All military NSF personnel must be eligible for access to classified information. Additionally, all civilian (both government and contract) NSF personnel must be eligible for access to classified material based on the scope and level of classified information that may be encountered during the execution of assigned duties.

## 0503. NCIS SECURITY TRAINING, ASSISTANCE, AND ASSESSMENT TEAMS

a. NCIS Deputy Assistant Director, Combating Terrorism Directorate (Code 21A) manages the STAAT Program which provides on-site assistance, training, and advice to Naval activities worldwide (ashore/afloat) in various PS, LE and AT disciplines. Mission requirements or tasks from ashore and afloat Navy components or others will be presented at the STAAT Biannual Regional Scheduling Conference.

b. STAAT will directly support NSF, fleet assets, NCIS field offices, and other selected LE organizations and foreign security services. STAAT shall:

(1) Conduct CNOIVAs for Navy activities.

(2) Conduct PIVAs, airfield integrated vulnerability assessments, hotel vulnerability assessments and humanitarian assistance site vulnerability assessments.

(3) Conduct PS/LE assistance visits.

(4) Conduct personal vulnerability assessments of personnel in high risk billet.

(5) Conduct pre-arrival port security assist visits.

(6) Assist BSOs in conducting security staffing/post validations.

(7) Assist the Naval IG office in their area visits.

(8) Provide in-service LE training programs for NSF and NCIS, as well as interoperability exercises with selected foreign LE services.

(9) Provide PS, LE and AT information, personnel, and industrial security training.

(10) Assist with AT and LE exercises.

(11) Conduct MWD certification.

(12) Provide PS/LE technical assistance and training to individual commands upon request.

# CHAPTER 6

## SECURITY AND LAW ENFORCEMENT TRAINING

### 0600. GENERAL

a. NSF personnel will satisfactorily complete the training identified below prior to being assigned security duties. Those training topics below that are further annotated with LE and AS are required only for personnel performing LE/sentry duties. Personnel performing unarmed duties (e.g., unarmed vehicle inspector) are required to satisfactorily complete the training appropriate to their job requirements. Personnel required to be armed as a condition of employment are required to satisfactorily complete all AS annotated subjects. Standardized NSF training material is available on Navy Knowledge Online (NKO).

b. Center for Security Forces (CENSECFOR) is responsible for developing learning solutions and standardized curricula for individual skills training topics.

**0601. NSF APPRENTICE TRAINING REQUIREMENTS**. NSF Apprentice Training may be accomplished via MA "A" School (after September 2006), local or regional security training academy, or a combination to meet the training topics in table 6-1 below. With the exception of weapons qualifications, completion of the Navy's Armed Sentry Course (A-830-0018), or both the NSF Sentry (A-830-2216) and Security Reaction Force Team Member (Basic) (A-830-2217), satisfies the AS skills training (if completed within 3 years prior to assuming AS duties). Personnel qualified as ASs are not certified to perform LE duties unless additional localized training on LE is completed.

### 0602. ANNUAL SUSTAINMENT TRAINING REQUIREMENTS

a. NSF personnel will satisfactorily complete sustainment training for the topics listed in table 6-1 below. This training will be conducted in a manner consistent with implementing guidance established by the appropriate BSO and GCC requirements. Personnel performing unarmed sentry duties (e.g., unarmed vehicle inspector) are required to satisfactorily complete sustainment skills appropriate to their job requirements.

**TABLE 6-1**
**TRAINING MATRIX**

| Security training requirements | Apprentice training | Sustainment training |
|---|---|---|
| ***Administration*** | | |
| Overview/Orientation | X | |
| NSF Duties and Functions | X | |
| Standards of Conduct | X | X |
| Forms and Reports/Report Writing (LE/AS) | X | |
| Area Familiarization/On-Job-Training/FTO (as appropriate to the job assignment) | X | |
| Changes in Standard Operating Procedures, Post Orders, etc. | X | X |
| ***Antiterrorism*** | | |
| AT Level I | X | X |
| Vehicle and Personnel Movement Control (LE/AS) | X | |
| Threat Spectrum (LE/AS) | X | |
| FPCONs and Measures | X | |
| PS Safeguards (LE/AS) | X | |
| ***Legal subjects*** | | |
| Jurisdiction and Authority (LE/AS) | X | X |
| Search and Seizure (LE/AS) | X | X |
| UCMJ (LE/AS) | X | X |
| Self-Incrimination/Admissions and Confessions (LE/AS) | X | X |
| Apprehension versus Arrest (LE/AS) | X | X |
| Legal Testimony; Captain's Mast/Courts Martial (LE/AS) | X | X |
| ***Traffic laws and enforcement*** | | |
| Traffic Control (LE/AS) | X | X |
| Random Vehicle Inspection (LE/AS) | X | X |
| ***Patrol*** | | |
| Crime Scenes/Preservation of Evidence (LE/AS) | X | X |
| Watch-Standing Procedures (LE/AS): | X | X |
| Sentry, ECP | X | X |
| Vehicle/Pleasure Craft/Other Vessel | X | X |
| Situational Awareness | X | X |
| Incident Reporting | X | X |
| Interpersonal Skills | X | X |
| Information Gathering | X | X |
| Tactical Communications (LE/AS) | X | X |
| Illegal Drug Identification (LE/AS) | X | |
| Mobile Patrol Procedures, Vehicle, and Boat (LE/AS) | X | X |
| Drugs of Abuse Identification | | X |
| Vehicle Stops/Search of Vehicles | X | X |
| ***Other security events*** | | |
| Crowd Control (LE/AS) | X | X |
| Preplanned Response Procedures (bomb threat, small boat attack, suspicious package, etc.) | X | X |
| ***Professional skills*** | | |
| Weapons Qualifications (LE/AS) | X | X |
| Use-of-Force Continuum (LE/AS) | X | X |
| Physical Control Techniques (LE/AS) | X | X |
| Approved Non-lethal Weapons training in accordance with Inter-Service, Non-lethal, Individual Weapons Instructor Course (INIWIC) standards (LE/AS) | X | X |
| Cardiopulmonary Resuscitation (CPR) | X | X |
| First Aid (First Responder) | X | X |
| Emergency Vehicle Operations (LE/AS) | X | X |

