Now that CNICINST 5530.14 has been signed, we anticipate that upcoming changes will occur in THREE PHASES. Our goal is to have all three changes/phases completed no later 30 Apr 2012.

Phase I - Change 1 to CNICINST 5530.14

1. Staffing start date: 6 Oct 11
2. Date up for signature: 6 Nov 11
3. Tentative topics for Change 1:

   b) Decal portion or status update
   c) Search prior to ambulance transport of violent patients
   d) Low man gate Procedures
   e) NSF Responsibilities for Courthouse Security
   f) Establish standardized physical exam procedures for 083/085 (initial and sustainment)
   g) LE database information access
   h) Investigatory limitations for 083s
   i) Capabilities of NCIS Agents/Analysts
   j) Dispatch time requirements
   k) CLEOC Roles and responsibilities
   l) eGuardian and Suspicious Incident Templates
   m) VWAP
   n) TSC Handling codes
   o) Post Checks
   p) Decal guidance and or update
   q) Wide Area Alert Network emergency management 3440
   r) Police Vehicle Markings
   s) Remedy
   t) Low Man Gates
   u) Barrier/Bollard update to include types and training
   v) Small arms ranges
   w) QRT (Shoot, Move, Communicate)
   x) Inert training device handling and storage
   y) IATP
   z) CVAMP
   aa) NCACS
   bb) Decal
   cc) Risk Informed Investment Strategy
   dd) AEL/Equipment update
   ee) IDS
1. Staffing start date: 6 Dec 11
2. Date up for signature: 10 Jan 12
3. Tentative topics for Change 2:

a) Senior Personnel Training Requirements
   - Patrol Supervisors
   - Senior Civilian 083 (Chief of Police)
   - Security Officer

b) Oversight visit Requirements
   - Inspections, Technical Assistance & Inspections
   - Conform to DoDI 2000.16 and other requirements

c) Standardized Credentials for NSF

d) NSF equipment update

e) Negligent Discharge (Internal review board process)

f) Minimum installation Law Enforcement capabilities
   required to respond to a crisis: (SRT, C/HNT, MWD, possibly EOD)

g) Intelligence Led Policing

h) Physical security waivers and exception updates

i) HSB Gun Mount requirement- Forward, Aft, Side, ETC

j) Hostage negotiation team standards, requirements, responsibilities, and certification

k) Law enforcement waivers

l) Special missions/events

m) TSC handling codes

n) Post checks

o) Internal Threat Program

p) Firearms simulators

q) Small arms portable ranges

r) Establish and identify specific requirements for
   basic physical security measures such as CCTV and
   IDS

s) 083/085 functional differences and the selection
   process

t) Duties of 085 vs 083

u) How post and reliefs, compensatory time off for
   holiday’s requirements are resourced.

v) NMET’s Appendix

w) COL’s Appendix Functions Of Annual ATWG:
   Standardization
1. Staffing start date: 6 Feb 12
2. Date up for signature: 10 Mar 12
3. Tentative topics for Change 3:
   a) Special reaction team (SRT) capabilities, certification, and requirements (primarily for MOU/ MOA purposes)
   b) Intelligence led policing
      • Police intelligence templates
      • Police intelligence training requirements
   c) DNA collection requirements for criminal investigations directed at Navy MAs.
   d) Patrol zones
   e) STEP program update
   f) Courthouse security
   g) Physical security waivers and exceptions updates
   h) Wide Area Alert Network
   i) Notification of NCIS and TMU/reporting
   j) Surveillance Detection Program
   k) NSF equipment update
   l) Inert Training device handling and storage
   m) Field Training Officer Program
   n) Jurisdiction and authority update
   o) By NSF position or post identifies capabilities desired of NSF to determine whether they are achieving the intended result. With regard to all MPV-P validated positions and special events. The result should be based on the installation design basis threat, measured in DRRS-N and the appropriate PESTOFF pillar.
   p) Use the installation design basis threat to prioritize NSF functions, and develop measurable capabilities to determine if the NSF is achieving the desired result.
   q) MWD
      • Manning
      • Missions
      • Patrol zones
      • Training
CNIC INSTRUCTION 5530.14

From: Commander, Navy Installations Command

Subj: CNIC ASHORE PROTECTION PROGRAM

Ref: (a) OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program, 28 Jan 09
(b) OPNAVINST 3300.53C, Navy Antiterrorism Program, 26 May 09
(c) OPNAVINST 3400.12, Required Operational Capability Levels for Navy Installations and Facilities, 29 Oct 08
(d) DoDI 2000.16, DoD Antiterrorism Standards, 02 Oct 06
(e) DoDD 2000.12, DoD Antiterrorism (AT) Program, 18 Aug 03 (certified current 13 Dec 07)
(f) CJCS Instruction 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force SROE/SRUF for U.S. Forces, 13 Jun 05
(g) NTTP 3-07.2.3, Law Enforcement and Physical Security for Navy Installations, 29 Jan 09
(h) NTTP 3-07.2.1, Antiterrorism, Sep 06
(i) 50 U.S.C., Section 797, Jan 03
(j) SECNAV M-5214.1, DON Information Requirements (Reports) Manual, 01 Dec 05
(k) SECNAV M-5210.1, DON Records Management Manual, 16 Nov 07

Encl: (1) CNIC ASHORE PROTECTION REQUIREMENTS AND STANDARDS

1. Purpose. The purpose of this instruction is to implement responsibilities, set forth best practices, and provide requirements and direction for the protection of people and assets throughout CNIC as directed in references (a) through (f).

2. Cancellation

   a. CNICINST 5530.1A dated 11 December 2007: Taxicab, Limousine and Shuttle Access on Navy Installations
b. CNICINST 5530.3 dated 29 February 2008: Rental Car Access on Navy Installations

c. CNICINST 5560.1 dated 28 June 2006: Online DoD Decal Renewal System

d. CNICINST 5530.4 dated 2 June 2008: Auxiliary Security Force

e. CNICINST 3400.1 dated 10 Dec 2006: Antiterrorism and Emergency Preparedness Consequence Management Required Operational Levels For Navy Installations


3. Background

a. This instruction provides a common organizational framework for Navy Security Forces (NSF) during routine and emergency response activities between Navy Regions, Installations, and ships.

b. The CNIC Ashore Protection Program incorporates a systems approach to integrating antiterrorism (AT), physical security (PS), and law enforcement (LE) capabilities for the prevention or mitigation of hostile actions against personnel, resources, and facilities, both afloat and ashore. This program serves as the principal process for the integration and implementation of the AT, PS, and LE requirements, standards and guidelines directed by references (a) through (f).

4. Policy

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

b. This instruction does not directly apply to afloat units, Navy Nuclear Security, personnel security, information systems security, or chemical agent security.

c. Where this instruction conflicts with the Geographic Combatant Commander (GCC) or assigned Operational Commander
(i.e. Naval Component Commander (NCC)) protection requirements, the GCC's/NCC’s requirements take precedence.

d. Deviation from the policy and standards in this instruction must be documented in the appropriate planning procedures and implementing guidance. A request for a waiver or exception must be submitted in accordance with (IAW) paragraph 0412 of enclosure (1).

e. The policy language used in this instruction includes:

   (1) Policies that include the words “shall, will, or must” are directive in nature and provide standards, measures or actions. An inability to meet these requirements necessitates a request for a waiver or exception.

   (2) Recommended procedures include the word "should". These recommendations provide a framework that support the mandatory polices.

   (3) Enabling procedures include the words "may or can". These are not requirements, but are possible actions or measures to take at the discretion of the responsible party.

   (4) Prohibitive procedures include the words "shall not, will not, or may not" if the action is prohibited without prior authorization. Actions that are advised against but left to the responsible party's judgment include the words “should not”

f. Union notification and subsequent bargaining requirements must be satisfied prior to implementation of this instruction. Regional program managers will advise CNIC Codes N13 and N3AT when notification has been accomplished, and provide periodic status of bargaining until completed.

g. This instruction amplifies the AT, PS and LE aspects of Protection, pillars which complement, integrate with, and support the three Protection core lines of effort (see Figure 1). The primary area of focus for this document is FP. 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.
5. Responsibilities

   a. CNIC N3AT is responsible for:

      (1) Identifying the resources programmed to implement and maintain the Protection Program as part of the planning, programming, and budgeting system process.

      (2) Performing Protection Program planning and resourcing as outlined in reference (b).

      (3) Providing unified and consistent protection procedures, standards of service, and practices for effective and efficient management of installation support.

      (4) Developing, managing, and distributing an Ashore NSF Table of Allowance (TOA).

   b. Region Commanders (REGCOMs) are responsible for:

      (1) Promulgating guidance for Installation Commanding Officers (COs) to establish security measures in accordance with regional guidance and higher headquarters directives.
(2) Exercising geographical area of responsibility command and control and developing and implementing a comprehensive protection plan designed to accomplish all requirements or standards contained in this document.

(3) Assessing installations/facilities to ensure they develop, maintain and implement protection plans and programs. Examples include but are not limited to: AT Plan, Physical Security Program, Law Enforcement Program, General Public Visitation, and Standard Operating Procedures.

c. Installation Commanding Officers (COs) are responsible for:

(1) Providing security for resources, facilities, mission critical assets, CIP, and personnel under their authority (including family members and civilians when applicable) and control consistent with threat, risk, vulnerability, criticality, assigned roles, missions, and resources.

(2) Providing awareness information and educational materials to help service members, civilian employees, and contractor personnel prepare themselves and their family members to reduce their individual risk and vulnerability to terrorism and criminal activity.

(3) Reporting to the REGCOM in whose area of responsibility (AOR) they are physically located for all matters relating to the Protection Program.

(4) Performing and coordinating all Protection Program requirements within the installation's areas of responsibility.

(5) Establishing a comprehensive installation Protection Program that includes AT, PS, and LE. The program shall be reviewed and updated as required, annually at a minimum.

d. Tenant Commanding Officers and Officers-in-Charge are responsible for:

(1) Coordinating all matters pertaining to the Protection Program with the CO.

(2) Participating as an active member of the installation Protection Program, Crisis Action Team (CAT),
Threat Working Group (TWG), and Antiterrorism Working Group (ATWG).

(3) Complying with reference (a) which prohibits tenant activities residing on a Navy Installation from establishing a separate armed security and/or LE unit without approval from Chief of Naval Operations (N4).

6. Action

a. CNIC shall assist REGCOMs, COs, and supporting security staffs to establish the security posture necessary to defend against acts of terrorism and criminal activity and support all-hazard responses.

b. REGCOMs shall:

   (1) Adhere to requirements set forth in this instruction, and utilize references (a) through (k).

   (2) Require Commanders/Commanding Officers to implement plans, policies, and procedures as a result of lessons learned and best practices, which are incorporated in Navy doctrine publications.

   (3) Ensure Navy installations that are unable to implement this instruction submit requests for waivers and/or exceptions as required.

   (4) Additionally, in cases where the REGCOMs and COs are prohibited from implementing requirements of this instruction, a report shall be submitted via their operational chain of command with an information copy to CNIC.

c. Installation Commanding Officers shall adhere to requirements set forth in this instruction, and utilize references (a) through (k).

7. Forms and Reports

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

b. Forms to be used by Navy security units can be obtained at https://navalforms.daps.dla.mil/web/public/home. Locally generated forms will not be used in lieu of official forms.
c. Records created as a result of this instruction, regardless of media and format, shall be managed IAW reference (k).

M. C. VITALE
Vice Admiral, U.S. Navy

Distribution:
Electronic only, via CNIC Gateway 2.0
https://g2.cnic.navy.mil/CNICHQ/Pages/Default.aspx
CNIC ASHORE PROTECTION
REQUIREMENTS AND STANDARDS
# TABLE OF CONTENTS

## CHAPTER 1 PROTECTION PROGRAM MANAGEMENT
- 0101 Scope .................................................. 1-1
- 0102 Command Structure ...................................... 1-1
- 0103 Echelon II ............................................. 1-1
- 0104 Echelon III ............................................ 1-3
- 0105 Echelon IV ............................................. 1-5
- 0106 Required Operational Capabilities (ROC) ................ 1-7
- 0107 Defense Readiness Reporting System-Navy (DRRS-N) ...... 1-9
- 0108 Navy Mission Essential Tasks (NMET) .................... 1-10
- 0109 Protection Planning Process ............................ 1-10
- 0110 Training and Exercises .................................. 1-11
- 0111 Interoperability ....................................... 1-12

## CHAPTER 2 NAVY SECURITY FORCE COMPOSITION
- 0201 Mission ................................................ 2-1
- 0202 Navy Security Forces ................................... 2-1
- 0203 Responsibilities ....................................... 2-2
- 0204 Post Orders ............................................ 2-3
- 0205 Weapons Security ....................................... 2-3
- 0206 Contract Security Service ................................ 2-4
- 0207 Civil Service Members of the Navy Security Force ....... 2-4
- 0208 Regional Security Force (RSF) ......................... 2-5
- 0209 Auxiliary Security Force (ASF) ......................... 2-7
- 0210 CNIC N3AT Non-Guard Security (NGS) Support Services 2-14
- 0211 Navy Reserve (NR) NSF .................................. 2-15
- 0212 Alcohol and Prescription Drug Use ...................... 2-15

## CHAPTER 3 ANTITERRORISM
- 0301 General ................................................ 3-1
- 0302 Overview .............................................. 3-1
- 0303 Types of Assessments ................................... 3-1
- 0304 Navy Force Pro ......................................... 3-3
- 0305 Risk Management ........................................ 3-3
- 0306 Antiterrorism Planning ................................... 3-4
- 0307 Antiterrorism Officer (ATO) ............................ 3-5
- 0308 Installation AT Plan ................................... 3-6
- 0309 Antiterrorism Working Group (ATWG) .................. 3-6
- 0310 Individual Antiterrorism Plan (IATP) and Travel Tracker/Notifer (TT/N) .................................. 3-7

## CHAPTER 4 PHYSICAL SECURITY
- 0401 Physical Security Programs ............................... 4-1
- 0402 Objective .............................................. 4-1
- 0403 Policy ................................................ 4-2
- 0404 Protection Capabilities .................................. 4-2
0405 Defense in Depth.................................................4-3
0406 Sex Offender Tracking, Assignment, and Installation
   Access Restrictions..............................................4-3
0407 Taxi, Limousine, and Shuttle Access..........................4-3
0408 Installation and Facility Control...............................4-7
0409 Navy Commercial Access Control System.......................4-23
0410 DoD Identification Cards, Badges, and Smart Cards........4-26
0411 DoD Decal Program.............................................4-28
0412 Deviation Process...............................................4-29
0413 Harbor Patrol Unit/Harbor Security Boat......................4-30
0414 Active Vehicle Barrier Procedures.............................4-31
0415 Crime Prevention...............................................4-34

CHAPTER 5    LAW ENFORCEMENT
0501 Responsibilities.................................................5-1
0502 Traffic..........................................................5-5
0503 Driving Under the Influence of Alcohol/Drugs................5-5
0504 Traffic Accident Investigations...............................5-6
0505 Selective Traffic Enforcement Program (STEP).................5-7
0506 Criminal Investigations........................................5-8
0507 Desk Journals.....................................................5-9
0508 Crime Statistics................................................5-9
0509 Personal Firearms Safety, Control, and Accountability....5-10
0510 Courthouse Security.............................................5-11
0511 Cell Phone and Texting.........................................5-11
0512 Pre and Post Shift Activities..................................5-12

CHAPTER 6    TABLE OF ALLOWANCE AND UNIFORM STANDARDS
0601 Purpose..................................................................6-1
0602 Definitions..........................................................6-1
0603 Background..........................................................6-1
0604 Responsibilities....................................................6-2
0605 Procedures for Initiating TOA Changes........................6-3
0606 Uniform and Appearance Standards for DON Civilian
   Police/Security Guards...............................................6-9
0607 Policy..............................................................6-10
0608 Personal Appearance..............................................6-10
0609 Hair, Grooming, and Appearance Standards....................6-10
0610 Hygiene and Tattoos..............................................6-13
0611 Supervisory Responsibility.......................................6-14
0612 Honors....................................................................6-14
0613 Uniform Allowance...................................................6-14
0614 Authorized Uniforms................................................6-16

CHAPTER 7    TRAINING
0701 Background.........................................................7-1
CHAPTER 1
PROTECTION PROGRAM MANAGEMENT

0101. **Scope.** The Navy Region and Installation Protection Program, which primarily focuses on the Force Protection (FP) line of effort, shall establish program management guidelines that clearly delineate operational and administrative command responsibilities in accordance with (IAW) references (a) through (f). The Protection Program resides within the Operations Directorate. Mission Assurance is the preceding concept to the Protection Community diagram in Figure 1.

0102. **Command Structure.** Figure 1-1 shows the operational and administrative chains of command for FP Program management in and out of the continental United States (CONUS, OCONUS).

![Command Structure Diagram]

**Figure 1-1. Command Structure**

0103. **Echelon II**

a. Fleet Commanders. In accordance with (IAW) the Unified Command Plan, Naval Component Commanders (U.S. Pacific Fleet, U.S. Naval Forces Europe, and U.S. Naval Forces Central Command) shall execute tactical control for FP over all Navy activities,
facilities and forces within the Geographic Combatant Commander (GCC) area of responsibility (AOR).

b. Commander, Navy Installations Command (CNIC).

(1) CNIC Operations Officer (N3). The CNIC Operations Officer, as directed by the Commander, is overall responsible for the administration of all CONUS Navy Region and Installation Protection Programs. The CNIC Operations Officer maintains the administration of all OCONUS regional and installation Protection Programs in coordination with Naval Component Commanders (NCC) and numbered Fleet Commanders.