b. Local and regional training academies shall develop training addressing local policies and directives for incorporation into the standardized training curriculum.

c. Failure to satisfactorily complete sustainment training by the anniversary of the initial or previous sustainment training will result in removal of the individual from assigned duties until such time that the training can be satisfactorily completed. Each standardized plan of instruction will contain the initial training, testing, remediation, and point of failure information.

d. Internal evaluation will be a continuous process that includes assessing the trainee's performance and evaluating the effectiveness of instructional material and presentation methods. Internal evaluations will take the form of written and graded practical examinations and instructor appraisals of students at the completion of instructional segments.

e. External evaluations will determine whether graduate trainees can perform the AS/LE tasks for which they were trained. It will also determine whether the knowledge and skills being trained are required by the tasks to be performed. External evaluations should take the form of on-the-job critiques of recently graduated trainees by an FTO, training supervisors, and security force planners/assessors.

f. Training records for all NSF personnel will be maintained to document all required screenings, annual sustainment training and the qualifications for their assigned post. Training records shall be reviewed quarterly and maintained locally for a period of 3 years after the member's departure.

## 0603. NON-LETHAL WEAPONS (NLW) TRAINING

a. The flow of training for NLW will be: train leaders, train instructors, train unit. In the case of instructors, the process will involve a train-the-trainer system of instruction that utilizes one formal training course to train senior instructors. Senior instructors will perform training at schools, training centers and in mobile training teams to train basic instructors, who will in turn train the NLW users.

b. The Inter-service Non-lethal Individual Weapons Instructor Course (INIWIC) (Marine Corps Course Number A16H5A3/USN Course Identification Number (CIN) A-830-0040) held

at the Marine Corps Unit, Fort Leonard Wood, MO, is the only formal DoD/DON NLW senior instructor-training course. CENSECFOR is quota control for this course.

c. Training for users of NLW will be based on the type of unit and the equipment issued and will be conducted in a structured manner utilizing the INIWIC curriculum course of instruction material. The training requirements of the INIWIC will be the minimum standard for the training of all Navy NLW users.

d. Graduates of the INIWIC course will be referred to as senior instructors and are authorized to train instructor candidates and other personnel in the use of Mechanical Advantage Control Holds (MACH), Hand-Held Defensive (OC) spray, straight baton, expandable baton, handcuffs and flexi-cuffs. Senior instructors will provide USN-specific NLW training to NLW basic instructors, who, in turn, are authorized to train the end user.

e. Instructors who are actively involved in training users will retain their instructor status. Instructors who are inactive for a period of 2 years or more must attend a class delivered by senior instructors to regain their instructor status.

f. Basic instructors are:

(1) Authorized to train individual users only on the equipment and techniques that they have been certified to teach.

(2) Not authorized to train additional instructors.

(3) Not authorized to train individuals to use any NLW other than those listed above.

(4) Not authorized to train individuals assigned to special crowd control units.

g. Training for units that conduct crowd control operations must be delivered by a senior instructor.

(1) This level of instruction by senior instructors will be used to train individual users and will not be used to train additional trainers.

(2) The training provided at this more advanced level will include, at a minimum, the following topics from the INIWIC curriculum:

(a) Rules for the use of force in accordance with reference (aa) identifying proper levels of force, levels of resistance, and how non-lethal technologies affect the force continuum.

(b) Instruction in crowd control techniques and tactics.

(c) Instruction in the stages of conflict management, verbal aggression, non-verbal communication, physical aggression, physiological diversions and communications skills.

(d) Uses of riot control agents and delivery methods in accordance with the unit equipment allowance.

(e) Instruction in crowd control application of the rigid straight baton, expandable straight baton, and riot control baton, if issued to the unit.

(f) Instruction in ROE and the law of armed conflict, as delivered in the INIWIC curriculum.

(g) Instruction in the capabilities and employment of issued NLW munitions.

h. For additional NLW not listed in subparagraph g(2)(d) of this section, training content and delivery solution will be determined by CENSECFOR.

i. For NLW equipment and munitions issued via the Allowance Equipage List/Table of Equipment that are not covered at INIWIC, the following procedures will apply:

(1) Senior instructors are to be trained by manufacturers' representatives.

(2) The senior instructors will provide training to basic instructors.

j. CENSECFOR will coordinate INIWIC quota assignments in accordance with this policy.

k. All individuals trained to use NLW in accordance with this policy are required to receive annual re-qualification training (quarterly re-familiarization is also highly recommended). Annual re-qualification will consist of:

(1) OC Spray: Level 2 or 3 exposure. (Note: Level 1 exposure is required for initial qualification.)

(2) Baton/MACH/Self-Defensive Hand Cuffing: Evaluation of performance measures/tasks required during initial certification.

## 0604. NSF SPECIAL DUTIES AND QUALIFICATIONS

a. All members of the NSF are required to fully meet the qualifications for the function they are performing prior to standing or to assuming the duty, including current weapons qualification on the assigned weapon(s) per reference (tt).

b. Security Officer. Installation and afloat (carriers and large deck amphibious ships) security officers shall successfully complete the Navy Security Force Officer course (A-7H-0007). Each security department will be under the supervision of a security officer who reports to the CO or regional security representative, as appropriate. The security officer will be the principal staff officer to the commander for security and LE matters. The security officer shall be appointed in writing and provided with the training, resources, staff assistance, and authority required in managing and carrying out an effective security program. Specific security officer responsibilities are identified in reference (n).

c. MWD Kennel Masters and Handlers. MWD provide detection and patrol capabilities used by NSF. Kennel masters will be qualified patrol/detector dog handler (NEC 2005) with a minimum of 3 years of experience, and must complete the MWD Supervisor (NEC 2006) course. At commands not having an assigned kennel master, the senior dog handler will be designated as the kennel supervisor, in addition to working his/her assigned dog. Specific responsibilities and duties are identified in reference (ss). Each region shall have a regional kennel master. The regional kennel master must have the NEC 2006 and will report to the RSO. In addition, the regional kennel master will have oversight of all MWD assets within his/her region.

d. Surveillance Detection Units (SDUs)

(1) Surveillance detection teams will be under the operational control of the investigations branch and will seek to detect preoperational terrorist and criminal activities around the installation. All surveillance detection activity will be coordinated with the supervisory special agent of the cognizant NCIS office and with the ISO prior to initiation of any surveillance detection activity. Due to unique SOFAs, host-nation security agreements, and/or interagency agreements that may be in effect for any given country, it is imperative to coordinate with NCIS prior to initiating any surveillance detection activity in foreign locations.

(2) SDUs will be required to train and function within the operating procedures of the ISO. The ISO shall certify that personnel assigned to this function are properly trained before they are assigned to any surveillance missions. A copy of this certification letter will be retained in the NSF surveillance member's training record. The local NCIS office via the RICs will provide in-service training to support this mission. In-service training will be conducted and documented as stipulated in the performance work statement where SDUs are supplied by a non-guard service provider.

# CHAPTER 7

## LEGAL ASPECTS

### 0700. GENERAL

a. PS and LE policy is controlled by a complex array of local, state, and federal statutes, court decisions, and DoD/DON regulations. Within the Department of Defense, the Office of the Judge Advocate General is responsible for reviewing laws, regulations, and court decisions and establishing policies and procedures. SJAs and RLSOs are the security officer's primary resource for guidance on security/LE legal matters.

b. Security officers and NSF training supervisors shall continually monitor changes to the law as it relates to LE procedures and revise apprentice and sustainment training, localized ASF, and AS and LE training lesson plans accordingly. In addition, security officers shall use guard mount to disseminate changes (reference (o)).

### 0701. JURISDICTIONAL REQUIREMENTS

a. The ISO shall describe the jurisdiction of the NSF within written RRP and ensure they understand their jurisdictional limits. RRP must include, and all NSF must be familiar with, the geographic and subject boundaries of their jurisdiction, any agreements or understandings with local LE, and any formal agreements with host nations. The local SJA shall assist the ISO in drafting instructions, training, and RRP pertaining to authority and jurisdiction.

b. NSF shall respond to any criminal or other emergency incident occurring aboard the installation. NSF may respond to off-base incidents only in those cases where there is a clearly established U.S. Government interest, such as military aircraft mishaps. Preliminary response to incidents includes efforts to prevent loss of life or mitigate property damage and to contain or isolate any threat to safety as necessary. After the NSF preliminary response, many incidents may call for referral to other agencies for their subsequent assumption of jurisdiction. Other agencies that may assume control and jurisdiction include the Federal Bureau of Investigation, NCIS, Environmental Protection Agency, explosive ordnance disposal, and the fire department.

c. Within the Department of the Navy, NCIS is primarily responsible for investigating actual, suspected, or alleged major criminal offenses. Major criminal offenses include offenses punishable by death or imprisonment for a term exceeding 1 year. The NSF will immediately notify NCIS regarding major criminal offenses before any substantive investigative steps are taken, including interrogations or searches of property, unless such steps are necessary to protect life or property or to prevent the destruction of evidence.