(2) CNIC Force Protection Program Director N3AT. As directed by the CNIC Operations Officer (N3), N3AT is responsible for providing policy, guidance, structure, resourcing and assignment of responsibilities for comprehensive protection capabilities at Navy Regions and Installations. The N3AT shall serve as the Program Coordinator at the CNIC level. Responsibilities shall include but are not limited to the following:

(a) Resourcing and budgeting within FP functional area defined as antiterrorism (AT), physical security (PS), and law enforcement (LE), including the development of applicable Program Objective Memorandum (POM) inputs and the development and distribution of fiscal controls for the Regional FP Program.

(b) Oversight of all protection working groups at the CNIC headquarters level.

(c) Promulgate, distribute, review, and update all CNIC protection program requirements.

(d) Review of the program-related federal, Department of Defense (DoD), Joint, and Navy publications for interpretation and possible inclusion/implementation within the Protection Programs for shore installations.

(e) Participation in Joint Force Protection Programs and working groups to assist in the development of related requirements, procurement strategies, and fielding schedules.

(f) Serve as the principal point of contact (POC) for the regional Protection Programs.
0104. **Echelon III: Regional Headquarters**

**a. CONUS Regions.** Figure 1-1 depicts operational and administrative chains of command for CONUS regions. Commander, United States Fleet Forces (USFF) is a supporting commander to Commander (CDR), United States Northern Command (USNORTHCOM), exercises Tactical Control (TACON) for FP of all ashore and afloat Department of Navy (DoN) personnel, resources, infrastructure, information, and equipment within the USNORTHCOM AOR, and is the Chief of Naval Operations (CNO) Executive Agent (EA) for FP in the USNORTHCOM AOR. CNIC exercises Administrative Control (ADCON) over Region Commanders (REGCOM). REGCOM exercise TACON for FP and ADCON over Installation Commanders (COS).

**b. OCONUS Regions.** Figure 1-1 depicts operational and administrative chain of command for OCONUS regions. Combatant Commanders exercise Operational Control (OPCON) over respective Navy Component/Fleet Commanders. Navy Component Commanders exercise OPCON over REGCOMs. CNIC provides support and coordination to Navy Component/Fleet Commanders and exercises ADCON over REGCOMs. REGCOMs exercise OPCON and ADCON over COS.

**c. Region Commander (REGCOM).** REGCOMs are responsible for the governance of their region and the delivery of base operating support within their assigned operational area (See Figure 1-2). The NCCs exercise OPCON over the REGCOMs within the assigned GCC AORs while CNIC exercises ADCON. The REGCOM is the Immediate Superior in Command (ISIC) for all COs within their region. In NORTHCOM AOR, they are responsible for any Navy facility not physically located on installations. The commander of these Navy activities shall report to the REGCOM in whose AOR the command is physically located for all matters related to Navy AT.

1. All REGCOMs shall designate a Regional Security Officer (RSO) who reports to the Regional Operations Officer (N3). The Regional Protection Program shall function as an element of the Regional Operations Program.

2. The REGCOM shall evaluate the Protection Program of subordinate installations, ensure compliance with this instruction and higher headquarters instructions, and ensure that COs conduct self-assessments annually. The REGCOM is responsible for ensuring that the regional Navy Security Forces (NSFs) are manned, trained, and equipped to ensure continuity of purpose in providing effective defense of installations and
associated AORs. Required Operational Capabilities (ROC) and Common Output Levels (COL) will be used as a basis for this manning, training and equipping. This responsibility involves program direction and oversight of the regional and installation Protection Programs and compliance with this document.

(3) All Navy commands, activities, and other units not physically located on a Navy installation shall report to the Navy REGCOM in whose region they are physically located for all operational matters related to Navy FP. These installations and activities include Navy organizations that may not be in the chain of command of the applicable Navy REGCOM such as:

- Navy units operating off-installation
- Pre-commissioning units until special commissioning
- Recruiting offices
- Navy shipyards
- Laboratories, warfare centers and other activities of the Navy research enterprise
- Reserve activities
- Navy medical treatment facilities
- Communication locations
- Security groups
- Civil works activities
- Outlying educational institutions
- Housing, NEX/commissary activities, MWR, and family support sites outside Navy controlled security perimeters

Figure 1-2. CNIC Regions and Installations
d. Regional Operations Officer (N3). Reports directly to the REGCOM and provides supervision and oversight of the Regional Protection Program and the assigned RSO.

e. Regional Security Officer (RSO) / Force Protection Program Director (N3AT). The RSO serves as commander's representative on all regional Protection Programs on behalf of the Regional Operations Officer, and provides day-to-day leadership and management of regional Protection Programs.

f. Regional Protection Program Management and Organization. Each Region is unique in terms of operational requirements, AOR, scope, manpower, resources, and priority. Installations which are geographically separated shall ensure that they have successfully identified and integrated all protection plan procedures issued in regional policy.

g. Regional Antiterrorism Officer (ATO). Per reference (b), REGCOM shall ensure that an ATO responsible to the REGCOM for AT requirements is assigned in writing. The ATO is the primary advisor to the REGCOM on all AT matters reporting via the RSO and Regional Operations Officer as depicted in Figure 1-3.

h. Organizational Construct. Figure 1-3 depicts the recommended organizational construct for the Regional Protection Program.

0105. Echelon IV: Installation Headquarters

a. CO. The CO reports to the REGCOM in the respective AOR, for all Protection Programs. The REGCOM is the ISIC of the CO. The CO shall conduct the following:

(1) Implement protection policies and procedures contained in references (a) through (f) and (i)

(2) Report to the REGCOM in whose AOR the installation is physically located for all operational and administrative matters relating to Navy Protection Programs.

(3) Ensure effective unity of command over all armed security forces aboard the installation during response to a high threat incident. Ensure no more than one armed security/LE force exists aboard the installation without approval of CNO N4 IAW reference (a) or the exception for Strategic Weapons Facility, Atlantic (SWFLANT) and Pacific (SWFPAC).
(4) Be responsible for installation perimeter and area security, including coordination with tenant activities.

(5) Establish and publish a Protection Program, including AT, PS and LE SOP’s. The installation and tenant command AT Plans must be coordinated to ensure compatibility. A copy of tenant command AT Plans should be on file at the installation level and mentioned as such in the installation AT Plan.

(6) IAW reference (a) designates an ISO in writing.

(7) IAW references (b) and (d) designates an ATO in writing.

(8) Publish a consolidated list of all restricted areas aboard the installation, including those of tenant commands. This list will be provided to CNIC via the REGCOM, April of each year. The list will specify whether those areas containing assets vital to national security, are inherently dangerous, contain critical infrastructure or mission essential vulnerable assets (MEVA) IAW with reference (a).

(9) Ensure that protection training is conducted for all NSF per applicable directives, instructions, and regulations.

(10) Provide NSF with mission objectives based on higher headquarter requirements and Navy Mission Essential Tasks (NMETs).

(11) Ensure that each geographically separated facility has successfully identified and integrated all local procedures, including all-hazards response, contact information, mutual aid information, and other local requirements/needs into the installation AT and associated Protection Plans.

b. Tenant Commanding Officers/Officers in Charge (OICs) are responsible for ensuring adequate physical security measures are in place at their activities and for providing sufficient resources to implement, manage, and execute an effective Protection Program. To ensure continuity of effort, training in security related functions should be coordinated with the host command. Tenant Commanding Officers/OICs shall coordinate with COs for any armed security requirements and make all arrangements a matter of formal documentation.
c. Installation Security Officer (ISO). The ISO reports operationally to the CO and administratively to the RSO. The ISO shall serve as the CO’s representative on all installation Protection Programs. The ISO shall be responsible for providing day-to-day leadership and management of installation PS and LE Programs. The ISO shall ensure that those programs complement the overall regional protection efforts.

d. Installation ATO. The ATO is responsible for all AT requirements and is the primary advisor on AT matters to the CO. The ATO shall report operationally to the CO. The Regional ATO shall support the installation ATO administratively as depicted in Figure 1-3.

![Figure 1-3. Notional Regional Protection Program Organization](image)

0106. Required Operational Capabilities (ROC)

a. Per reference (c), ROC level classifications are categorized as levels 1 thru 5. Tier classification is based on the criticality of assets assigned and functions performed and supported. The tiered implementation approach is necessary to prioritize resource allocation and provide a risk-based approach to investing in installation protection. IAW reference (c), recommendations for changes to current ROC levels can be made by the installation, region or Fleet Commander by utilizing the
format in enclosure (1) of reference (c). Requests fall into two categories; Routine and Emergent.

(1) Routine requests should be submitted on an annual basis and shall be submitted by the CO via the REGCOM, Budget Submitting Offices (BSO) and fleet commander to the Office of the Chief of Naval Operations (OPNAV) N3AT annually by 15 April.

(2) Emergent request examples include installation mission changes and movement of critical assets. An increase in ROC classification may incur a resourcing requirement that cannot be immediately met so it is imperative that CNIC, REGCOMs and COs participate in the planning and programming process. Nothing contained herein precludes REGCOMs from adjusting resources or forces within their AOR to respond to emergent ROC designation changes.

b. The Navy must size and locate its ashore infrastructure IAW reference (j) to ensure CNIC’s vision for the future:

(1) Helps keep the multiple and disparate infrastructure plans unified and aligned with higher order guidance.

(2) Support the Navy’s strategic aims.

(3) To help deliver to the Navy Enterprise the Right Capabilities, at the Right Time, in the Right Places for the Right Price.

c. CNIC shall:

(1) Participate in annual review and approval of ROC list with OPNAV N3/N5 and other Echelon II commands.

(2) Execute AT resourcing controls as provided by OPNAV.

(3) Implement and resource approved ROC level assignments.

(4) Review system command (SYSCOM) capability development to verify that AT and Emergency Management (EM) system solutions currently in development meet AT and EM program priorities as defined by the fleet ROC framework.

(5) Coordinate with fleets to determine foundational capability levels of protection afforded all Base Operating Support (BOS), AT and EM capabilities.
(6) Allocate ashore resources according to standards and conditions of operational tasks associated with ROC levels.

d. REGCOMs shall:

(1) Ensure ROC policies and standards established are integrated into all appropriate regional policy guidance.

(2) Conduct an annual review of each installation within their region and provide recommendations for modifications of ROC levels to their Operational Commander.

(3) Submit all requests for changes to the approved ROC levels annually to the fleet commander for review no later than 15 March IAW reference (c).

(4) Submit all requests for emergent changes to the approved ROC levels to the appropriate fleet commanders for review IAW reference (c).

e. COs shall:

(1) Submit annual recommendations for ROC level modification to the REGCOM by 15 February IAW reference (c).

(2) Submit a change request to the REGCOM IAW reference (c) if a situation emerges during the year that warrants a change to an installation’s ROC level assignment.

0107. Defense Readiness Reporting System-Navy (DRRS-N)

a. CNIC has established reporting criteria and the process of developing resource data to assist COs in making informed assessments. In support of CNIC efforts to enhance linkage between shore readiness and Fleet readiness, installations shall report readiness in DRRS-N. As such, each CO shall report readiness using DRRS-N.

b. Resource data is defined as data regarding personnel, equipment, supplies, training, ordnance, and facilities (PESTOF). DRRS-N will compute a Red, Yellow, or Green readiness assessment for each NMET and capability that will assist the CO when developing Commander's Assessments. NMETs can be found on the CNIC Gateway website.
c. These efforts support the CNIC Strategic Plan and directly impact CNIC’s mission as a supporting command to the war fighter to enable and sustain Fleet, Fighter and Family readiness.

0108. **Navy Mission Essential Tasks.** NMETs are tasks developed IAW reference (k), which reflects a command's mission capability requirements and provides the basis for deriving the command's warfare training requirements. To accommodate the constraints on training resources, commanders must identify the tasks most essential to their assigned or anticipated missions, with priority given to their wartime missions. These essential tasks are referred to as mission-essential tasks. REGCOMs and COs shall comply with these efforts to support the CNIC Strategic Plan. These efforts have a direct impact on CNIC's mission as a supporting command to the war fighter to enable and sustain Fleet, Fighter, and Family readiness.

0109. **Protection Planning Process**

a. The CNIC Ashore Protection Program establishes planning standards and procedures which set policy for all regions and installations. Subsequent chapters contained herein provide specific planning elements of a Protection Program.

b. The FP process considers assessment of the threats, management of the risk, and prioritization of actions, monitoring the situation, and maintaining flexibility. Figure 1-4 indicates how FP is integrated into the Joint Planning Process.
0110. Training and Exercises

a. All installations must conduct a series of AT exercises in addition to an annual installation wide AT exercise to validate their AT Plans with a detailed record to be maintained of lessons learned. IAW reference (d), maintain AT exercise documentation for no less than 2 years to ensure lessons learned are incorporated. Based on installation ROC Level, COs may be required to exercise portions of the AT Plan throughout the year to increase efficiency and responsiveness. Exercises should involve all installation support organizations as applicable.

b. All personnel assigned to CNIC shore activities will receive annual and documented all-hazards awareness training, including chemical, biological, radiological, nuclear and high-yield explosives (CBRNE). Training can be completed on Navy Knowledge Online (NKO) and Total Workforce Management System (TWMS), which can be tracked by Navy Training Master Planning
0111. **Interoperability.** The ability of systems, units, or forces to provide and accept services from other systems, units, or forces and to use the services to enable them to operate effectively together IAW reference (1).

a. CNIC will ensure that equipment, training, professional certifications, and exercises acquired through the joint program supports interoperability by adhering to appropriate civilian standards whenever possible.

b. ISOs shall ensure that tactics, techniques, and procedures (TTP), equipment, training, personnel proficiency certifications and exercises promote interoperability with respective mutual aid partners to the maximum extent possible.

c. Physical security of separate activities and installations will be coordinated with other military activities/installations in the immediate geographic region or area and with local civilian LE agencies or host-government representatives. Opportunities to "partner" or share special capabilities among regional users will be fully explored and documented to ensure economy of effort. Specifically, installations should develop Memorandums of Understanding (MOUs)/Memorandums of Agreement (MOAs) for a capability the Navy does not possess.
CHAPTER 2
NAVY SECURITY FORCE COMPOSITION

0201. Mission. Navy Security Forces are designated personnel specifically organized, trained, and equipped to provide FP, which includes AT, PS, and LE, under the authority of the REGCOM and CO. The mission is limited by both jurisdiction and authority to the protection of Navy shore installations and forces. NSF jurisdiction and authority are strictly limited to the installation and other noncontiguous sites under the jurisdiction of the REGCOM and CO. Due to host nation sovereignty, OCONUS NSF have no jurisdiction off the installation and in some cases do not have jurisdiction on the installation.

0202. Navy Security Forces. The NSF at shore activities consist of military and civilian personnel performing LE or security functions for the ISO who reports to the CO and coordinates with the RSO.

   a. The NSF includes Master-at-Arms (MA), DoN Police Officers (GS-0083), DoN Security Guards (GS-0085), Contractors (KTR), Security Specialists (GS-0080), and Security Clerical and Assistance Series (GS-0086). Contracted security personnel are not authorized to perform LE duties that are normally assigned to military or civilian inherently government positions. Today's installation security force represents a diverse composition of professionals requiring a wide knowledge of management responsibilities not only in the area of protection, but also in the oversight of personnel with varying conditions of employment.

   b. In accordance with reference (a), all NSF at installations shall be integrated into a single force structure. Tenant activities are not authorized to establish a separate armed security and LE force without approval from OPNAV N46P and in consultation with the CO.

   c. The NSF shall be assigned to provide AT, LE and PS duties IAW references (a), (m) and (n). The Mission Profile Validation-Protection (MPV-P) process clearly delineates the validated positions identified for NSF and due to ongoing manning issues, other duties are prohibited, (e.g., Quarterdeck Watches, CDO, OOD, Colors, Urinalysis Collecting, CMAA, Harbor Security Boat (HSB) maintenance [other than pre-operational maintenance], Barrier Operations, etc.) NSF duties shall be determined and assigned by the RSO/ISO as appropriate.
d. Supporting the decision to limit NSF duties to armed security related functions is the factor that off-shift personnel are subject to instant recall and must be "fresh" to support any threat to security and any increase of Force Protection Conditions (FPCONs).

0203. Responsibilities. The CO has the inherent responsibility for the overall security of their installation utilizing multiple factors to include risk-based analysis. ISOs are required to keep the CO informed and up to date on all security matters and provide a detailed report on the status of the protection program at regular intervals. The CO is responsible for the day to day operations of the Security Detachment and the ISO; administrative and resource management control resides with the REGCOM through the RSO. In coordination with the REGCOM, COs and ISOs are to develop support agreements with local, state, and federal entities as they relate to the security of the installation. In overseas locations, some activities are protected by foreign nationals. In such cases, rules and policies in accordance with the Status of Forces Agreement (SOFA) must be adhered to and strictly followed for compliance.

a. RSO. The RSO is a military officer usually with the designator 649X/749X or a civilian employee and reports directly to Regional Operations Officer (N3). Duties include but are not limited to the following:

(1) Provide or coordinate protection services to the regions, installations, and tenant commands, military and civilian employees, family members, and members of the general public located on and/or conducting business in government owned and leased buildings within the region’s area of responsibility.

(2) Develop force protection policies, procedures, plans, goals, and objectives for the region. Coordinate with other military and civilian managers to establish mission requirements and objectives, plan for their accomplishment, review their status and progress, and provide input to the Operations Officer on all policy matters. Prepare budget submissions and track and report on performance metrics.

(3) Serve as the responsible spokesperson and coordinator between the various regional echelons, other commands, and agencies on project agreements, MOUs/MDAs, and similar agreements within the regional protection program.
(4) Reports to the Operations Officer on protection preparedness.

(5) Support the region's readiness posture by developing and periodically updating emergency mobilization plans for the assigned AOR. Analyze possible mission requirements and prepare for execution through training, planning, and commitment of resources for optimum availability to support the region's mission. Responsible for oversight of the regional security training program and manage, train and equip NSF personnel.

(6) Monitor regional activity, and advise the REGCOM, via the Operations Officer, on all security-related matters and conditions.

(7) Provides oversight and management of the regional security force.

b. ISO. The ISO is a military officer in the designator 649X/749X or a civilian employee of an appropriate grade and experience and reports to the RSO for administrative control (ADCON), oversight, and resource issues. The ISO reports to the CO for OPCON on matters involving the security of the installation or activity. Duties include but are not limited to the following:

(1) Supervises and directs Navy Security force assets to ensure the protection of the installation and assist with maintaining good order and discipline.

(2) Plan, manage, implement, and direct the installation protection programs.

0204. Post Orders. The ISO has the responsibility to establish and publish post orders which pertain to each fixed and mobile post IAW reference (a). The ISO is responsible for drafting, implementing, and maintaining all post orders at their installations. A sample post order is depicted in reference (m). Post orders shall be reviewed by and coordinated with the RSO, to ensure alignment with regional procedures, prior to approval by the CO. These orders are the written and approved authority of the CO for members of the NSF to execute and enforce regulations. All post orders shall be reviewed at least annually.

0205. Weapons Security. The authority to arm the NSF at CNIC shore installations is vested in the CO per reference (o), and
in overseas locations as governed by SOFA or local agreements. NSF regularly engaged in LE or security duties shall be armed and qualified per reference (o). In the case of contract security personnel, the contractor must certify in writing that all contract personnel assigned to NSF are qualified according to Navy standards per reference (o) and have successfully completed training in the use of force. Additionally, the contractor must comply with provisions prescribed by the state in which the contract is administered, including current licensing and permit requirements.

0206. Contract Security Service. This provision applies to the procurement of existing or new contractor guard service requirements (as permitted by existing law) within the Navy.

a. Contractor personnel shall not be assigned to perform LE duties.

b. All contract guard services shall be obtained through Commander Navy Facilities Engineering Command (NAVFAC).

c. The current edition of the joint CNIC and NAVFAC Security Operations Notice to All is performance-based and supports the new performance assessment model for oversight of contractor performance. This template will be used in the development of all guard services contracts.

d. Site adaptation of the template to local needs is permissible. However, the template is intended to standardize contract format, terminology, performance metrics, uniforms, guard qualifications, training, etc. Therefore, changes to the template must be submitted to CNIC N3AT for prior approval using the NAVFAC waiver form and procedures. CNIC will then forward the approved changes to NAVFAC for waiver approval.

e. Contract guard personnel performing guard services onboard a CONUS Navy installation or activity shall have a completed favorable National Agency Check with Local Agency and Credit Check (NACLC) prior to assignment.

0207. Civil Service Members of the Navy Security Force. In general, NSF personnel should be physically agile, mentally alert and possess good judgment. Navy Civilian Police (083)/Security Guard (085) (NCP/SG) personnel shall meet all of the Civil Service qualifications for NSF personnel as specified in Civil Service qualification standards. Positions will be classified based on duties actually performed. These personnel
shall be designated as key and essential in times of emergencies IAW reference (p).

a. As a component of the NSF, all NCP/SG personnel are responsible to the CO and are subordinate to the RSO/ISO as appropriate. An internal administrative Chain of Command, to facilitate management of the civilian component, shall be structured in the following manner.

(1) Senior Navy Civilian Police Officer
(2) Civilian Police Operations Officer
(3) Watch Commander
(4) Shift Supervisor
(5) Shift Sergeant
(6) Police Officer

The civilian chain of command is strictly for administrative purposes (promotion, civil service administrative functions, etc).

b. These designations are not to be confused with the operational responsibilities assigned to both military and civilian personnel of the NSF. The ISO is responsible for establishing an operational chain of command that fully integrates both military and civilian NSF into a cohesive efficient organization. Positional authority allows civilian NSF to supervise military NSF and conversely, military NSF to supervise civilian NSF. Regardless of rank, positional authority as assigned by the ISO, will apply.

0208. **Regional Security Force (RSF).** Applicable only to CONUS regions and installations, the RSF is a task organized unit comprised of active duty MA personnel from all installations within a region. The RSF is organized into a deployable unit for activation during such incidents as terrorist attack, natural disaster or significant man-made disasters. RSF operations are designed to provide inside the fence-line support to Navy regions and installations. Augmentation in support of off-installation, USNORTHCOM-directed Defense Support to Civil Authority (DSCA) operations is beyond the scope and purpose of the RSF. This unit provides REGCOMs with an additional level of defensive capability to reinforce and
maintain an appropriate FPCON and PS posture during or immediately following an event.

a. CNIC is in a supporting role to USFF and REGCOMs as required.

b. CONUS Region Commanders shall conduct planning to support RSF contingency operations as both supporting and supported commander and shall:

   (1) (FOUO) Establish the RSF consisting of pre-identified individual MA personnel as follows:

      (a) CNRMA, CNRSE, CNRSW: 2 X 50 person RSF
      (b) CNRNW: 1 X 50 person RSF
      (c) CNRMW and NDW: None

   (2) Train, equip and when directed by USFF, deploy the RSF.

   (3) Develop a regional RSF instruction to include, but not limited to; number of RSF personnel, rosters, equipment and supplies required to deploy, identify sources/avenues for expeditious purchase of equipment/supplies, any additional logistical requirements to support a request for deployment and funding procedures.

c. COs shall ensure a protection plan exists which provides adequate security posture for the installation in the event a portion of its NSF is deployed with the RSF.

d. Training. Personnel assigned to an RSF shall be qualified for, and expected to perform typical Navy installation MA duties. Support personnel requirements exceeding this description shall be resourced separately and not be counted as personnel assigned to an RSF. Capabilities and training requirements for personnel assigned to an RSF do not exceed capabilities and training standards for MAs routinely assigned to installation NSF.

e. Funding. RSF funding shall initially be provided by the supporting region. All associated costs shall be captured and forwarded to CNIC Headquarters.

f. Additional guidance for Navy RSF contingency operations can be found in reference (q).
0209. **Auxiliary Security Force**

a. Per reference (a), the Auxiliary Security Force (ASF) is used to augment an installation's NSF during increased FPCONs or when directed by the CO and ISO of the installation to which assigned. ASF are prohibited from performing LE functions due to ASF training level which does not include all required LE subjects for certification. Navy installations with a non-deployable military population will establish an ASF. If installations have only deployable assets or no active duty personnel, alternative means such as entering into an ISSA/MOU/MOA with a sister service, host nation or local authorities to provide support to meet FPCON Charlie requirements. If the actions identified above do not provide adequate resources to meet FPCON Charlie measures, CNIC shall be notified immediately through established reporting channels. CNIC will evaluate and identify alternative solutions.

(1) The ASF should be sized to permit full manning of posts required in FPCONs CHARLIE, and DELTA or as directed by the REGCOM or higher authority. COs are authorized to activate and employ their ASF as necessary to meet mission requirements at those locations where manpower constraints preclude reaching FPCON CHARLIE, OR DELTA standards. On DoD Joint Base Installations, where Navy is the Supporting Command (Lead Component), MOU/MOAs will be established to source ASF personnel from all Service Supported and Tenant commands to meet protection requirements.

(2) The size of the ASF depends on size and complexity of operations, critical assets, tenant population, and the number of personnel required to man additional security posts to protect mission-essential assets during increased FPCON levels. The ASF should be sized to permit full manning of posts required in FPCONs CHARLIE and DELTA for a minimum of 30 days. At those locations where manpower constraints preclude reaching FPCON CHARLIE or DELTA standards with ASF, COs will immediately report shortfalls to respective REGCOMs.

b. Responsibilities.

(1) REGCOMs shall:

(a) Mandate establishment of installation-level ASF units and ensure sufficient resourcing to ISOs for the purpose of training and outfitting assigned personnel.
(b) Establish and fund a Table of Allowances (TOA) in support of installation ASF units. Allowances should consider the turnover rate of personnel and service life of equipment and uniforms.

(c) Review on a semiannual basis ASF manning, use of ASF outside the scope of paragraph 0209 a.(1) of this instruction, and compliance of tenant commands in providing personnel to ASF, including participation in formal training curricula. ASF status shall be reported in the appropriate pillar in DRRS-N and to operational commanders.

(d) Identify ASF manpower resources for installations with insufficient military populations to support ASF by using other regional installations' manpower. In regions where contract guards are used, Indefinite Delivery/Indefinite Quantity (IDIQ) may be considered. This applies to Pre 911 designated contract guards. If unable to meet ASF requirements using these resources, CNIC shall be notified.

(2) Through their designated representatives, RSOs will ensure installation compliance with this instruction and review ASF semiannual reporting.

(3) COs shall:

(a) Establish and direct all non-deployable Navy tenant commands and non-Navy units with military personnel assigned to provide personnel, to serve on the ASF using the fair share quota methodology:

**Fair Share Quota Methodology**

Using the MPV-P process and the approved Installation AT Plan, determine the number of personnel required to man all posts under FPCONs CHARLIE/DELTA (Example=180). Determine the current/validated NSF staffing for appropriate FPCON (BRAVO for most installations), (Example=144). The difference (36) is the ASF requirement.

Determine the number of ASF-eligible personnel assigned to the installation (Example=142). Divide the ASF requirement (36) by the ASF-eligible personnel (142) to determine the fair share ratio (0.253). Apply the ratio (multiply) to each department/tenant with ASF-eligible personnel to determine their fair share (round up over .50).
<table>
<thead>
<tr>
<th>Department or tenant command</th>
<th>ASF-eligible assigned</th>
<th>Ratio</th>
<th>Fair share to provide to ASF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Ops</td>
<td>40</td>
<td>0.253</td>
<td>10</td>
</tr>
<tr>
<td>AIMD</td>
<td>26</td>
<td>0.253</td>
<td>7</td>
</tr>
<tr>
<td>USAF Ops</td>
<td>25</td>
<td>0.253</td>
<td>6</td>
</tr>
<tr>
<td>Supply</td>
<td>12</td>
<td>0.253</td>
<td>3</td>
</tr>
<tr>
<td>PSD</td>
<td>20</td>
<td>0.253</td>
<td>5</td>
</tr>
<tr>
<td>NAVSEA</td>
<td>19</td>
<td>0.253</td>
<td>5</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>142</strong></td>
<td></td>
<td><strong>36</strong></td>
</tr>
</tbody>
</table>

Commands having five or fewer personnel assigned to the command or other manning limitations where providing fair share for ASF duties would result in absolute mission failure may request a waiver from the REGCOM. The request must be made in writing, cite supportable justification, and be endorsed by the first flag officer in the tenant's chain of command.

(b) Establish schedules and procedures for the recurring review of the installation's non-deployable military population and updating of ASF quotas. COs shall use current manning documents to validate tenant command population baselines. COs shall review ASF manning on a quarterly basis.

(c) Outline situations in which ASF activation is expected, including, but not limited to, elevated FPCONs; establish perimeters during bomb threats or hostage situations; provide crowd control during civil disturbances which effect the security of the installation and public events; provide anti-looting and general security in post-disaster situations such as destructive weather, major fires, or explosions; and augment installation NSF as determined by the CO or REGCOM during periods of RSF deployment.

(d) Establish procedures for nominee screening and assignment.

(e) Establish requirements and procedures for the management of the ASF inventory, including personnel availability, return-to-command, replacement, permanent change of station transfer, and leave/temporary assigned duty (TAD).

(f) Direct the establishment and outline the authorities of ASF operational and administrative chains of command, including disciplinary action and parent command/activity notification of performance. Ensure commanding officers/OICs of personnel who fail to report for training and/or duty are officially notified in writing, and inform the
tenant command's immediate superior in charge, CNIC (N3AT), and the REGCOM.

(g) Establish procedures for training ASF, to include initial, proficiency, and recurring training, and identification of special qualifications.

(h) Set the requirement for equipping and outfitting of ASF personnel and procedures for determination, acquisition, and inventory of ASF equipment.

(4) Commanding officers/OICs of tenant commands/activities and host installation department heads with non-deployable military personnel shall support and participate in the host installation's ASF program as described in this section.

(5) ISOs shall:

(a) Via the CO, command the assigned ASF and be responsible for individual training, watch standing, exercises, and outfitting at the activity level.

(b) Report to the CO in the deployment of all ASF and provide program oversight and accept/reject nominees as recommended by the ASF Coordinator.

(c) Annually review posts which ASF may augment and make recommendations to the CO as needed to establish or delete posts based on threat, vulnerability, and criticality.

(d) Ensure all posts, and the number of personnel required to man those posts during increased FPCONs, are designated in the installation AT Plan.

(e) Coordinate training of ASF.

(f) Provide a monthly report to the CO noting all personnel not reporting for duty as required or any tenant or department head refusing to provide support as required.

(6) The ASF Coordinator (an E7 or above) shall be assigned on a collateral duty basis within the installation security detachments. ASF Coordinators shall:

(a) Maintain coordination with department/tenant coordinators/POCs.
(b) Establish a phone tree for recall through department and tenant representatives.

(c) Screen individuals to ensure qualifications.

(d) Recommend to the ISO acceptance/rejection of nominees based strictly on failure of a nominee's ability to meet established standards.

(e) Ensure ASF personnel successfully complete training per subparagraph e. of this section.

(f) Issue all necessary gear and clothing for ASF duties.

(g) Ensure all gear is returned prior to member’s departure.

(h) Establish a monthly watch bill using all ASF members.

(i) Ensure each member participates annually in a major exercise.

(j) Return personnel to their respective commands that do not meet initial assignment qualifications and require the tenant/department to supply an immediate qualified relief.

(k) Delegate supervisory authority commensurate with rank and expertise within the ASF organization, while establishing an in-house chain of command.

(l) Monitor performance of posted ASF personnel, via the NSF Operations Officer, to ensure adequacy of proficiency training.

(m) Regularly inform the ISO of the status of ASF, including tenant and departmental support, numbers required/assigned, training, and exercises planned.

(n) Monitor through contact with tenant command and departmental representatives, as well as through leave/TAD requests to ascertain the number of available resources at a minimum of once a month.
(o) Maintain an inventory control system to monitor necessary gear/equipment issuance and accountability.

(p) Notify the ISO of any command not providing ASF support when tasked to do so or of any individual failing to report as required.

c. Composition. The ASF shall be primarily composed of permanently assigned, non-deployable military personnel from host installation departments and Navy and non-Navy tenant commands. The ASF shall be primarily composed of E6 and below personnel. This provision does not preclude the assignment of other qualified military personnel, including senior enlisted, officers, and volunteers, when authorized by the individual’s chain of command and approved by the ISO. Composition may also include personnel as described in paragraph 0209 b.(1)(d) of this instruction. It is recommended that the ASF be organized into two watches to coincide with "port and starboard" operational tempo during increased FPCONs. This composition shall include supervisory personnel as well as individual post standers.

d. Nomination. Tenant command commanding officers/OICs and installation department heads shall nominate individuals to serve on the installation's ASF. Those nominated shall have no convictions for domestic violence as delineated in the Lautenberg Domestic Violence Amendment to the Gun Control Act of 1968 (reference (r)). They must possess sound judgment, have no drug or alcohol dependencies, and have received no non-judicial punishment or civil or court-martial convictions in the previous two years.

(1) Nominating authorities should be cognizant of the individual's personal conduct and state of mind so as not to nominate an individual facing depression or other psychological issues that may lead to unintended consequences. Prior to assignment to the ASF, individuals will be interviewed by the ISO or ASF Coordinator to determine their competence and demeanor to carry a firearm and comply with the intent of reference (i). Those individuals whose demeanor is in question shall be rejected. The ISO will make a recommendation to the CO for acceptance/rejection of a candidate.