# CHAPTER 8

## USE OF FORCE AND WEAPONS POLICIES

**0800. GENERAL.** NSF personnel will use sufficient, though not excessive, force to stop whatever offense is being committed. Since "sufficient" and "excessive" are nonspecific terms, any use of force must be justifiable when employed. In the application of deadly force, training and procedures will be conducted in accordance with references (aa) and (uu).

**0801. ARMING REQUIREMENTS**

a. NSF who regularly perform LE and PS duties, including installation entry control and patrols, shall be armed. Specific arming and weapons policy for each post shall be directed in installation post orders. No person will be armed unless currently qualified in the use of assigned weapons and authorized in writing by the CO or designated representative. NSF members will carry a fully loaded weapon and possess at least two full reloads of additional rounds of ammunition (except shotgun) readily available on the person. Weapons-carrying conditions are fully explained in reference (tt). The carrying of unloaded weapons by on-duty personnel is prohibited except while on the firing range or during approved training exercises.

b. No contract guard will bear firearms onboard a Navy installation until written certification of qualification meeting Navy standards is provided by the contractor and the guard has successfully completed training in the use of force. In addition, contractors must comply with provisions prescribed by the state/country in which the contract is administered, including current licensing and permit requirements as needed for the individual or company based on the use of deadly force criminal/civil liabilities. Non-government owned weapons used in the execution of such contracts shall be controlled and issued in the same manner as government owned weapons.

c. NSF performing duties in direct support of nuclear weapons security or special nuclear material shall be guided in the use of deadly force by reference (bb).

d. While in possession of a privately owned firearm, NSF personnel will not identify themselves as a representative of the NSF or other government LE agency.

e. Any NSF member convicted of or under investigation for domestic violence shall not be permitted to possess a firearm (see section 0311 of this instruction).

**0802. NON-LETHAL WEAPONS.** NSF personnel shall be armed with weapons or equipment other than firearms that when applied, even though their intended purpose is non-lethal, could cause death or serious bodily harm (reference (vv)). NLW add an extra level of force that NSF personnel may employ to deescalate a situation prior to the necessity of using deadly force.

# CHAPTER 9

## EMERGENCY VEHICLES

### 0900. GENERAL

a. BSOs will ensure that the NSF is furnished with sufficient vehicles to maintain required patrol standards, respond to alarms and emergencies, and maintain supervision. This responsibility includes the replacement of vehicles when they are no longer reliable for the performance of PS/LE functions.

b. Emergency vehicles that will be used in, or will transit, proprietary or concurrent jurisdiction areas on or off base shall conform to local and state requirements for the equipping and certification of LE emergency vehicles.

c. Emergency vehicles operated on Navy installations in the United States shall conform to the emergency lighting requirements of the local state code. As a general policy, emergency lighting on emergency vehicles will be mounted on the roof of the vehicle with any additional operational lights mounted on fenders, grills, etc. ISOs may authorize certain vehicles to have lights inside of the vehicle on the dashboard or rear deck.

d. Vehicles operated on Navy installations in foreign countries will use flashing red or red/blue combination lights as determined by local requirements. Echelon 2 commands of overseas activities may approve waivers for emergency vehicle standards when compliance is not viable due to non-availability of vehicles or equipment or to restrictions imposed by local SOFA or North Atlantic Treaty Organization agreements. OPNAV (N46P) approval is required for extensions and exceptions.

### 0901. EMERGENCY VEHICLE USE

a. Emergency vehicles will be used by NSF personnel solely for the performance of their assigned PS/LE duties. All NSF personnel who operate emergency vehicles shall attend Naval Safety Center or Department of Transportation approved Emergency Vehicle Operators Course at least once every 3 years.

b. ISOs shall establish, in writing, those areas where on-duty NSF may make an expedient stop for the purpose of subsisting.

c. When engaged in pursuit driving, NSF personnel must use safe speed and always consider public safety. When a pursuit crosses into a jurisdiction where an MOU or MOA exists, the concurrent agencies must be notified as soon as practical. When a pursuit crosses into a jurisdiction where no MOU or MOA exists, state and local laws regarding hot pursuit will be obeyed.

(1) Pursuits at high speeds are justified only when NSF members know or have a reasonable belief that the violator has committed or attempted to commit a life-threatening offense or felony. This includes offenses that involve an action or threatened attack which NSF members have reasonable cause to believe that the incident has resulted in (or is likely to result in) death or serious bodily injury (e.g., murder, attempted murder, kidnapping, aggravated assault, armed robbery, or arson of an occupied building or resource).

(2) If necessary and within local constraints, NSF patrols are permitted to use pursuit driving at safe speeds to apprehend motor vehicle operators who have committed traffic violations, minor offenses, or felonies not previously addressed.

(3) At no time will NSF use pursuit driving at speeds that will endanger the public or contribute to the possible loss of control of the vehicle.

(4) The responsibility for making the decision to pursue an offender and method used lies with the individual NSF patrol. However, if a pursuit is initiated, the ISO or watch commander will monitor and may terminate the pursuit at any time if he or she feels it is in the best interest of safety.

# CHAPTER 10

## SECURITY FORCE COMMUNICATIONS SYSTEMS

### 1000. GENERAL

a. Navy activities must maintain communications systems for use in emergencies to facilitate effective command and control and allow for increased requirements to maintain sure and rapid communications throughout response and recovery operations. Reference (bb) provides policy for provisioning internal security (including police and security) with communications equipment, including control (base), mobile, and repeater systems.

b. The provisions within this chapter apply to shore installations and shore-to-ship security communications.

### 1001. REQUIREMENTS

a. ICOs, through the region commander, shall ensure that comprehensive communication plan annexes are included in AT plans or other relevant plans. These annexes will include the concepts of emergency communications, a frequency plan, system requirements, and equipment requirements for the NSF.

b. The NSF shall have sufficient equipment to maintain continuous two-way voice communications among all elements of the security force. Two-way radio shall be the primary means of communications between the dispatcher and field personnel.

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

d. Interoperability shall exist between NSF and other emergency responders.

e. The provisions of reference (f) take precedence, where applicable.

f. Operational tests of all communication circuits will be conducted daily to ensure they are operating properly. Electronics personnel will conduct maintenance inspections of all communications equipment periodically.

## 1002. COMMUNICATIONS EQUIPMENT

a. Routine NSF duties require effective coordination and communication with other police agencies, fire departments, emergency medical services, Navy activities, and public service organizations. NSF must be outfitted with communications equipment that provides effective communications not only between the NSF members, but also with those emergency responders and security activities with whom they may interact in any given situation.

b. As Navy commands replace aging equipment and adopt new technologies, they must ensure that essential communication links exist within their safety, security, and service activities that permit units from multiple activities to interact with one another and to exchange information according to a prescribed method to achieve predictable results. These methods and results will be contained in communications annexes to AT plans.

c. To ensure cost-effectiveness, efficiency, and the greatest possible interoperability with federal, state, and local community emergency responders, Navy activities should comply with the NAVFAC AT rollout when purchasing any type of communications equipment. NAVFAC will ensure that communications equipment meets established digital standards for wireless communications users.

# CHAPTER 11

## INCIDENT REPORTING AND THE NAVY SECURITY NETWORK

**1100. GENERAL.** NSF units shall use the DONCJIS Web-based reporting system to support higher headquarters and to comply with mandated National Incident-Based Reporting System (NIBRS) and Defense Incident-Based Reporting System (DIBRS) crime and incident reporting requirements.

**1101. REPORTING REQUIREMENTS**

a. Criminal complaints, activities, and significant incidents will be reported via an IR using DONCJIS.

b. ISOs will direct the preparation of an IR for every criminal complaint or significant incident that is brought to the attention of the NSF. Complaints against members of the NSF, on or off duty, will also be documented on an IR.

c. DONCJIS will be the only system used for vehicle registration.

d. Matters in the following categories will be reported on the documents indicated and will not be reported by IR:

(1) Non-significant incidents recorded in the Department of Navy Desk Journal will be recorded using the DONCJIS Desk Journal module (e.g., such as funds escorts, traffic control operations, etc.)

(2) Contact with individuals under suspicious circumstances but with no immediate indication of criminal activity recorded on OPNAV 5580/21 Field Interview Card.

(3) Impounding abandoned motor vehicles or voluntary storage of motor vehicles on OPNAV 5580/12 Department of the Navy Vehicle.

e. Consolidated Law Enforcement Operations Center (CLEOC) data will be available for up to 3 years beyond the full implementation of DONCJIS. Since data in that system can not be moved over to DONCJIS, CLEOC information will be maintained until it is closed out.

# APPENDIX A

## POST VALIDATION MODEL AND STAFFING

1. Post Validation Model

a. Mission Profile Validation - Protection (MPV-P) is the CNO (N4) developed model used to determine posts required to meet protection requirements, associated staffing and resource options. This model and security staffing process enables installations, claimants, and resource sponsors to identify and prioritize requirements, capabilities, and resources. MPV-P incorporates the Required Operational Capability (ROC) construct, FPCONs, validates technology as a resource capability, and contains both workload and resource based requirements to provide layered defense to assets through FPCON Bravo.

b. MPV-P is the only approved model authorized for use to determine and validate shore installation and activity security post and staffing requirements.

c. All shore installations and activities will be validated using MPV-P. Once validated, MPV-P results (post validations) should be reviewed routinely for modification, specifically when triggered by a change in:

(1) Mission (ex: ROC, assets, base realignment and closure affects)

(2) Resources (ex: technology install/removal)

(3) Significant increase in workload/throughput data

d. Post validations will be conducted every 5 years.

e. Post validations, including interim changes, will be submitted to Ashore Readiness Division (OPNAV (N46)) for approval. OPNAV (N46) will establish and publish a process to enable region commander, BSO, NCC, and claimant review and comment prior to signature.

2. Staffing Standards

a. Specific resource and workload metrics, methodology, calls for service, case load, etc., used to determine post and resource requirements are contained in MPV-P. Staffing

positions, typically non-guard and security departmental organization, will be assessed by normal frequency, task, and function criteria.

b. Where feasible, NSF administrative management should be organized into a regional force structure. Staffing standards, when applied within a regional framework, have proven to be the most cost-effective and efficient security force structure. They provide the following capabilities and enhancements:

(1) Common procedures and equipment for all units in the area.