(2) All personnel are required to meet DoD/Navy standards for height, weight, and body fat and must have passed the most recent physical readiness test in accordance with references (t) and (u) or other service requirements.
(3) Nominees to the ASF must be available for a minimum of 18 months of performance, not be currently scheduled for an Individual Augmentee or General Service Administrator assignment, and not have any training for more than one month in duration during any six-month assignment to ASF.

e. Training. The minimum training requirements for all personnel assigned to ASF duties are completion of Armed Sentry Training, either via completion of AS/ SRF-B (A-830-0018) or completion of both NSF Sentry (A-830-2216) and Security Reaction Force Team Member-Basic (A-830-2217) courses. See paragraph 0705 of this instruction for additional information.

f. Recall. Only an CO or REGCOM may recall ASF personnel. For the purpose of this instruction, recalling individuals for monthly watch standing does not apply. An entire ASF unit may be recalled, or specific members may be recalled at the discretion of the recall authority. During the period of recall for FPCON increases, exercises, and/or special events, all ASF members are under the command of the ISO and will not be released without prior authorization of the CO.

g. Deployment. For training and qualification sustainment purposes, each member of the ASF will be required to perform two full-shift sustainment watches and one full-shift training day for a minimum 24 hours monthly. Posting and training assignments will be made with the intent of qualifying and familiarizing individuals with the posts and duties they are expected to stand and perform when actually recalled. Annual participation in a major exercise is a requirement and a part of the member’s ongoing training and qualification program.

h. Arming. ASF personnel performing security duties shall be armed IAW reference (o). Type of arms issued to the member shall depend on the arms designated as appropriate based upon Security Force Orders. The ISO shall ensure that, prior to being issued a weapon, personnel have been properly trained and are qualified IAW reference (o).

i. Assignment. To ensure all members assigned to the ASF reach their full potential, they will be assigned for a minimum of 18 months. This period will ensure members receive initial training, stand sufficient monthly watches to gain familiarization and proficiency with each post, and participate in an annual exercise to allow them to be used and evaluated based on real-world events. Consideration should be given to
longer assignments whenever possible to retain experienced personnel, limit repetitive training, reduce costs associated with training and firearms qualification/ammunition, and limit the amount of clothing/gear issuance and reissuance. In unique situations which may preclude an 18-month assignment, COs will submit a written waiver request to the REGCOM. Waiver requests shall include specific and supported justification for special consideration and recommended assignment term. At locations with tour lengths less than 18 months, waiver requests are not required; however, COs shall strive to maximize the time members are assigned to ASF.

j. Reporting. All regions will report to CNIC (N3AT) FP Program Director, on a monthly basis, the number of personnel required to man all ASF posts, the number of personnel assigned to ASF, and the number of personnel anticipated to be unavailable for the upcoming month due to leave, TAD, or other reasons negatively impacting operational readiness. The report will also address the assignment of personnel to any task not validated in the AT Plan as an authorized ASF post.

k. Each department/tenant providing ASF personnel should assign a senior person as the POC for ASF matters to coordinate with the installation ASF coordinator. That person will ensure those assigned from their respective units meet all qualifications for assignment. They will inform the installation ASF coordinator of any changes in a member’s status that would preclude them from assignment to ASF such as suicidal tendencies, drug charges/use or a medical condition as an example. The department/tenant command must immediately provide a qualified alternate ASF member.

0210. **CNIC N3AT Non-Guard Security (NGS) Support Services.**

CNIC N3AT NGS Support Services is the Government's Agency Tender Most Efficient Organization (MEO) developed under OMB Circular A-76. NGS services are performed by both government civilian employees and contractor personnel reporting to the Region/Installation organization to which assigned providing clear, unambiguous unity of command. NGS services consist of Commercial and Mobile Vehicle Inspection services, Explosive Detection Dog (EDD) services, Pass and ID services, Armory and Ready for Issue services, Training, Physical Security Program support, Firearms Range support in some locations, Supply Logistics and Administrative Support services.

0211. **Navy Reserve (NR) NSF.** In accordance with reference (a) NR NSF units are established at each installation with the
intent to meet additional NSF manning requirements resulting from prolonged increased FPCONs. The NR NSF unit CO/OIC shall be the primary point of contact for the CO.

a. Region Commanders have the authority to reassign NR NSF personnel within the region as needed.

b. The NR NSF unit shall be integrated into the installation's security detachment 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 shall ensure travel and per diem funding is available to support on-site drill periods.

c. The CO of the supported installation is responsible for training, equipping, outfitting, and documenting the qualifications of the assigned NR NSF personnel.

d. The installation AT plan shall identify how the NR NSF shall be manned, trained, equipped and most importantly, utilized to meet increased FPCON.

0212. Alcohol and Prescription Drug Use. In carrying out the COs responsibility to maintain good order and discipline, along with protection of personnel and assets aboard a Navy installation, NSF personnel shall adhere to the following prohibitions with regard to alcohol and prescription drug use.

a. All NSF personnel shall not consume any alcoholic beverages within eight (8) hours prior to the commencement of their assigned shift. In the event of emergency recall or being called due to shift shortages and this 8 hour minimum has been breached, the NSF member shall advise the supervisory staff of this and a determination will be made on a case by case basis by the RSO or ISO as appropriate.

b. NSF personnel taking prescription drugs, or an over the counter drug, which may adversely affect the performance of his/her duties, shall advise the supervisory staff of this and a determination shall be made on a case by case basis by the RSO or ISO as appropriate.
CHAPTER 3
ANTITERRORISM

0301. General. The Regional ATO shall develop an AT Plan which will be signed by the REGCOM. ISOs and ATOs shall develop an AT Plan based on guidance provided to them by all higher-echelon commanders and signed by the CO.

0302. Overview. A comprehensive Antiterrorism Program will encompass a systematic and effective approach to providing defensive measures to reduce vulnerability to terrorist attacks. This includes ensuring AT Programs address risk management, training, exercises and readiness. AT Plans are integral parts of a complete AT Program. All regions and installations shall use approved AT Plan templates in accordance with reference (v). AT Programs will be assessed in accordance with appropriate references.

0303. Types of Assessments

a. Critical Infrastructure Assessment: IAW reference (d) critical infrastructure assessments identify regional and installation critical assets/infrastructure and personnel necessary to carry on mission-essential functions. Critical Infrastructure Assessments are required by each installation and will require participation by the installation N3, N4, N6 and tenant commands at a minimum. The physical security division of the installation security department will support the Critical Infrastructure Assessment and provide necessary physical security surveys.

b. Threat Assessment: Determination of specific terrorist or criminal threats to a region, installation, or geographic area, and shall be conducted at a minimum annually. IAW reference (b) NCIS shall conduct these assessments. In addition to the Threat Assessment conducted by NCIS, installations are required to develop a list of most likely/dangerous threats from which they extrapolate a Design Basis Threat (DBT), which their AT plan and resourcing strategy is based. This list shall identify those threats that will not be defended against and the rationale for this decision (risk management). Specific terrorist threat information may be classified in nature. If so this information will be handled in accordance with Navy classified material requirements.

c. Vulnerability Assessments (VA): Per reference (d), an assessment to determine the vulnerability to a terrorist attack
against an installation, unit, exercise, port, ship, residence, facility, or other site. It identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism.

d. IAW reference (d), Joint Staff Integrated Vulnerability Assessments (JSIVA) shall be classified according to the Defense Threat Reduction Agency (DTRA) classification guide. DTRA Vulnerability Assessment Guidelines, promulgated by Joint Staff/DTRA shall be used as a guide for these assessments.

e. IAW reference (b), Chief of Naval Operations Integrated Vulnerability Assessments (CNOIVA) is conducted by OPNAV 314 who directs NCIS Security Training, Assistance and Assessment Team (STAAT) to perform the assessments using DTRA Vulnerability Assessment Guidelines.

(1) Each installation requiring an IVA will receive either a JSIVA or CNOIVA every three years.

f. IAW reference (v), Local Vulnerability Assessments (LVA) shall be conducted by the installation ATO, at least annually using the DTRA Vulnerability Assessment Guidelines. JSIVA’s or CNOIVA’s meet the requirement of the annual LVA.

g. Higher Headquarters Assessment (HHA). Per reference (d), an overall assessment by a higher headquarters of how an organization is managing its AT program, to include management and compliance effort by subordinate organizations. HHA satisfies the annual AT Program Review requirement. CNIC has developed a programmatic approach to address protection shortfalls and recommend mitigating courses of action. This assistance is identified as the Installation Protection Assessment Cell (IPAC), and is intended to identify the baseline of protection requirements (should be), requirements that are not in compliance (as is), and develop risk mitigation solutions through multiple levels of analysis (to be). IPAC is a tool to complement and support protection assessments that are routinely scheduled at regional installations. IPAC evaluates the installations protection from a programmatic standpoint. IPAC analysis provides the installation with a way-ahead to best address the root cause of the non-compliance in order to provide a long term solution, not a temporary fix. This analysis can employ already existing resources to better manage the overall protection program of an installation. Additionally, this analysis can be utilized by the CO to evaluate the risk to the installation and make informed decisions about what actions the NSF must support in a resource constrained environment.
h. IAW reference (d), Personal Security Vulnerability Assessments (PSVAs) for all high-risk personnel will be initiated within 90 days of assignment to a high-risk billet. NCIS maintains a PSVA schedule which provides CNO semiannual updates.

i. IAW reference (b) NCIS STAAT will conduct Port Integrated Vulnerability Assessments (PIVA) and Airfield Integrated Vulnerability Assessments (AIVA).

j. Special Vulnerability Assessments. IAW reference (b), the NCC may upon occasion have the need for special assessments. These may include restricted waters (choke points), land deployment sites, humanitarian effort sites, hotels, etc.

k. A comprehensive AT program review shall be conducted at least annually by all commanders required to establish AT programs.

0304. Navy Force PRO

a. Risk mitigation plans for critical vulnerabilities identified during installation vulnerability assessments are crucial to prioritizing and mitigating these vulnerabilities. Regions and installations should utilize the software tool NAVY FORCE PRO to conduct continuous vulnerability risk mitigation at their respective installations.

b. The installation ATO will be the individual responsible for receiving Navy Force PRO training and operating the software. Software shall be NMCI or One-Net compliant as appropriate.

c. Training will be provided by the Navy Force PRO developer at all Navy Region sites and coordinated thru the ATWG’s.

0305. Risk Management

a. The AT Risk Management process begins with an assessment of the terrorist threat to DoD personnel and facilities. Each installation is mandated to develop an AT VA capability as prescribed by references (e) and (v).

b. Risk Management is a process that assists AT decision-makers in reducing or offsetting terrorist attack effects per reference (v). The process identifies, assesses, and controls
risk arising from operational factors and helps in determining which assets require the most protection.

0306. **Antiterrorism Planning**

   a. The purpose of a Regional AT Plan is to document specific Regional AT requirements and procedures and promulgate these to the installations and subordinate commands in the region.

   b. The Regional AT Plan is a compilation of specific measures necessary for the development and implementation of a comprehensive, integrated AT Program in compliance with references (b) and (w).

   c. The AT Plan is a critical element of an effective AT Program focused on the deterrence, detection, defense, and response to terrorist incidents. Accordingly, the focus of the Regional AT Plan should be on outlining region responsibilities and tasking the region staff directorates, installations, and subordinate commands with AT responsibilities and requirements. Likewise, the Region AT Plan should assist the installations and subordinate commands in the development of their respective AT Plans. CNIC regions must have a robust plan in place to support installations and subordinate commands and to remain compliant with GCC, NCC, and CNIC AT goals and objectives.

   d. Region AT Plans must address risk management, including terrorist threat assessments, criticality assessments, vulnerability assessments, and risk assessments, as well as AT and PS measures, FPCON implementation, terrorist incident response, and consequence management measures across the applicable region.

   e. Where there are multiple Commanding Officers/ Commanders located on an installation, the CO is responsible for coordinating the AT Plans and efforts for all units on the installation. In all cases, tenant commands shall integrate and synchronize their plans into the overarching installation plan.

   f. Commands shall leverage Naval Criminal Investigative Service (NCIS) capabilities regarding terrorism threat intelligence, LE, PS, and counter-surveillance when developing AT Plans and operations. The Multiple Threat Alert Center (MTAC) shall be the focal point for the integration of national-level, local, and/or host-nation intelligence, counterintelligence, and criminal intelligence pertaining to criminal, foreign intelligence, and terrorist threats.
0307. **Antiterrorism Officer (ATO)**

a. An ATO shall be assigned at the region staff level and at the installation level. The ATO is charged with managing AT matters. The installation ATO shall coordinate with tenant command ATOs for unity of effort. IAW reference (b) the ATO shall meet the following minimum requirements:

1. Be a commissioned officer, chief petty officer (E-7 or higher), or civilian (GS-11 equivalent or higher). This position is inherently governmental in nature and may not be assigned to a contractor.

2. Attend the ATO Course of Instruction (COI) (J-830-0015) within 3 years prior to assuming the ATO duties. This course includes service specific modules and training in methods to obtain specific data for varying geographic areas, and includes Joint Staff Antiterrorism Enterprise Portal (ATEP) and Core Vulnerability Assessment Management Portal (CVAMP) training into ATO training on NIPRNET and SIPRNET systems.

3. Refresher training shall be completed at least once every 3 years via the ATO COI J-830-0015.

b. ATOs must have a detailed and thorough knowledge of AT programs and must understand how the program applies to their installation or staff. The ATO must ensure that each person within the unit is aware of the terrorism threat and is trained to employ methods to reduce risk or mitigate the effects of a terrorist attack. The knowledge factors include but are not limited to:

1. NCIS MTAC
2. Navy Blue Dart Program
3. Suspicious activity reporting
4. Dissemination of terrorist threat information
5. DoD AT standards
6. CNO AT Standards
7. IVA process
(8) Port Assessment (PA)/Airfield Assessment (AA) process
(9) Funding for AT
(10) Levels of AT training
(11) Overseas travel security
(12) High-risk billet requirements
(13) Foreign travel planning requirements for personnel
(14) SIPRNET network access
(15) CVAMP network access
(16) Unified Facility Code (UFC) criteria

0308. **Installation AT Plan**

a. Every installation shall have an approved, signed and validated executable AT plan. The AT plan shall be reviewed and exercised at least annually. The AT plan is a component of the overall protection program.

b. COs shall ensure that IAW reference (v) and Combatant Commander's guidance, annual threat, criticality, vulnerability, and risk assessments are conducted.

c. Successful AT Plans must be executable and realistically matched to requirements and available resources. All personnel must clearly understand their responsibilities and receive training on AT plan measures. For example, the Random Antiterrorism Measures (RAM) Plan is not the sole responsibility of the Security Detachment, but involves all departments and tenant activities on every installation IAW reference (v).

0309. **Antiterrorism Working Group (ATWG).** The REGCOM and CO shall establish an ATWG at their respective levels that meet to develop and recommend policy; prepare planning documents; oversee the implementation of the AT program; develop and refine AT plans; and to address emergent or emergency AT program issues. The ATWG shall meet at least semi-annually or more frequently depending on the Threat Level or threat activity.

a. At a minimum, regional membership shall consist of, the commander or a designated representative, RSO, ATO, installation
ISO’s, installation ATO’s, regional department heads, USCG representative, NCIS and local, federal and state LE officials.

b. At a minimum, installation membership shall consist of, the commander or a designated representative, ATO, ISO, NSF senior personnel, department heads, NCIS and tenant command representatives (ships in-port, aviation squadrons, etc).

0310. **Individual Antiterrorism Plan (IATP) and Travel Tracker/Notifier (TT/N)**

a. IATP are required when on official travel in the Pacific Command (PACOM) AOR. Although not required for other areas, commands and personnel are encouraged to submit an IATP or TT/N when on travel.

(1) An IATP is an automated, electronic document completed for a specific destination or country prior to travel to ensure the traveler is briefed on and understands relevant threats and conditions at their destination.

(2) The IATP travel plan is electronically entered into a country specific tracking database which automatically notifies the traveler and his/her Chain of Command (COC), via auto-generated e-mail, if there is an increase in terrorist or criminal activity, political violence, or FPCON level, or if the State Department or COCOM issues a sudden Public Announcement, Travel Warning, or Travel Restriction. This action keeps the individual or transient traveler aware of the threat environment throughout all phases of travel, i.e., planning, actual travel and up to completion.

(3) In response to acts of terrorism or natural disasters, the individual’s command, as well as higher headquarters, can query the system to instantly account for their personnel on travel to any destination in the world, in real time.

b. The automated TT/N program mirrors and provides similar capabilities to the individual traveler and the COC as the IATP, but does not require the approval process mandated for travel to countries in the PACOM AOR.

c. AOR specific location briefs should include the destination FPCON level, Terrorist Threat Level (TTL), Political Violence Threat Level (PVTL), and Criminal Threat Level (CTL). The traveler should also be provided and/or have access to the
Department of State (DOS) Consular Information Sheet, DOS Travel Warnings and/or DOS Public Announcements which are currently in effect for the intended destination(s). The DOS Consular Information Sheet contains unclassified safety and security information. This may include information on specific terrorist groups, their history, and methods of operation as applicable to the intended destination(s). American Embassy phone numbers and emergency phone numbers are also listed in the DOS Consular Information Sheet. The traveler must also be aware of and comply with any/all specific Combatant Command (COCOM) requirements, such as the buddy-rule requirements and travel restrictions.

d. AT Level 1 Awareness training is an annual requirement and must be completed within 12-months of travel IAW OPNAVINST 3300.53c, Navy Antiterrorism Program. It is to be completed prior to submitting an IATP or TT/N.

e. IATP and TT/N Program.

(1) The automated IATP and TT/N program is available at: https://paccas.nmci.navy.mil/navy/cpf/atfp/home.nsf.

All IATP and TT/N submissions shall be submitted utilizing the web-based automated program. To ensure data point entry into the Country Specific Threat Matrix Tracking Database and to facilitate instant accountability of personnel on official or unofficial travel, other IATP formats and/or methods of submission and approval should not be used.

(2) For official and unofficial travel, an IATP should be submitted and processed with enough local lead time to ensure the required timelines stated in the DoD Foreign Clearance Guide are met regarding the submission of a Theater and/or Country Clearance Message (TCCM) as required. For unofficial travel and if there is no TCCM requirement, the IATP must be submitted NLT 3 days prior to travel. There is no time limitation for TT/N submissions due to the fact they do not require an approval process.

(3) IATP/TT/N submissions are reviewed for completeness and accuracy by an appointed unit, installation, or command IATP coordinator (collateral position) prior to forwarding the document for final approval. The IATP coordinator shall ensure the AOR location specific brief and Level 1 AT training dates are current, the buddy-rule requirement has been met when required, that complete and verifiable contact information is in place, and the appropriate approval level is listed in the COC.
The IATP coordinator will make enough substantive comments to the approval authority in order that the approver will not have to open the document and go through it page by page. The approval authority should be able to click on the link in the auto-generated e-mail, log in, and approve or disapprove the IATP, with or without comments.

(4) The IATP/TT/N does not replace other traditional forms of travel approval, i.e., verbal approval, leave request/form, special request form, TAD request, travel orders, etc. With the exception of the Theater and Country Clearance Message, an IATP or TT/N is the final step in the pre-travel process. Since the IATP is intended to be part of an already approved process, it does not require a full COC review. The automated program processes an IATP for approval via a very limited review/routing process.

(5) Refer to PACOM OPORD 5050 for travel to countries in PACOM AOR for approval levels.

(6) For travel to countries not in the PACOM AOR, use of the TT/N is encouraged. The TT/N does not require an approval process. If a Commanding Officer optionally directs use of an IATP vice a TT/N, the same approval levels required for PACOM will apply.

(7) When traveling as a member of a group or unit deployment, one IATP/TT/N can be completed for the entire group/unit. Separate individual plans are not required for personnel complying with the group/unit travel plans. If an individual's travel will differ significantly from that of the group/unit, then a separate IATP/TT/N must be completed for the portion of travel that differs. An example is when the traveler is going on leave prior to or after a group/unit deployment. This also applies to unofficial/personal travel such as group tours with MWR.
CHAPTER 4
PHYSICAL SECURITY

0401. Physical Security Programs. The Physical Security Program is a component of the Protection Program 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. PS involves the total spectrum of procedures, facilities, equipment, and personnel employed to provide a secure environment. The PS Program includes the requirements for threat assessments, surveys and inspections.

0402. Objective

a. Protection of people and assets onboard a Navy installation or site must start with an understanding of the risk posed from a possible terrorist attack or natural disaster. Application of the PS standards set forth in UFC publications and reference (a) should be consistent with the perceived or identified risk. All personnel, both military and civilian, onboard Navy installations have a responsibility in protection of personnel and assets. Perfect or absolute security is always the goal of those responsible for security of a facility or activity, but such a state of absolute security may never be fully achieved. There is no object so well protected that it may not be stolen, damaged, destroyed, or observed by unauthorized individuals. A balanced security system provides protection against a defined set of threats by informing the user of attempted intrusions and providing resistance to the would-be intruder’s attack paths. This resistance must be consistent around the entire perimeter of the protected area.

b. Physical Security measures deter, detect, assess, warn, defend, and recover against threats from terrorists, criminals, and unconventional forces. Measures include fencing and perimeter standoff space, lighting and sensors, vehicle barriers, blast protection, intrusion detection systems (IDSs), electronic surveillance and access control devices and systems.

c. These measures are augmented by procedures such as security checks, inventories, and inspections. PS measures, like any defense, should be overlapping and deployed in depth, as discussed in this chapter. Required PS measures are detailed in referenced DoD publications and service regulations.
d. A principle to adhere to is DBT which provides the basis for the physical security system in place at an installation. In order to counter the threat for which our physical security systems are designed a fundamental principle of physical protection is that it should be based on the current evaluation of the threat. This evaluation is formalized through a Threat Assessment process. The DBT is derived from this Threat Assessment.

0403. **Policy**

a. Implement policy guidance IAW reference (x) to establish minimum security standards for controlling entry to Navy installations. The standards shall be implemented CONUS to include Alaska and Hawaii, its territories and possessions, as resources, law and capabilities permit. OCONUS installations will comply with SOFA and other requirements, as able. Access control standards shall include:

   (1) Identity validations

   (2) Determining the suitability of an individual requesting and/or requiring access

   (3) Vetting

b. Establish a defense-in-depth concept to provide graduated levels of protection from installation perimeter to critical assets by:

   (1) Establishing positive access control measures at entry control points (ECPs).

   (2) Enforcing the removal of, or denying access to, persons who are a threat to security, good order and discipline.

   (3) Designating restricted areas to safeguard property or material for which the CO is responsible.

   (4) Using RAM’s within existing security operations to reduce patterns, change schedules and visibility. This tactic reduces the effectiveness of preoperational surveillance by hostile elements.

0404. **Protection Capabilities.** The protection activities of deter/detect, assess/warn, defend and recover translate to capabilities, as depicted in Figure 4-1. The ability to execute
protection activities constitutes capabilities (e.g., detect is a protection activity; the ability to detect is a capability).

![Diagram of Force Protection]

**Figure 4-1. DoD Proposed Ashore AT Architecture**

**0405. Defense in Depth.** IAW reference (v) commanders shall employ defense in depth when designing PS programs. This is the central concept in the Navy's strategy toward defending against threats. It involves a series of redundant measures, varying actions, and multiple layers of defense. Defense in depth gains its strength from the layering of defenses in order to mitigate the defeat of one PS measure eliminating single points of failure and preventing the success of a terrorist attack. This combination presents a more challenging target to potential terrorists and increases the probability of defeating an attack. Furthermore, a layered defense ensures that potential threats are identified as early as possible, allowing for the determination of hostile intent and increasing the time available to apply multiple defensive measures.

**0406. Sex Offender Tracking, Assignment, and Installation Access Restrictions.** Reference (y) implements reference (z) which provides policy and defines the roles and responsibilities for controlling access to Navy installations and Navy owned or leased military housing or Public-Private Venture (PPV) housing by sex offenders. Reference (y) provides all necessary guidance to prohibit to the maximum extent permitted by law or otherwise waived by competent authority, the policy that sex offenders are to be identified and prohibited from accessing Navy installations and facilities.

**0407. Taxi, Limousine, and Shuttle Access**

a. This policy applies during FPCON NORMAL and ALPHA only. Commanders may restrict access at heightened FPCONS and must ensure that registered companies understand that their access may be restricted due to a change in security conditions. Due
to unique circumstances and other agreements with host nations, this policy may not be applicable to all OCONUS installations. Installations and facilities that do not have manned entry control points are exempt.

b. Existing taxi/transportation contracts are not affected by this policy. Once existing contracts with taxi/transportation companies expire, all taxi/transportation companies are permitted to apply for installation access.

c. Region Commanders and Installation Commanding Officers have a mandate under reference (a) to provide PS for their installations. Consideration and balance must also be given to quality-of-life issues for personnel.

d. The primary objectives of this section are to:

(1) Establish a uniform Navy protocol across CNIC regions for installation access by regulated transportation services for personnel who have legitimate installation access to locations on and off the installation.

(2) Authorize issuance of appropriate credentials for physical access to Navy installations by taxicab, limousine, and shuttle services and their drivers.

(3) Provide guidance to identify a Single Source Coordinator (SSC) who shall have oversight of the registration and clearance of taxicab, limousine, and shuttle services and drivers who are authorized to conduct business on an installation. (See Appendix B for definition for SSC)

e. The SSC shall facilitate the registration requests of one or more taxicab, limousine, and shuttle companies to conduct business on an installation. The registration shall ensure that each vehicle owned by a taxicab, limousine, or shuttle service is registered with the state division of motor vehicles, is safety inspected in accordance with state and local requirements, has proof of insurance, and is licensed to operate as a transit, cab, limousine, or shuttle service with the state, county, city, or local public utilities commission or similar body as required. Private vehicles operating as unlicensed cabs shall not be permitted to register under this instruction.

f. Each taxicab, limousine, and shuttle that has been properly registered, inspected for safety, insured, and licensed by the host nation, state, county, city, or other regulating
government entity shall be granted access if it is operated by an authorized driver possessing a region or installation issued photo identification card.

g. The SSC shall register each taxicab, limousine, and shuttle driver that operates a taxicab, limousine, and shuttle on an installation. The registration shall ensure each driver is properly licensed to operate a vehicle for hire and has a current host nation or state issued driver’s license. A driver shall be required to have a criminal history check that meets the commander’s requirements. At a minimum, criminal history checks shall be in accordance with existing processes for contractors.

h. Once a person is certified as having passed a criminal history check and is properly licensed, the SSC shall provide a photo identification card, which shall expire no longer than one year from date of issuance. The photo identification card shall include at a minimum, the full name of the individual, picture, drivers license and taxi license numbers, and the name of the company they are employed by. The identification card shall be displayed on each entry to an installation. SSCs with non-appropriated funds may charge a reasonable fee to cover costs of administering this policy.

i. Commanders will require an inspection of each taxicab, limousine, or shuttle entering an installation to safeguard personnel. This inspection may be accomplished at the commercial vehicle inspection station. Except for ROC Level 1 installations, the lack of a dedicated commercial vehicle inspection team shall not preclude entrance by a taxicab, limousine, or shuttle. Taxicabs, limousines, and shuttles are always subject to inspection at ECPs. If conducted at the ECP, vehicle inspections will, at a minimum, consist of a visual inspection of the trunk and passenger compartment.

j. ROC level 1 and 2 installations shall restrict taxicabs, limousines, and shuttles from areas that include high-value assets and restricted areas.

k. Registered companies will be informed that any violation of federal law, base regulation, or other disruptive activity shall result in the termination of that company’s access under this program.
1. Registered companies will be informed that CNIC may elect to terminate this program at any time at CNIC’s sole discretion.

m. In the event a taxicab, limousine or shuttle is not registered by the SSC and issued an identification card, regions and installations may admit these vehicles subject to the following conditions:

   (1) The taxicab, limousine, or shuttle is delivering a fare that has legitimate installation access.

   (2) The taxicab, limousine, or shuttle driver has been properly registered and licensed by the host nation, state, county, city, or other regulating government entity that regulates and licenses drivers in that geographic area.

   (3) The taxicab, limousine, or shuttle passenger and trunk area is inspected before proceeding beyond the ECP.

   (4) A temporary pass will be issued by the ECP sentry that expires in a reasonable amount of time for the fare to be delivered to a destination and the taxicab, limousine, or shuttle to return to the ECP where it entered the installation. The commander may require the ECP sentry retain the taxicab, limousine, or shuttle’s “license to operate” until the driver returns to the ECP.

   (5) The taxicab, limousine, or shuttle may not pick up another fare while on the installation.

n. REGCOMs/COs shall:

   (1) Identify the SSC for the region/installation to administer this section. The SSC position is an unfunded requirement that must be met within the region/installation current resources. This position may be filled by Security, MWR or Non-Guard Services personnel.

   (2) Set the local policy pertaining to inspection of taxicabs, limousines, and shuttles for the installation.

   (3) Establish a local policy to validate an empty taxicab, limousine, or shuttle has a legitimate call for service when entering an installation.
(4) COs have the discretion to establish one or more taxi stands on an installation for a taxicab, limousine, or shuttle to queue for fares.

 o. SSC shall:

 (1) Process taxicabs, limousine, and shuttle service companies using the existing region/installation authentication process.

 (2) Ensure drivers have had a criminal history check conducted before issuing an identification card.

 (3) Collect expired passes and credentials and conduct quarterly reviews with the taxi/transportation companies to verify credentialed drivers’ employment with the company.

0408. Installation and Facility Access Control. Installations shall develop a comprehensive personnel and vehicle access, identification, and movement control system which provides a visible means to identify and account for personnel and vehicles authorized access to Navy installations. Installation Commanding Officers shall establish a process for removal of, or denying access to, persons who are not authorized, or represent a threat in accordance with the sensitivity, classification, value, or operational importance of the installation and the requirements of this instruction. The Installation Commanding Officer has the authority to alter and enforce additional access control policy measures during elevated FPCONs and emergent situations to protect persons and property subject to their control.

 a. Access Control

 (1) Access control is a key component of the installation's protection program. Installation access control standards shall include identity proofing and vetting to determine the fitness of an individual requesting and/or requiring access to installations prior to issuance of local access credentials. Access control procedures and processes as part of the installation's AT Plan shall have clearly documented TTP, which are essential in providing clear and consistent access control to installations.

 (2) Access control is defined as PS measures that include PS equipment, personnel, and procedures used to protect installations and Navy assets from possible threats. ECPs have the primary function of detecting and deterring unauthorized
intrusion onto an installation. ECP duties include, but are not limited to, the following:

(a) Monitoring and maintaining vehicle and pedestrian ingress and egress through the ECP.

(b) Maintaining situational awareness of the gate and surrounding area both on and off the installation, including detecting impaired drivers; conducting vehicle, personnel, and document inspections; and detecting surveillance.

(c) Conducting RAMs to reduce patterns, change schedules, and visibly increase the security profile of an installation to enhance the detection of violation(s) and reduce the effectiveness of surveillance by hostile elements and/or unauthorized personnel.

(d) Taking effective measures, including using barriers and other technology and appropriate use of force, to stop unlawful intrusions.

(3) In OCONUS locations where US forces are tenants and the Host Nation exercises access control of a facility or installation, a Commanding Officer will follow the guidance provided in this chapter to maximum extent possible without violating agreements or host nation laws.

b. Installation access control plans shall address and comply with the entry control standards provided here as guidance to REGCOM and CO including:

(1) Types of access include:

(a) Unescorted individuals.

(b) Escorted individuals.

(2) Other considerations for controlling installation access, but are not limited to:

(a) Escort qualifications, responsibilities, and authorizations.

(b) Sponsorship qualifications, responsibilities, and authorizations.
(c) Access privileges at each security level and each FPCON.

(d) Mission-essential employee designation, if applicable.

(e) Emergency response designation, if applicable.

(d) Day and time designation for access.

(e) Locations authorized for access

c. Entry Control Business Rules.

(1) Access control procedures and policy must be consistent and established on a common baseline of rules and conditions for providing access on normal and exigent situations. Region Commanders and Installation Commanding Officers will ensure that the business rules are used as a foundation for developing policy, implementing guidance, and procedures related to installation entry control.

(2) Site specific access controls must be addressed in regional and installation level instructions and implementing guidance.

d. Entry Control Standards

(1) Entry Control Standard 1: Program implementation. The Installation Commanding Officer shall establish program guidelines that clearly delineate operational and administrative command responsibilities.

(a) RSOs and ISOs shall be responsible for access control procedures and techniques. BOS access control capabilities may be managed from a regional or installation level. Region and installation rules, regulations, and procedures (RRP) shall be updated to include and align with this instruction.

(b) Tenants onboard Navy installations with mission related access control functions and requirements shall coordinate access control requirements and TTP with host installation Security Detachments as an annex to their AT Plans. Where these missions impact installation security force personnel and resourcing, tenants will be assessed and an Inter-Service Support Agreement developed to address requirements for
these reimbursable posts and functions. Host installations will identify tenant access control requirements to the region.

(c) Entry control procedures (such as inspecting an individual and their possessions while on the installation) shall be coordinated and reviewed by the Region SJA for legal sufficiency prior to publication and implementation.

(2) Entry Control Standard 2: Identification, Authorization, Authentication, Credentialing and Access. A combination of active and passive measures will control access to an installation. The processes of identification, authorization, authentication, credentialing, and granting access must be uniform and integrated. Personnel access identification checks will continue to be performed physically and visually until upgraded or replaced with Federal Personal Identity Verification (PIV) compliant systems that provide the capability to rapidly and electronically authenticate credentials and individuals’ authorization to enter.

(a) Credential capabilities must be sustainable and scalable for all conditions (e.g., natural disasters, Fleet Week, air shows, etc.) and at all FPCONs. Access control capabilities must allow for site specific requirements, including performance capabilities such as personal identification numbers, biographic and/or biometric use.

1. The process of credentialing and granting access, while inherently related, occurs in physically different locations. The Visitor Control Center (VCC) should be located away from and outside the ECP IAW reference (aa). ECPs shall issue temporary passes when the VCC is not open. Rental agreements combined with the appropriate identification are sufficient for vehicle access. Specific RRP shall be initiated to positively identify and verify a visitor’s identity and right to access an installation before temporary passes are issued at an ECP.

2. Installation access privileges, systems and processes must function in concert with the Federal Personal Identity Verification policy and procedures. System capability for identity verification shall be compatible with other government-issued cards, including Common Access Card (CAC), DoD Smart Cards, DD Form 2, and DD Form 1173. No system shall be procured for the purpose of issuing credentials in place of government-issued cards. The only exception is the Navy Commercial Access Control System (NCACS) which is an enterprise
identity management and perimeter installation access control solution designed to manage commercial vendors, contractors, sub-contractors, suppliers and service providers (vendors/contractors) who are not eligible for a CAC coming aboard CNIC installations.

(b) Only personnel delegated by the installation commander shall perform access control duties that include:

1. Identity proofing.
2. Vetting and determination of fitness
3. Access authorizations and privileges

(c) Acceptable Identification Documents. Applicants will provide a valid form of identification listed below for the purpose of enrollment and initiation of security checks. Prior to acceptance, personnel processing applicant will screen documents for evidence of tampering, removal of protective laminate, or other alteration. Documents that appear to be tampered with, having damaged laminates, or otherwise altered will not be accepted. Acceptable documents are as follows:

1. United States passport.
2. Permanent resident card or Alien Registration Receipt Card (Form I-551).
3. Unexpired foreign passport with a temporary (I-551) stamp.
5. Unexpired foreign passport with an unexpired Arrival-Departure Record (Form I-94) bearing the same names as the passport and containing an endorsement of the alien's nonimmigrant status if that status authorizes the alien to work for the employer.
6. Driver's license or identification card issued by a state or outlying possession of the United States, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address.
7. Identification card issued by federal, state, or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address.

8. College or secondary school, if located on the installation, identification card with photograph.


10. Military dependent identification card.

11. U.S. Coast Guard Merchant Mariner Credential (MMC) or Merchant Mariner's Documents (MMD).


13. Driver's license issued by a Canadian government authority.

14. School record, report card, day-care record, or nursery school record will be accepted for persons under the age of 18 who are unable to present a document listed above.