(2) Increased ability to prioritize critical situations and provide coordinated, flexible command and control for all security forces.

(3) Realized savings affiliated with regional security systems.

(4) Increased security, inherent with a regional reinforcement capability.

(5) Enhanced training achieved by a consolidated AT planning, exercises, and training program.

c. As functions are regionally aligned, operational control of NSF shall always remain with the ICO.

3. Security Patrols

a. There are no minimum number of patrols assigned to installations. All installations shall be provided an LE response capability, which may be provided by nearby installations or local LE.

b. Security patrols are armed, single-person mobile patrol units assigned to a specific asset protection zone. Asset-based patrols shall be validated for specific assets in designated restricted areas (flightlines, piers, SCIFs, etc.).

c. Asset-based patrol zone size will be determined using the individual asset response time requirements. Asset-based patrols also serve as deterrent patrols capable of performing traditional directed and non-directed patrol activities, particularly at lower FPCONs.

d. Additional incident-based patrols may be validated using workload (calls for service) where patrol activities exceed the capability of, or the time-to-respond tether of, asset-based patrols. At installations without assets that have specified response/patrol requirements, patrols will be validated using only workload factors.

e. Patrols within noncontiguous fence lines and installation outliers, including off-base housing, will be assessed and validated individually based on ROC level and parent installation capabilities.

f. Planning and resource factors used to determine the total number of patrols, including backup patrols, include installation size, population, calls for service, speed limits, and geography (time/distance).

g. Patrol and watch section supervisors will be validated based on section size (minimum 15/section) and/or complexity of operations (ROC 1/2 installations).

4. Gate Staffing Process

a. Every installation with a gate and perimeter fencing or barrier will have at least one primary external vehicle ECP validated. Installation ECPs, when not automated, are manned by armed personnel. Noncontiguous fence lines and installation outliers will be assessed individually based on ROC level and parent installation capabilities.

b. Additional external ECPs will be validated based on workload (throughput) using metrics that enable FPCON Bravo level identification verification.

c. Non-automated pedestrian access control points will be kept to a minimum and will validated by workload.

d. ECPs with high-volume traffic (vehicular and foot) may require multiple sentries to handle the workload. Each post will be individually assessed and validated to support the workload and security requirements of the post.

e. Internal ECPs will be validated to control access to restricted areas and assets as described in section 0210 of this instruction.

5. Patrol Boat Staffing

a. Patrol boats will be validated based on the assets to be protected and waterfront area to be patrolled in accordance with section 0216 of this instruction and reference (n).

b. Each HSB will be validated for a minimum of at least two personnel.

6. Investigation Staffing

a. The number of investigators will be determined by conducting an assessment of the annual case workload per installation. Commands with an insubstantial workload should train back-up investigators.

b. At regions with multiple installations whose case workload does not warrant the validation of a full-time investigator, one or more investigators may be validated for as-needed assignment within the region.

7. Administrative/Support Staffing

a. Non-Guard Services (NGS) comprise vehicle inspection teams, administrative support, pass and identification, trainers, explosive detection dogs, armorer, logistics, surveillance detection, and crime prevention personnel. Requirements are so divergent that trained staffing personnel will validate each location.

b. At installations whose NGS are performed by a service provider (A-76), the performance work statement shall serve as the requirement.

8. FPCON Charlie and Delta Staffing. Specific capabilities, workload, and utilization of baseline NSF are so divergent based on each installation's AT plan, mission, and assets, that trained staffing personnel will validate ASF and NR NSF requirements at each location.

# APPENDIX B

## DEFINITIONS/ACRONYMS

### Glossary

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 activity CO as to the methods and procedures to be employed.

Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. AT measures are taken to detect, deter, defend, defeat and mitigate acts of terror.

Armed Sentry (AS). A person equipped and properly qualified with a firearm and ammunition whose primary function is to protect personnel and/or property.

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 NSF. The ASF is used to augment the installation's permanent security force during increased threat conditions or when directed by the chain of command.

Contact Sentry. The NSF or ASF member who is first to make contact with those seeking entrance into the installation, pier, flightline, or other controlled entry point. The contact sentry will verify that individuals seeking to gain access have valid military or civilian photo identification and that automobiles have proper documentation (vehicle decal, pass, or rental agreement) prior to granting access. The contact sentry may be required to perform inspections of packages, vehicles, or individuals.

Cover Sentry. The cover sentry, or back-up sentry, is the NSF member who provides the second layer of defense/deterrence and is assigned to cover and defend the contact sentry(ies). This sentry must be behind cover and have the ability to bring his/her weapon to the ready to engage or stop a deliberate breach of the gate.

Critical Asset. Critical assets may be DoD assets or other government or private assets (e.g., industrial or infrastructure critical assets), domestic or foreign, whose disruption or loss would render DoD critical assets ineffective or otherwise seriously disrupt DoD operations.

Deadly Force. The force that a person uses causing, or that a person knows or should know would create, a substantial risk of causing, death or serious bodily harm.

Electronic Security Systems. Part of PS concerned with the safeguarding of personnel and or property by use of electronic systems. Systems include, but are not limited to, intrusion detection systems, AECS, and video assessment systems.