(d) As funding becomes available, Regions and installations will procure electronic Physical Access Control Systems (PACS) that provide the capability to rapidly and electronically authenticate credentials and individuals authorization to enter an installation.

(e) Denial of Base Access. The establishment of standards for base access is ultimately the responsibility of the Installation Commanding Officer. Any adverse information identified during criminal history checks must be evaluated by a competent individual designated by the Installation Commanding Officer, who is qualified in interpreting criminal record information. Likewise, positive mitigating factors should be considered into the final determination. The following minimum standards should be considered for denying installation access for a civilian employee, contractor/subcontractor, family members or non-affiliated civilians:

1. Any felony conviction within the past 10 years.
2. Membership within the previous 10 years in any organization that advocates the overthrow of the U. S. Government.

3. Any conviction of an offense meeting the sexual offender criteria in reference (y).

4. Any person barred from a Navy installation. Once a barment letter is issued, the installation SJA will enter the letter into CLEOC. If the nature of the barment action extends beyond the installation to Region or enterprise levels, the Region or CNIC SJA will be notified to process the appropriate barment letter and enter the letter into CLEOC. Visitor Control Center personnel shall access CLEOC to ensure personnel requesting installation entry are not barred prior to granting access.

(f) This list of offenses that should deny access is not all-inclusive and may be modified as required by the REGCOM or CO. Appeals to denial of base access will be through the CO to the REGCOM.

(3) Entry Control Standard 3: Access Categories. Installation access must be granted in a clear and uniform manner to reduce the likelihood of unauthorized access to the installation or facilities inside the installation that require greater controls. Access control will be aligned with day-to-day access needs in addition to personnel categories as a part of the CNIC EM and Continuity of Operations (COOP) Programs. The following categories identify the types of installation access and associated personnel category eligibility.

(a) DoD ID Holder. U.S. Uniformed Military Service members and DoD federal civilian employees are hired and paid from appropriated and non-appropriated funds under permanent or temporary appointment. The CAC is the principal authorized credential for personnel in this access category. Status as a DoD ID cardholder supersedes all other access control categories. Personnel in this access category shall be designated as Personnel Category 1, 2, 3, or 5 as identified in reference (p).

(b) U.S. Government Employees (non-DoD). U.S. Government Employees with proper identification and an approved visit request will be allowed access to the installation with their issued federal government credentials. Federal LE special agents and uniformed police officers will be granted access upon
presentation of appropriate credentials and not require a visit request. For non-DoD LE personnel, the person’s last name and agency will be reported via radio and captured on record in command communication log.

(c) Host-Nation/Third-Country Nationals. This access control category includes host-nation and third-country nationals assisting U.S. operations per international agreement. Personnel in this access control category will be granted access using employing government-issued credentials, host-nation/third-country national conditions for employment and verification of need to access. Personnel in this access control category will be designated Personnel Category 1 or 4.

(d) DoD and Non-DoD Emergency and First Responders. Personnel in this access category have been identified as a legitimate responder with official credentials issued by federal, state or local government. This category also applies to contractors who are specifically tasked to provide essential services during higher FPCONs and other identified incidents (e.g., natural disaster). Personnel in this access control category will be designated Personnel Category 5. Access control SOP’s shall identify emergency and first responders consistent with EM Plans and address access control for all personnel IAW reference.

(e) Trusted Traveler procedure may be used during FPCONs NORMAL, ALPHA, and BRAVO as local security conditions permit. The Trusted Traveler procedure is governed and implemented locally and is not recognized from installation to installation.

1. The Trusted Traveler procedure allows a uniformed service member or Government employee with a valid CAC, a military retiree (with a valid DoD identification credential), or a dependent of at least 16 years of age (with a valid DoD identification credential) to present their identification token for verification while simultaneously vouching for any vehicle occupants. The number of personnel a Trusted Traveler is allowed to vouch for and/or sponsor at any one time shall be determined by the installation commander or designated representative.

2. Members identified as Trusted Travelers are responsible for the actions of all occupants for whom they vouch and for meeting all security requirements for escort as established by the Service or installation commander.
(f) Family Members. Individuals defined as "family members" include spouses, unmarried widows, unmarried widowers, and unmarried children (including adopted children or stepchildren) who are under 21 and unemancipated or under 23 and enrolled in a full-time institution of higher learning. In addition, this group includes the family members of DoD civilian employees, particularly those assigned overseas. DD Form 1173 is the current credential for personnel in this access category. Personnel in this access category shall be designated Personnel Category 2 only.

(g) Unescorted Day/Visitor Access (Other than Contractor Employees). These will be issued for visits of a short duration (less than 30 days)(e.g., family visits, retired Civil Service using morale/welfare/recreation [MWR] facilities that are not in possession of a retired civilian ID card, sporting events, and various meetings). Installation passes shall be renewed daily or issued for the duration of family visits or scheduled meetings. Contractors shall not use daily access procedures to circumvent criminal history check requirements outlined below. Personnel in this access control category shall be designated only Personnel Category 2. Unescorted day/visitors require the following for access:

1. An installation sponsor request forwarded to the Security Detachment.

   Note: Any request for entry by civilian news, radio, television, or other media shall be referred to the installation public affairs officer prior to installation entry.

2. A valid form of federal or state government identification that includes a photograph or information such as name, date of birth, gender, height, eye color, and address.

3. If driving a motor vehicle, a valid driver's license, vehicle registration, and proof of insurance.

4. Sex Offender Registration and Notification Act of 2006 (SORNA) check for DoD non-affiliated and affiliated personnel will be conducted IAW paragraph 0406.

(h) Contractors/Vendors.

1. Temporary business access will be granted for contractor/vendor employees requiring physical access for
periods from one day to one year. Regularly scheduled delivery personnel (e.g., FEDEX, UPS, pickup and deliveries) requesting business access shall submit proof of employment and proof of an employee criminal history check to include a SORNA check conducted within the past year covering the previous ten years as a minimum. If the delivery service has a government contract, the government contracting entity will submit a letter of sponsorship to the credentialing office specifically naming the contractor, length of contract, and personnel requiring access to the installation as well as any required special access to restricted areas. Contractor employee criminal history checks are conducted at contractor expense and shall include U.S. citizenship or legal alien status. Acceptable documents are listed in Table 4-1. Personnel in this access category will be designated Personnel Category 2 or 3. Refer to Para 0409 for specifics of the Navy Commercial Access Control Systems Program. Contractor delivery personnel who require infrequent access to Installations will be required to have criminal history and SORNA checks conducted by the Visitor Control Center prior to allowing access.

2. Permanent business access will be granted to contractor personnel for a period up to, but not to exceed, three years for physical and/or logical access. Personnel requiring access shall submit all items and fulfill all requirements listed in Table 4-1 and are subject to a local criminal history and fingerprint check in accordance with local and/or host-nation laws. When a contractor is granted access, the criminal history check shall be reevaluated annually or as local law or host-nation agreements permit. Contractor employee criminal history checks are conducted at contractor expense. Contractor personnel that require logical access will be issued a CAC, which shall be administered via the Contractor Verification System (CVS). Personnel that meet these criteria are Personnel Categories 1, 2, or 5.
### Table 4-1
List of Acceptable Documents
(One from List A or one from each of Lists B and C)

<table>
<thead>
<tr>
<th>List A</th>
<th>List B</th>
<th>List C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents that Establish Both Identity and Employment Eligibility</td>
<td>Documents that Establish Identity</td>
<td>Documents that Establish Employment Eligibility</td>
</tr>
<tr>
<td>• U.S. Passport (unexpired or expired)</td>
<td>• Drivers license issued by a state or outlying possession of the United States that contains a photograph or information such as name, DOB, gender, height, eye color, and address</td>
<td>• U.S. Social Security card (other than a card stating it is not valid for employment)</td>
</tr>
<tr>
<td>• Certificate of U.S. Citizenship (Form N-560 or N-561)</td>
<td>• ID card issued by federal, state, or local government agency that contains a photo, or information such as name, DOB, gender, height, eye color, and address</td>
<td>• Certification of Birth Abroad issued by the State Department (Form FS-545 or DS-1350)</td>
</tr>
<tr>
<td>• Certificate of Naturalization (Form N-550 or N-570)</td>
<td>• School ID card with photo</td>
<td>• Original or certified copy of a birth certificate issued by a state, county municipal authority, or outlying possession of the United States bearing an official seal</td>
</tr>
<tr>
<td>• Unexpired foreign passport with I551 stamp or attached Form I-94 indicating unexpired employment authorization</td>
<td>• Voter registration card</td>
<td>• Native American tribal document</td>
</tr>
<tr>
<td>• Permanent Resident Card or Alien Registration Receipt Card with photo (Form I-151 or I-551)</td>
<td>• U.S. Military card or draft record</td>
<td>• U.S. Citizen ID Card (Form I-197)</td>
</tr>
<tr>
<td>• Unexpired Temporary Resident Card (Form I-688)</td>
<td>• Military dependent ID card</td>
<td>• ID card for use of resident citizen in the United States (Form I-179)</td>
</tr>
<tr>
<td>• Unexpired Employment Authorization Card (Form I-688A)</td>
<td>• U.S. Coast Guard Merchant Mariner Credential (MMC) or Merchant Mariner's Documents (MMD)</td>
<td>• Unexpired employment authorization document issued by DHS (other than those listed in List A)</td>
</tr>
<tr>
<td>• Unexpired Reentry Permit (Form I-327)</td>
<td>• Native American tribal document</td>
<td></td>
</tr>
<tr>
<td>• Unexpired Refugee Travel Document (Form I-571)</td>
<td>• Drivers license issued by a Canadian government authority</td>
<td></td>
</tr>
<tr>
<td>• Unexpired employment authorization document issued by the Department of Homeland Security (DHS) that contains a photo (Form I-688B)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(i) Private Public Venture (PPV) Housing.

There are CNIC installations that have PPV Housing within the confines of the installation and lease quarters to non-DOD civilians. The following guidance will be utilized in these circumstances:

1. Prior to entering into a housing lease with Non-DOD Civilian applicants, the Housing Representative shall:
   
   a. Request the PPV Partner conduct a local criminal history check. If contractual agreements prevent this action, the Installation Security Department shall conduct a criminal history check prior to allowing installation access.
b. Ensure applicants understand vehicle registration requirements.

c. Forward the names of Non-DOD civilian applicants and family members over the age of 18 to the Visitor Control Center.

d. Ensure applicant and family members over the age 18 complete all necessary paperwork for installation entry a minimum 5 days prior to the effective date of the lease.

e. Confirm the housing lease term to establish the required access.

f. Housing Representative will report any changes in the lease that would affect installation access control to the installation security department.

2. Upon completion of the Non-DOD Civilian applicant's criminal history check, the Visitor Control Center shall:

a. Notify the Housing Representative.

b. Issue Non-DOD Civilian applicant and family members over the age of 10, an Installation Photo Identification which will reflect installation name and the initials "PPV".

c. Photo Identification will not exceed 24 months or the term of the lease whichever is less.

d. Issue applicant a contractor decal for the PPV occupants registered vehicles not to exceed 24 months or the term of the lease whichever is less.

3. Upon check out of Non-DOD Civilian PPV resident from housing, housing Representative will collect the PPV Identification's and Decals. The housing representative will then notify the Installation Visitor Control Center of the lease termination and I.D/ Decal collection.

4. Non-DoD personnel in PPV Housing will be designated Personnel Category 2.

(j) Not Regularly Scheduled Delivery Access. These will be issued to nongovernmental delivery vehicles requiring physical access. This category poses the greatest AT threat to
our installations and is the most difficult to regulate without impacting operations. Delivery personnel requiring access shall submit appropriate documentation as listed in Table 4-1 and may be issued an installation pass. NSF personnel shall inspect delivery vehicles through the designated Commercial Vehicle Inspection process and as required by the GCC guidance, RAM’s or FPCON increases. Personnel in this access control category will be designated either Personnel Category 2 or 3.

(k) Volunteers. Persons working on a Navy base not having DoD personnel or family member access but providing volunteer time as a part of a recognized and approved program in accordance with reference (bb) may be granted physical access to an installation for a maximum duration of one year.

(l) School bus and state/local bus service vehicles will be authorized entry to installations for the purpose of picking-up or dropping off government personnel and their dependants. Each installation must ensure the bus operating entity (school district, city, state, etc) performs criminal history checks for all drivers prior to authorizing installation access.

(m) Vehicles. Vehicles that access an installation on a daily basis are divided into four categories: military vehicles, contractor or vendor vehicles, privately owned vehicles (POVs) and rental vehicles.

1. Military vehicles are vehicles that are purchased, leased, or rented for use exclusively by the military.

2. Contractor/vendor vehicles are privately or company owned and operated vehicles for commercial or commerce use.

a. Contractor/vendor vehicles shall be clearly marked as to their authorization for access. Security members shall ensure that contractors, vendors, taxicabs, limousines, and shuttles are on the business access list that is approved by the Installation Commanding Officer before allowing access and that vehicle access identification is clearly displayed.

b. Taxicabs, limousines, and shuttles may be permitted to have a pickup stand located on the installation at the discretion of the REGCOM/CO; however, they may not enter
the base unless they have a call for service and/or have a legitimate fare to deliver.

3. POVs are vehicles used for personal and private use, such as a family van, sedan, pickup truck, etc. Decals for POVs will be issued per reference (cc). Private vehicles operating as unlicensed cabs or jitneys shall not be permitted to register with the installation in accordance with this instruction.

4. Rental Vehicles. Any person who would otherwise be granted access to an installation may enter an installation while driving a rental vehicle by presenting a current rental vehicle agreement and appropriate identification.

<table>
<thead>
<tr>
<th>Category</th>
<th>Personnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Emergency-Essential Military, Navy/DoD Civilians, &amp; Navy/DoD Contractors</td>
</tr>
<tr>
<td>2</td>
<td>Other U.S. Personnel, including: Family members living on &amp; off base, Non-emergency-essential Military, USG Civilians, &amp; USG Contractors</td>
</tr>
<tr>
<td>3</td>
<td>Other personnel supporting U.S. Military Operations including: Non-U.S Citizens employed by Navy or Navy contractor (if not in Category 1 or 2), foreign military personnel employed by the Host Nation</td>
</tr>
<tr>
<td>4</td>
<td>Allied/Coalition Personnel including: Host Nation and Third Country Nationals assisting U.S. operations per international agreement</td>
</tr>
<tr>
<td>5</td>
<td>First and Emergency Responders: Fire &amp; Emergency Services, HAZMAT Response Teams, NSF, EMS, EOD, Emergency Response Teams (ERTs), OHS Spill Response and Fire Brigades. Emergency Responders, including EM, ROC/EOC Staff, Dispatch Staff, Medical Treatment Facility/Healthcare Providers, Public Health Emergency Officers, Mass Care, Mortuary Affairs, &amp; designated safety and industrial hygiene, public works, public affairs, and supply/logistics personnel.</td>
</tr>
</tbody>
</table>

Personnel categories as defined by reference (p).

(4) Entry Control Standard 4: Key and Essential Personnel. Access control policy and procedures at FPCON CHARLIE and DELTA and other major incidents (hurricanes, etc.) must be consistent with increased vigilance and security. The
AT Plan shall identify essential personnel consistent with EM Personnel Categories as outlined in reference (p) and identified in Table 4-2. Successful key and essential management is an element in helping to minimize traffic congestion associated with higher FPCONs by clearly identifying authorized personnel.

(5) Entry Control Standard 5: Entry Control Point Categories. ECP new construction or major modifications (50% or more) should utilize reference (aa) for the specific purpose of ensuring positive access control. ECP categories shall be based on intended function and anticipated usage. The following classifications are consistent with reference (aa) and allow for consistent planning and employment of access control procedures. Table 4-2 will be used in conjunction with the tiered capabilities outlined in Access Control Standards 6 and 7. All perimeter ECPs must be capable of processing vehicles and pedestrians in an efficient and effective manner, including appropriate inspections during varying FPCONs.

<table>
<thead>
<tr>
<th>Use Classification</th>
<th>Operational Hours</th>
<th>FPCON Considerations</th>
<th>Preferred Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>24/7 (open continuously)</td>
<td>Open through FPCON DELTA where required by higher authority</td>
<td>Vehicle registration/visitor pass capacity. Regular operations, visitors with authorization. May also be designated as the commercial vehicle inspection station.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Regular hours, closed at times</td>
<td>Potentially closed at or above FPCON CHARLIE</td>
<td>Regular operations, visitors with authorization. May also be designated as the commercial vehicle inspection station.</td>
</tr>
<tr>
<td>Limited use</td>
<td>Only opened for special purposes</td>
<td>Closed at most times</td>
<td>Tactical vehicles, hazardous materials, special events, etc.</td>
</tr>
<tr>
<td>Pedestrian access</td>
<td>Varies</td>
<td>Potentially closed at or above FPCON CHARLIE</td>
<td>Personnel only. May be located near installation housing areas, near schools, or as part of primary or secondary ECP.</td>
</tr>
</tbody>
</table>

(6) Entry Control Standard 6: Operational Access Control Requirements. Access control capabilities shall be established based on installation criticality as well as FPCONs using individual commander’s policy. These capabilities shall be a part of a region-based approach that lends itself to interoperability not only among installations in a region but across regions and other service installations.
(a) ROC levels shall be the foundation for plans and procedures pertaining to access control. Lower ROC designations reflect lower criticality and an increased willingness to accept risk. Access control requirements are progressive in nature and built on previous FPCONs within specific ROC designations.