Entry Control Point (ECP). Installation ECPs include those used for vehicle or pedestrian access. Installation ECPs should use appropriately armed and positioned sentries, as well as vehicle barriers, to ensure the integrity of these vital areas. In non-Navy ports, the entrance to the area where the ship is moored is considered an ECP.

Force Protection (FP). Actions taken to prevent or mitigate hostile actions against DoD personnel (including family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy.

Force Protection Condition (FPCON). The DoD FPCON progressively increases protective measures implemented by the DoD components in anticipation of or in response to the threat of terrorist attack. The DoD FPCON consists of five progressive levels of increasing AT protective measures.

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.

Navy Security Force (NSF). The NSF consists of armed personnel regularly engaged in LE and security duties involving the use of

deadly force and unarmed management and support personnel who are organized, trained, and equipped to protect Navy personnel and resources under Navy authority.

Non-lethal Weapons (NLW). Weapons that are explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment.

Physical Security (PS). 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.

Physical Security Program. Part of the overall protection posture at an activity including policy and resources committed to safeguard personnel, protect property, and prevent losses. PS is further concerned with means and measures designed to achieve FP and AT readiness.

Physical Security Survey. A specific on-site examination or evaluation of PS and loss-prevention programs of an activity by the ISO or designated PS specialist to determine vulnerabilities and compliance with PS policies. Surveys are primarily used as a management tool by the surveyed command.

Protection Plan. Any plan that incorporates two or more programs directly associated with FP.

Ready-For-Issue. Storage of a relatively small amount of weapons and ammunition for duty section police, security guards, and response forces so that they are available for ready access.

Restricted Area. An area that is posted, and normally fenced, from which personnel, vessels, aircraft, or vehicles other than those required for operations are excluded for reasons of safety or security. This does not include those designated areas restricting or prohibiting over-flight 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. These areas must be authorized by the installation/activity, provide notice to the public, and employ PS measures.

## List of Acronyms

| | |
|---|---|
| AA&E | Arms, Ammunition, and Explosives |
| AECS | Automated Entry Control System |
| AOR | Area of Responsibility |
| ART | Armed Response Team |
| AS | Armed Sentry |
| ASF | Auxiliary Security Force |
| AT | Antiterrorism |
| BSO | Budget Submitting Office |
| CAC | Common Access Card |
| CBS | Close Boundary Sentry |
| CCI | Command Criminal Investigator |
| CENSECFOR | Center for Security Forces |
| CFR | Code of Federal Regulations |
| CLEOC | Consolidated Law Enforcement Operations Center |
| CNOIVA | Chief of Naval Operations Integrated Vulnerability Assessment |
| CO | Commanding Officer |
| COTP | Captain of the Port |
| CVAMP | Core Vulnerability Assessment Management Program |
| DoD | Department of Defense |
| DON | Department of the Navy |
| DONCJIS | Department of the Navy Criminal Justice Information System |
| ECP | Entry Control Point |
| FP | Force Protection |
| FPCON | Force Protection Condition |
| FTO | Field Training Officer |
| GCC | Geographic Combatant Commander |
| HSB | Harbor Security Boat |
| ICO | Installation Commanding Officer |
| INIWIC | Inter-service, Non-lethal, Individual Weapons Instructor Course |
| IR | Incident Report |
| ISSA | Inter-Service Support Agreement |
| ISO | Installation Security Officer |
| JSIVA | Joint Staff Integrated Vulnerability Assessment |
| LE | Law Enforcement |
| MA | Master-at-Arms |
| MACH | Mechanical Advantage Control Holds |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| MPV-P | Mission Profile Validation - Protection |
| MSC | Military Sealift Command |
| MWD | Military Working Dog |
| NAVFAC | Naval Facilities Engineering Command |

| | |
|---|---|
| NAVFACENGCOM | Commander Naval Facilities Engineering Command |
| NCIS | Naval Criminal Investigative Service |
| NEC | Navy Enlisted Classification |
| NGS | Non-Guard Services |
| NLW | Non-Lethal Weapon |
| NR | Navy Reserve |
| NSF | Navy Security Force |
| OC | Oleoresin Capsaicin |
| OPNAV | Office of the Chief of Naval Operations |
| POA&M | Plan of Action and Milestones |
| PIVA | Port Integrated Vulnerability Assessment |
| PS | Physical Security |
| RIC | Regional Investigations Coordinator |
| RLSO | Regional Legal Service Office |
| ROC | Required Operational Capability |
| ROE | Rules of Engagement |
| RRP | Rules, Regulations, and Procedures |
| RSO | Regional Security Officer |
| SAC | Special Agent-in-Charge |
| SCIF | Sensitive Compartmented Information Facility |
| SDU | Surveillance Detection Unit |
| SECNAV | Secretary of the Navy |
| SJA | Staff Judge Advocate |
| SOFA | Status of Forces Agreement |
| SSBN | Ballistic Missile Submarine |
| SSDF | Ship's Self-Defense Force |
| SSS | Strategic Sealift Ship |
| STAAT | Security Training, Assistance and Assessment Team |
| SWF | Strategic Weapons Facility |
| UFC | Unified Facilities Criteria |
| USACE | U.S. Army Corps of Engineers |
| U.S.C. | United States Code |
| USCG | U.S. Coast Guard |

## APPENDIX C

## REFERENCES

(a) OPNAVINST F3300.53B, Navy Antiterrorism Program (NOTAL)
(b) OPNAVINST 5530.13C, DON Physical Security Instruction for Conventional Arms, Ammunition, and Explosives (AA&E)
(c) DoD Instruction 2000.16, DoD Antiterrorism Standards, of 02 Oct 06
(d) DoD Directive 2000.12, DoD Antiterrorism Program, of 18 Aug 03
(e) DoD 5200.08-R, Physical Security Program, of 09 Apr 07
(f) SECNAVINST S8126.1, Navy Nuclear Weapons Security Policy (NOTAL)
(g) OPNAVINST 5210.16, Security of Nuclear Reactors and Special Nuclear Material
(h) SECNAVINST 5239.3A, DON Information Assurance (IA) Policy
(i) SECNAVINST 5510.36A, DON Information Security Program Instruction
(j) SECNAVINST 5510.30B, DON Personnel Security Program (PRP) Regulation
(k) DoD Instruction 5210.65, Minimum Security Standards for Safeguarding Chemical Agents, of 12 Mar 07
(l) OPNAVINST 3400.12, Required Operational Capability Levels for Navy Installations and Activities
(m) NTTP 3-07.2.1, Antiterrorism/Force Protection (NOTAL)
(n) NTTP 3-07.2.3, Law Enforcement and Physical Security for Navy Installations (NOTAL)
(o) NTRP 3-07.2.2, Force Protection Weapons-Handling Standard Procedures and Guidelines, August 2003 (NOTAL)
(p) Public Law 94-524, Presidential Protection Assistance Act of 1976 (NOTAL)
(q) DoD Directive 3025.13, Employment of Department of Defense Resources in Support of the United States Secret Service, of 13 Sep 85
(r) DoD Instruction 5030.34, Agreement Between the United States Secret Service and DoD concerning Protection of the President and Other Officials, of 17 Sep 86
(s) CNO WASHINGTON DC 051201Z JUN 08 (NAVADMIN 160/08), Subj: Individual Augmentee Policy Update
(t) SECNAV M-5210.1, DON Records Management Manual
(u) SECNAV M-5214.1, DON Information Requirements (Reports) Manual
(v) OPNAVINST 3500.39B, Operational Risk Management (ORM)

(w) NAVSEASYSCOM Standard Item 009-72, Physical Security at Private Contractor's Facilities (NOTAL)
(x) SECNAVINST 5530.4D, Naval Security Force Employment and Operations
(y) DNS Memo Subj: Discontinuation of the DoD Form 2220 (Vehicle Decals), of 23 Aug 07 (NOTAL)
(z) UFC 4-022-01, Security Engineering: Entry Control Facilities/Access Control Points, of 25 May 05
(aa) SECNAVINST 5500.29C, Use of Deadly Force and the Carrying of Firearms by Personnel of the Department of the Navy in Conjunction with Law Enforcement, Security Duties, and Personal Protection
(bb) CJCSI 3121.01B, Standing Rules of Engagement/Standing Rules for the use of Force for U.S. Forces (NOTAL)
(cc) SECNAVINST 5430.107, Mission and Functions of NCIS
(dd) OPNAVINST 3750.6R, Naval Aviation Safety Program
(ee) DoD O-2000.12H, DoD Antiterrorism Handbook, of 01 Feb 04
(ff) BUMEDINST 6710.70, Guidelines for Controlled Substances Inventory
(gg) UFC 4-010-01, DoD Minimum Antiterrorism Standards for Buildings, of 08 Oct 03
(hh) UFC 4-010-02, DoD Minimum Antiterrorism Standoff Distances for Buildings, of 08 Oct 03
(ii) UFC 4-021-01, Design and O&M: Mass Notification Systems, of 09 Apr 03
(jj) SECNAVINST 5211.5E, Department of the Navy (DON) Privacy Act Program
(kk) SECNAVINST 5720.42F, Department of the Navy Freedom of Information Act (FOIA) Program
(ll) DoD Directive 3025.15, Military Assistance to Civil Authorities, of 18 Feb 97
(mm) SECNAVINST 5820.7C, Cooperation with Civilian Law Enforcement Officials
(nn) Manual for Courts Martial, United States, 2008 Edition
(oo) Joint Publication 3-07.2, Antiterrorism, of 14 Apr 06 (NOTAL)
(pp) OPNAVINST 1000.16K, Navy Total Force Manpower Policies and Procedures
(qq) DoD Instruction 5210.90, Minimum Training, Certification, and Physical Fitness Standards for Civilian Policy and Security Guards (CP/SGs) in the Department of Defense, of 09 Jul 07
(rr) OPNAVINST 3120.32C, Standard Organizations and Regulations of the U.S. Navy
(ss) OPNAVINST 5585.2B, DON Military Working Dog Manual
(tt) OPNAVINST 3591.1E, Small Arms Training and Qualification

(uu) DoD Directive 5210.56, Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties, of 01 Nov 01

(vv) DoD Directive 3000.3, Policy for Non-lethal Weapons, of 09 Jul 96