(b) Region Commanders and Installation Commanding Officers may require additional security based on installation criticality, FPCONs, and GCC guidance. This condition-based access control allows flexibility in providing varying levels of protection based on a risk-based strategy. Additional security requirements will be consistent with regional plans and CNIC guidance. Requirements imposed as a result of GCC guidance will be specifically identified in protection plans.

(7) Entry Control Standard 7: Visitor Control Center Standards. VCCs shall have capability to issue temporary credentials to all individuals and vehicles who are authorized to access facilities but who do not meet the requirements to be issued a CAC or vehicle decal. Additional rationale for issuance of temporary credentials shall be left to the discretion of the REGCOM/CO and shall be in writing. VCCs shall have capability to notify appropriate LE of suspicious activities and/or individuals. VCC shall visibly post information concerning Search Authority (Internal Security Act of 1950, 50 USC § 797) and Implied Consent policy (consent to a chemical test of blood, breath or urine for the purpose of determining the alcohol/drug content of his/her blood) in the VCC facility and web site where applicable.

(8) Entry Control Standard 8: Contracting Officers (KO) and Single Source Coordinators. KOs and SSCs shall include the guidelines contained in this enclosure as a part of solicitations, contracts, and agreements. Existing solicitations, contracts, and agreements should not be modified until renewed.

(a) The KO or SSC shall have oversight of the registration and clearance of vendors, contractors, taxicab, limousine, and shuttle services and drivers who are authorized to conduct business on the installation. Both the KO and SSC shall be authorized by the REGCOM or CO to act as the approval authority for the business entity operating in a region or on an installation. The KO or SSC shall monitor and ensure that vendors meet the requirements of this instruction before credentials are issued.
(b) The KO or SSC as appropriate shall liaison between the Installation Security Detachment and the contractor, including the following:

1. Official notification of contractor about company and employee status.

2. Request reporting as required by Security Detachment.

3. Collect revoked credentials within one working day of notification by the contractor or the Security Detachment of employee status change.

4. Ensure that the contractor is eligible to be authorized access before initiating efforts with the Installation Security Detachment (ISD).


(a) Emergency access control procedures and policy must be consistent with and address the requirement for established and viable means to allow rapid authentication and access for Category 5 personnel in times of crisis. There may be times where contractor response is crucial to preserve and/or restore critical facilities. Procedures shall be promulgated and implemented at each installation. Emergency access procedures shall permit contractors quick access without compromising installation security.

(b) Access for special events, circumstances, or activities entry (i.e. fleet week, air shows, ceremonies) shall be determined by the installation commander, be consistent with DoD and Navy protection policy, include formal coordination with the installation TWG and will include compensatory security measures.

(c) Installation Commanders will not authorize support for public events where the installation FPCON requirements cannot be met and sustained.

0409. NAVY COMMERCIAL ACCESS CONTROL SYSTEM (NCACS)

a. The NCACS is the standard identity management and perimeter installation access control solution for the access
management of vendors, contractors, suppliers and service providers who are not authorized a CAC.

b. Background and Concept of Operations

(1) Reference (a) provides over-arching Navy policy, guidance, information, procedures and responsibilities for the Navy Physical Security and Law Enforcement Program. The NCACS is an operational application of Navy security and law enforcement policy. It operates on the principle of driver, rather than cargo, verification with each access request.

(2) The NCACS identity management and perimeter installation access control solution is specifically designed to manage recurring vendors, contractors, suppliers and other service providers who are not authorized a CAC. It uses the following concept of operations:

(a) NCACS is a voluntary program in which participants who enroll and are subsequently approved for access by the installation are not required to obtain a new pass from the Base Pass and Identification Office for each visit and other than for RAM or in the case of an elevation of FPCON no commercial vehicle inspection is required.

(b) A credential is issued and base access granted once the enrollee passes vetting standards which may include a National Sex Offenders Database, local and regional debarment list/data base, and a National Crime Information Center (NCIC), if the capability exists, background check prior to distribution of the card. Appendix H provides specific vetting standards and credential issuance procedures.

(c) The process of vetting, the maintenance of databases, the creation of credentials, and the technology required for authentication will be provided by a service contractor under the NCACS.

(d) Government costs to implement the NCACS are minimal and consist of providing to the service contractor electrical power, analog phone lines and space for registration station kiosks at the Pass and Identification Offices.

(e) The majority of the NCACS costs are borne by the commercial vendors/contractors who require access to the installation and participate in the program, through fees paid to the service contractor.
(f) Costs to Vendor participants are recaptured through increased productivity of their employees due to the reduction of waiting times, and multiple visits to the Pass and Identification Offices and ECP.

c. NCACS Objectives

(1) Standardize the process across CNIC/Region/Installation to enroll, vet, credential and electronically control access privileges of non-CAC vendors/contractors requesting to access an installation.

(2) Improve efficiency and effectiveness at Pass and Identification Offices through a reduction in the issuance of routine business passes and other locally produced credentials.

(3) Comply with best security practices and Defense Information Assurance Certification and Accreditation Process (DIACAP) information assurance (IA) controls and prohibits the storage of Personally Identifiable Information (PII) on mobile devices.

(4) Ensure perimeter installation access control management in near real time: by individual (with biometric authentication of identity) and company; privileges by time of day, day of week and by installation (one or more as authorized).

(5) Remain responsible for program enrollment and background screening.

d. Responsibilities

(1) Each Region will establish a NCACS POC to the CNIC N61 Regional Support to CNIC N3 at (202) 433-2845.

(2) Each Installation will establish a NCACS SOP and Post Orders using Appendix H, CNIC NCACS SOP as a template.

(3) Installations will maintain a 1-day Visitor Pass program for those non-CAC vendors/contractors who choose not to enroll in the NCACS.

    (a) Installations will ensure, as per local implementing SOPs, that Visitor Passes are issued in compliance with Federal, DoD, DON and CNIC guidance.
(b) Local Commanders are responsible for determining what level of future resourcing is required for Pass and Identification Offices in the event that NCACS results in reducing the demands upon such offices.

e. Service Contractor

(1) As stated above, NCACS program performance and administration will be accomplished through a service contractor.

(2) The current service contractor is EID Passport Incorporated, Portland, Oregon.

(3) EID Passport, Incorporated, will utilize the RAPIDGate system to accomplish vetting, credentialing, and authentication.

(4) In the event that new or additional service contractors are selected to administer NCACS, notice will be provided.

f. Records Management. Records created as a result of this process, regardless of media and format, shall be managed in accordance with SECNAV 5210.1, Navy Records Management Manual.

g. Forms and Reports. The NCACS produces a Monthly Activity Report for each installation which provides an overview of active companies, participants, ingresses by ECP and other useful information for purposes of managing the program.

h. Predecessor Names. Previous designations of the NCACS have included “RAPIDGate” and “Non-Common Access Card Credentialing for Vendors/Contractors” (NC3VC) Program, and “Navy Quick Credentials” (NQC) Project. All references to previous names and titles of the NCACS System are to be updated and corrected to conform to current usage.

0410. DoD Identification Cards, Badges, and Smart Cards

a. The CAC shall be issued to active duty uniformed service members, selected Reserve members, members of the selected Reserve and National Guard, DoD civilian employees (GS, WG, AD, and NAF), eligible contractors and may be issued to retired DoD civil service employees per reference (dd). Contractor personnel will not be issued a CAC until a need arises for an
electronic card to gain physical access to controlled areas or logical access to Navy Marine Corps Internet (NMCI). Family members, retirees, and disabled American veterans will continue to use the standard DoD ID card and not be issued a CAC. Reference (a) contains policy and procedures for issuance and control of various DoD personnel ID cards, badges, and smart cards.

b. DoD Forms of ID Cards

(1) The CAC is the standard ID card issued to permanent employees. The military ID card is unique to DoD.

(2) DoD Building Pass (DoD Form 1468) and Temporary Pass (DD Form 2249) are ID cards issued for a designated period up to two years to temporary employees and contractors having no other appropriate form of identification and whose duties require their recurring official access to federal buildings during business and/or security hours.

(3) Retiree ID Card (DD Form 2) is issued to retired military employees.

(4) Other forms of DoD identification may be developed by REGCOMs, COs, and facility security officers for controlling access to a single or specific building or facility within a building or for Non-DOD civilians who reside in PPV housing within the installation. These ID cards shall not be used in place of authorized departmental ID cards and/or badges.

c. Issuing Authority. DoD ID cards may not be possessed or used unless approved by commanders and issued by a designated issuing authority. RSOs and ISOs may delegate this authority to field activities and designated officials.

d. Possession. Every person except those under the age of 12 years is required to carry a form of approved ID while on an installation.

e. Any misuse of an ID card or badge, including repeated loss or failure to carry while on duty, may result in retrieval of the card/badge, revocation of privileges, or administrative or criminal action. All ID cards and badges remain the property of the U.S. Government.

f. IAW reference (dd) if the CAC is lost or stolen, the holder shall be required to present documentation from the local
security detachment or CAC sponsor confirming that the CAC has been reported lost or stolen. The card issuer will then verify the cardholder’s identity against the biometric information stored in DEERS and confirm the expiration date of the missing CAC, prior to reissuance.

g. Other Agencies' Passes and Credentials. In addition to DoD ID cards, other credentials may be recognized and honored for admission to a facility. Bearers must present accredited identification and be on official business, and local security procedures must not prohibit entry.

0411. DoD Decal Program

a. All Navy-controlled installations shall continue to issue and use DD Form 2220 IAW reference (cc) to register POVs operated on the installation. Installations OCONUS are not required to issue and display the DD Form 2220 as an AT measure. When coexisting with another service that may not require the DoD decal, personnel assigned and working in a Navy facility shall display a decal. COs shall ensure that the Consolidated Law Enforcement Operations Center (CLEOC) or its successor system Pass and ID module is used for issuing DD Form 2220 and shall provide an online renewal capability. Temporary passes may be issued under rules established by the REGCOM or CO when conditions merit or when the VCC is closed.

b. All personnel applying for or renewing their vehicle registration decal shall be vetted IAW the SORNA. The website http://www.nsopr.gov will be used to determine whether a person is a registered sex offender. Registered sex offenders will be denied a DD Form 2220 and reported through the chain of command to the REGCOM and regional SJA.

c. Online Decal Renewal System. The online system is designed to standardize processing and decrease costs by reducing the manpower needed during normal business hours to process vehicle decal renewal requests. Requesting a vehicle decal via a secure website allows the decal user to save time, creates shorter wait times at Pass and ID Offices, and helps to increase productivity by shifting request processing to off-peak hours.

(1) The Regional Authorizing Official (RAO) for the Online Decal Renewal System shall have overall responsibility for maintaining that region's data and records and training...
decal processors. The RAO position should be performed by Non-Guard Services personnel.

(2) Under this program the RAO will serve as the region's primary POC on all matters relating to this program and align decal renewal regional policies and personnel duties with CNIC policy. The RAO shall provide all needed and pertinent information concerning the system to the system administrating official or decal processor and advise the administrator of any desired changes/additions to documentation.

(3) Base/Central Processing Site Authorizing Official. The Base Processing Authorizing Official (BPAO) will serve as a local contact overseeing the installation's decal renewal process. The BPAO position should be performed by Non-Guard Services personnel. The BPAO shall be the POC locally for any system malfunctions and perform as the decal processor.

(a) As the decal processor, the BPAO will verify submitted user information, contact decal users when additional information is needed, and process online requests. The BPAO will inform the decal user if the online renewal request cannot be finalized, or if the request is good and finalized, the BPAO will mail the decal and application information/instructions to the decal user.

(b) The decal processor shall update CLEOC or its successor system.

(4) Online User Requesting Decals. The online user will complete the initial vehicle registration with the region/installation or appropriate DoD organization and use the online system to renew vehicle decals. Users may renew vehicle decals in person at region or installation VCCs but are encouraged to use the online system.

0412. Deviation Process

a. Whenever mandatory security requirements contained in reference (a) cannot be met, commands shall enter the discrepancy into CVAMP and request waivers or exceptions from Deputy Chief of Naval Operations for Fleet Readiness and Logistics (N4) via the chain of command. All commands accepting a higher risk than established through Navy-prescribed AT standards or the Physical Security and Law Enforcement standards must implement a deviation request.
b. Deviation requests will be submitted IAW reference (a) utilizing the OPNAV Tasker System (TASKERS) on the Secret Internet Protocol Router Network (SIPRNET).


0413. Harbor Patrol Unit/Harbor Security Boat (HPU/HSB)

a. HPU/HSBs are programmed through the Office of the Chief of OPNAV N46 in a coordinated effort which include CNIC (N3AT) Force Protection and (N31) Port Operations, with technical guidance from Naval Sea Systems Command (NAVSEA) (PMS 325).

b. Requirements. In general, requirements are driven by the criticality of the asset to be protected IAW reference (a), which describes asset priorities and the security measures to be established for each.

(1) HSBs are required and assigned to protect afloat assets in waterfront restricted areas/exclusion zones and not to patrol or enforce waterside perimeters where no assets are home ported. Over time, requirements for HSBs should be reduced by implementation of secure enclaves using Port Security Barriers (PSB) and detection technology.

(2) While COs are responsible for asset protection at Navy installations, the U.S. Coast Guard Captain of the Port (COPT) CONUS has overall responsibility for port security IAW reference (ee). OCONUS, the SOFA with the Host Nation addresses the jurisdiction and authority for port security.

(3) Reference (ff) establishes the requirements for security force personnel, patrol boats, and security related equipment for Waterfront Restricted Areas and Nuclear Weapons Storage Areas. Strategic Weapons Facility (SWF) Commanding Officers are responsible for the operational employment of these security forces and security patrol boats.

c. Acquisition. Per reference (gg) NAVSEA (PMS 325) shall purchase, procure, acquire, or otherwise obtain all boats for operational use. Acquisition of boats is accomplished using Other Procurement Navy (OPN) funds. In addition to outright purchases, future acquisition methods may include leases or turnkey contracts.
d. Law Enforcement. If enforcement of a restricted area by Navy HSBs results in a Law Enforcement situation, U.S. Coast Guard or Host Nation LE personnel shall be called.

e. REGCOMs have budgeting and funding responsibility for boats assigned to subordinate activities.

0414. Active Vehicle Barrier Procedures. IAW reference (hh) requirements, REGCOMs and COs should ensure physical protection systems, which includes active vehicle barriers, are implemented and codified in regional and installation instructions and/or SOPs.

a. Applicability. The following directs standardized procedures for the execution of barrier operations, and outlines responsibilities of commanders in mitigating the physical security vulnerability of our installations. In overseas locations GCCs and NCCs may direct deviation from the policies regarding barrier protection where local conditions, treaties, agreements, and other arrangements with foreign governments and allied forces require. Included herein are procedures for the use of passive and active landward barriers and waterside barrier systems for the protection of resources located on installations. Nothing in this section abrogates the authority or responsibility of commanders to apply more stringent security standards required by other DoD commands during emergencies, increased threats, high-risk periods or as the commander deems necessary. Different barrier placement applies in all FPCONs. Commanders should strengthen barrier use procedures in response to higher FPCONs as appropriate.

b. Background. IAW reference (hh), PS is a primary command responsibility. The physical barrier program is that part of an installation’s AT Plan focused on the employment of active and passive systems to prevent access to installations in order to mitigate threat vulnerability and reduce reliance on fixed and/or response security forces.

(1) Barrier systems are an effective measure against unauthorized vehicle/personnel entrance to installations and are intended as a force protection multiplier in the commander’s installation protection plans.

(2) This guidance:

(a) Provides barrier use and general procedures that are realistic, harmonize with other installation disciplines,
and provide the necessary flexibility for commanders to protect the installation from terrorists, criminal activity, and other subversive or illegal activity while ensuring its ability to meet all operational tasking.

(b) Ensures coordination of barrier procedures with installation operations (including port and air operations), LE, AT, fire and emergency response, and safety programs to provide an integrated and coherent effort.

(c) Establishes training requirements and standards for security forces and affected audience communities.

c. Policy.

(1) Commanders protection plans during all FPCONs, shall fully incorporate the use of available barrier systems (both active and passive).

(2) Deployment of active (i.e., pop-up and bollard) barriers is a logical step in the escalation of force against an unauthorized entry attempt. Active barriers, if available, shall be deployed to prevent access of unauthorized vehicles.

(3) Barrier systems must be operated and maintained on a routine basis.

(4) Barrier system inoperability shall be reported to operational commanders, CNIC N3AT, and the cognizant REGCOM via OPREP reporting procedures IAW reference (ii) and entered into DRRS-N.

d. Responsibilities. CNIC shall develop training, qualification, and readiness requirements for personnel tasked to install and operate barrier systems.

(1) REGCOMs shall:

(a) Ensure the development of a regional policy which includes procedures and instructions describing the use of a full range of barriers to prevent, delay, or impede intruders in their efforts to reach their objective at each installation within their operating environment.

(b) Oversee the uniform execution of this policy.
(c) Determine additional direction necessary to implement these procedures.

(d) Make recommendations for updates to this policy when appropriate.

(2) COs shall:

(a) Implement this policy as directed.

(b) Develop procedures and instructions describing the use of a full range of barriers to prevent, delay, or impede intruders in their efforts to reach their objective.

(c) Incorporate this policy into applicable installation protection plans and RAM procedures.

(d) Incorporate this policy into SOPs of all installation and tenant activities.

(e) Implement a training program to ensure all assigned personnel understand capabilities and limitations of the barrier systems, and are fully trained in barrier operations, responsibilities, and procedures. At locations where contract guards man the ECP, also ensure that the company providing the service is advised of training requirements. The training program shall include barrier activation procedures (both routine and extreme situations), use of force, and decision making as outlined in post orders.

e. Procedures for landward barriers and obstacles shall be employed at ECP to control traffic flow. Barriers should be illuminated to provide easy observation.

(1) Active barriers (i.e., pop-up bollard) are a logical step in the escalation of force against an unauthorized entry attempt. While verbal commands, whistles, and sirens should be the primary method of notifying a vehicle of the need to stop, when these commands or indications do not result in the vehicle stopping, the barrier shall be activated. Security ECP personnel must clearly understand authorized deployment procedures in emergency situations, such as vehicles disregarding posted speed limits, stop signs, verbal commands and no indication of intent to slow or stop and the difference in nonemergency situations such as lost or confused motorists.
(a) Installations shall maintain active barriers, deployed in the up position, during low vehicular traffic periods and whenever ECP gates are closed.

(b) ECPs with active barriers shall be marked with warning signs and reduced speed limits.

(2) Passive Barriers.

(a) ECPs not equipped with an active barrier system shall, during low vehicular traffic periods, erect passive barriers (i.e., jersey barriers, water-filled barriers, or serpentine obstacle patterns) to force vehicles to slow down and make sharp turns, thus providing sentries both protection and time for observation and decision making while exposing potential unauthorized drivers to capture or other security response in accordance with the use of force continuum.

(b) Available barriers should be deployed at both inbound and outbound lanes of traffic.

f. Procedures for waterside barriers.

(1) Waterside barriers shall remain closed/intact, shall be opened only as required for authorized access, and shall remain opened only for the minimum necessary time. It is incumbent on fleet units and port operations program to coordinate to the maximum extent possible the scheduled opening and closing of the barriers.

(2) Barrier opening, while performed by port operations, shall be coordinated with installation security.

(3) To maximize standoff, waterside barriers should be placed as close as possible to the Waterside Restricted Area (WRA).

(4) Mooring buoys shall be lighted, and barriers shall be painted to maximize visibility.

0415. Crime Prevention. Crime prevention is a proactive method of reducing criminal opportunities, protecting potential victims, and preventing property loss. Each installation shall assign a Crime Prevention Coordinator to plan and coordinate crime prevention functions. As the result of the OMB Circular A-76 study, in CONUS, this coordinator function is now under the purview of the CNIC N3AT NGS Support Services structure. OCONUS
the function is performed by NSF personnel. Functions include but are not limited to the following:

a. Promulgate an SOP delineating preventative measures to deter crime onboard the installation.

b. Liaison with NCIS and local authorities to identify off-base areas where personnel are more likely to become a victim of a crime. When merited, recommend to the chain of command areas that should be "off limits", and include the SJA in this review.

c. Track criminal trends both onboard the installation and in the surrounding areas.

d. Maintain active liaison with NCIS and local LE agencies.

e. Participate in local crime prevention meetings and initiatives.

f. Advise chain of command and NCIS of observed trends and analysis information.

g. Research and ensure the installation participates in National Crime Prevention Council awareness programs and other initiatives.

h. Plan and execute Navy-specific programs regarding crimes prevalent in the local area or identified as concerns on the installation.

i. Prepare briefs for use by NSF and provide this information at roll calls and department head meetings and to tenant commands to raise awareness to local crime trends.

j. Conduct crime prevention surveys onboard the installation for housing areas, including bachelor housing, industrial areas, MWR facilities, and common-use areas and report findings and recommendations to appropriate parties. Compliance with all PPV rules for housing will be followed. Checklists should be adapted to local conditions. For checklist examples refer to Appendix C.

k. Administer the Operation Identification Program (Operation ID) for the region/installation.

(1) Operation ID consists of marking personal property with a unique owner applied number to assist in identifying,
recovering and returning stolen property to the rightful owner. Criminals often remove or obliterate serial numbers of stolen items.

(2) In addition to maintaining a list of personal property that includes make, model, description, and serial number, in a separate location from the actual property; police and public safety departments nationwide advise marking personal property with a personal identification number. The preferred method is a driver’s/operator’s license number (OLN) entered as the two letter state abbreviation followed by a slash and then their personal OLN, e.g., PA/12345678. (Do not use social security numbers due to PII issues.)

(a) A recommended method for marking items is by engraving or using permanent or ultraviolet ink which can result in identifying rightful owners.

(b) The NCIC has a field for Owner Applied Number (OAN) that can be entered into their data base to assist in identifying stolen property.

(c) Agencies that have access to the National Law Enforcement Telecommunication System (NLETS) can access state Driver’s/operator’s data systems and, with an OLN (or state identification number for persons that do not have a driver's license), can identify the name and address from the OLN and facilitate return of lost or stolen items.

1. Appendix C contains various examples of Crime Prevention Checklists that can be modified and adopted for local use. The checklists include examples for residential, personnel security, building security, and person property identification checklists.
CHAPTER 5
LAW ENFORCEMENT

0501. Responsibilities. REGCOMs and COs have an inherent responsibility to provide maximum protection for their installations and to all military, civilian, and contractor personnel located on their installations and/or property. In addition to AT and PS planning and execution, a robust and professionally executed LE Program is required to maintain good order and discipline. The CO is responsible for the operational control of the NSF and the ISO, while administrative and resource management resides with the RSO.

a. The REGCOM, CO, and ISO, in close coordination, shall develop MOUs/MOAs with local, state, and federal entities as they relate to the LE functions of the installation. Coordination will also include N8. In overseas locations, rules and policies in accordance with the SOFA and rules of engagement (ROE) per reference (f) will be followed in strict compliance.

b. Law Enforcement is primarily accomplished by NSF using accepted principles to enforce the Uniform Code of Military Justice (UCMJ) and local state or county statutes applying the Assimilative Crimes Act, 18 U.S.C. § 13. LE may be accomplished by Navy MAs and civilian employees classified as NCP GS-083 series. Contract guards are not authorized to perform inherently governmental duties, including LE.

c. Authority.

(1) Rule 302(b) (1) of the MCM 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 CO 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.

(4) 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.

(5) On duty NCP and SG personnel are considered part of the DON, therefore, are subject to the restrictions on aid to civilian law enforcement imposed by 18 USC 1385, commonly referred to as the Posse Comitatus Act. Accordingly, any proposed aid to civilian law enforcement must be reviewed by the servicing SJA.

(6) NCP jurisdiction and authority to perform law enforcement duties are valid while performing these duties during their official work hours only. An on-post apprehension conducted by NCP in an off duty status is a detention by a private citizen. NCP will not carry Navy weapons while off duty and are not authorized to store Navy weapons at a private residence. Navy weapons must be stored in an authorized storage facility. NCP, while on duty, will not carry privately owned weapons or privately owned ammunition. The carrying of privately owned weapons on board an installation by off duty NCP will be in accordance with policy established by the CO.

(7) The duty uniform and badge may be worn only while on duty or while traveling to and from work as determined by the ISO.

d. Navy Security Force personnel, while performing LE or security duties in an official Navy capacity are not authorized to perform duties as local police, sheriff, or any other LE official. This applies on and off a Navy installation. Because of potential conflicts of interest and Posse Comitatus Act
issues, it is Navy policy that NCP/SG will not be deputized or exercise any additional authority or jurisdiction granted by local, state, or federal governments to perform law enforcement duties on or off a military installation or facility while wearing the duty uniform and/or badge.

(1) IAW reference (jj), any existing cases of deputizing Navy uniformed law enforcement personnel by state and local governments that have not been approved by the Secretary of the Navy are invalid.

(2) Requests for an exception to this prohibition will be submitted IAW reference (jj). The approval authority is the Secretary of the Navy.

(3) This prohibition does not apply to NCP/SG employed while off duty by local, state, or federal governments.

e. The CO, after consultation with the servicing SJA and the ISO, will provide all personnel who perform law enforcement and security guard functions on the installation, to include any non contiguous installations, specific written guidance on:

(1) Their authority (specific empowerment and limitations) and jurisdiction.

(2) Procedures for suspending and withdrawing their law enforcement authority.

(3) Procedures shall be established to ensure all personnel who perform law enforcement and security guard functions acknowledge, in writing, a clear understanding of their jurisdiction and authority. Written instructions will be reviewed at least once a year and updated, if necessary.

f. REGCOMs shall promulgate guidance and policy for COs to incorporate into their protection planning process. Ultimately, the CO will be responsible to publish protection plans and LE SOPs addressing all aspects of LE as it applies to the installation. In addition to reference (a) policy, the following area shall be addressed.

g. Preplanned Responses (PPR) are developed, exercised actions and measures that are implemented to identify, track, assess and neutralize terrorist attacks. Regional Security Officers and ISO’s shall develop, as part of the overall planning process, PPR’s to address threats to personnel and
assets on-board Navy installations. In addition to PPR’s described in references (m) and (n) some additional examples are as follows:

(1) Bomb Threat
(2) Unauthorized Entry
(3) Improvised Explosive Device (IED/VBIED)
(4) Hostage Situation
(5) Chemical Biological Radiological Nuclear (CBRN)
(6) Anti-Swimmer
(7) Small Boat Intrusion
(8) Demonstrators
(9) Active Shooter

h. Active shooter Planning

(1) Shooting incidents by an individual or multiple individuals demonstrate the need for special attention to “active shooter” response. NSF initial and sustainment training address various scenarios which require various responses.

(2) Emphasis should be placed on ensuring NSF personnel adhere to Regional and Installation PPR’s, involving an active shooter, to reinforce the following

   (a) Timeliness to neutralize the threat in order to prevent further injury or death to innocent bystanders.

   (b) Neutralizing the threat to minimize further damage to assets.

(3) The RSO/ISO shall ensure all NSF personnel are briefed on PPR’s concerning active shooter. The active shooter situation, while different from many other responses, should still be deemed a “response”, which shall adhere to not only the PPR, but standard response protocol.

(4) Standing Rules for the Use of Force/Rules of Engagement (SRUF/ROE) will be included in the PPR and briefed to
all NSF personnel prior to exercising an active shooter scenario.

(5) Singling out this particular type of response is in no way intended to diminish the importance of other responses, but rather to emphasize the importance of neutralizing an active shooter.

0502. **Traffic.** Each CO will establish an effective traffic supervision program for the installation per reference (cc). As part of this program, COs may adopt state or host-nation traffic violations under the Assimilative Crimes Act.

a. Members of the NSF who are authorized to perform LE duties shall enforce traffic laws onboard Navy installations. Only two types of traffic tickets are authorized for violations: DD Form 1408 (Armed Forces Traffic Ticket) and DD Form 1805 (U.S. District Court Violation Notice). At no time shall any member of the NSF use local city, county, state, or host-nation tickets for traffic violations.

b. COs shall establish procedures for adjudicating traffic violation cases through administrative or judicial action consistent with the UCMJ and federal law.

c. In all cases where a traffic citation is issued (including written warnings) the NSF shall ensure a copy is provided to the service member’s chain of command. If a military family member is issued a traffic citation, a copy shall be routed through the sponsor’s chain of command. In the case of a civilian employee, a copy shall be provided to the supervisor or employer in accordance with local SOP. If there are insufficient copies of the preprinted traffic citation to accomplish this task, the NSF member issuing the ticket shall make copies to ensure compliance. The CLEOC, or its successor system, ticket module may be used for this requirement.

0503. **Driving Under the Influence of Alcohol/Drugs.** NSF shall be alert to any person operating a motor vehicle on an installation while under the influence of alcohol or drugs. Persons operating a motor vehicle on a military installation shall be deemed to have given their consent to one or more evidential tests for alcohol and/or other drug content of their blood, breath, or urine when lawfully stopped, apprehended, or cited for any offense allegedly committed while driving or in
physical control of a motor vehicle to determine the influence of intoxicants.

a. Procedures for measuring and determining blood alcohol content or presence of drugs shall be in conformance with those approved by the state or host nation where the installation is physically located. All devices that measure such readings shall be calibrated and tested in accordance with state or host-nation regulations.

b. NSF shall have RRP to ensure vehicles owned by individuals detained or apprehended for driving under the influence (DUI) are turned over to a sober driver with consent of the owner, secured at the scene, or towed to a secure impound location. When the violation involves intoxicated driving, a copy of the ticket shall be reproduced and forwarded to the installation alcohol and drug abuse facility.

0504. **Traffic Accident Investigations.** The purpose of investigating a motor vehicle accident is to determine causal factors, which include but are not limited to driver violations committed which led to the accident, vehicle equipment failure, roadway hazards, and environmental factors. The completed investigation report may possibly be used in criminal or civil action; therefore, attention to detail is vital.

a. Patrol personnel shall use the CLEOC, or its successor system, collision module to document investigations on all motor vehicle accidents occurring on the installation, except those involving fatalities. Fatal vehicle accidents require notification of NCIS and shall be investigated by properly trained and authorized personnel from within the command or local or state authorities. Fatal accident scenes shall be treated the same as major crime scenes and require NCIS notification.

b. The assigned investigator shall obtain all data from involved drivers, passengers, pedestrians, and vehicles which will include taking pictures of the accident scene. Use witness statement forms as applicable to scan into CLEOC or its successor system. The investigator shall take appropriate enforcement action by issuing written warnings or traffic tickets upon completion of the investigation.

0505. **Selective Traffic Enforcement Program (STEP).** A STEP program shall be implemented by each region/installation when practical. IAW reference (cc), selective enforcement deter
traffic violations and reduces accidents by the presence or suggested presence of law enforcement personnel at places where violations, congestion, or accidents frequently occur. Selective enforcement applies proper enforcement measures to traffic congestion and focuses on selected time periods, conditions, and violations that cause accidents. Law enforcement personnel use selective enforcement because that practice is the most effective use of resources.

a. The ISO should coordinate with the local Safety Office to determine the most frequent causal factors, locations and hours when accidents occur. The CO/ISO will assign increased patrols to these areas to specifically enforce the targeted violations. STEP increased patrols should result in a heightened awareness of violations and safer driving habits as well as a decrease in traffic accidents. STEP patrols should not be utilized for routine functions during the program operation. STEP patrols may be roving or traffic safety checkpoints.

b. A public affairs program utilizing the Plan of the Week and other region/installation resources shall be launched informing personnel that saturation patrols will be operating. The location and time of the saturation patrols will not be made a part of the news release.

c. STEP patrols will stop all observed violators but shall concentrate on the target violations during the scheduled STEP saturation. Typical target violations are:

(1) Driving under the influence/while intoxicated
(2) Excessive speed and aggressive drivers
(3) Failure to yield right of way
(4) Following too closely
(5) Using cell phones and other electronic devices while driving
(6) Not using restraint and safety systems (seat belts/shoulder harness/approved child safety seats and helmets;
(7) Unsafe equipment (tires, lights, wiper blades, etc.)
d. When taking enforcement action or otherwise interacting with any driver during the STEP saturation patrols, every patrol shall engage in a safety dialog pre-approved by the ISO with the driver and/or pass out traffic safety handouts. Handouts are often available through the National Highway Traffic Safety Administration (NHTSA). The Navy Safety Center is a valuable resource for statistical data and obtaining public information flyers for use in the STEP program. Additional information can be obtained through the NHTSA website http://www.nhtsa.dot.gov/.

0506. Criminal Investigations

a. The purpose of a criminal investigation is to determine what criminal act may have been committed, identify the victim(s), determine who committed the act, and take appropriate actions to adjudicate the responsible person.

b. IAW reference (kk) NCIS has primarily responsible for investigating major criminal offenses, including espionage and acts of terrorism. A major criminal offense is defined as any offense punishable under the UCMJ, or similarly framed federal, state, local, or foreign statutes, by confinement for a term of more than one year. When NCIS is not available or declines to investigate a criminal offense, Command Criminal Investigators (CCI) shall be tasked to complete and document all investigative procedures taken. All criminal investigations conducted by the CCI’s onboard an installation shall be reported in the CLEOC, or its successor system, using the Incident Report module.

c. NCIS shall establish guidelines to determine the category of criminal incidents which will be referred to them. These guidelines will also describe actions when a case is declined to include.

(1) Identify the Special Agent who declined the case.

(2) Identify the person to who he declined.

(3) Time and date case was declined.

(4) Identify the CCI who was assigned the case.

(5) Brief explanation of why the case was declined.

(6) Any other information deemed necessary to support the transfer of responsibility from NCIS to installation CCI.
d. If NCIS declines the investigation or the level and type of criminal act does not meet standards set by the RRP, a member of NSF, normally a CCI, shall be assigned to conduct the investigation. Where Regional Investigative Coordinators (RICs) exist, investigative procedures shall be in accordance with the NCIS RIC-mandated Investigator's Handbook or as directed by local RRP.

e. Contingent upon who assumes the case, the evidence handling, collection and storage procedures will be the responsibility of either NCIS or NSF CCI.

(1) When NCIS assumes the case, the NSF responsibility at the scene is to set a perimeter and protect all evidence for NCIS.

(2) When NSF CCI assumes the case, the evidence handling, collection and storage procedures will be IAW reference (m).

0507. **Desk Journals.** The CLEOC, or its successor system, desk journal shall be completed on all calls for service.

0508. **Crime Statistics**

a. Crime statistics are an important part of determining crime patterns and applying sufficient resources to prevent such crimes. NSF personnel shall utilize the CLEOC, or its successor system, for reporting all criminal incidents.

b. NCIS maintains the central repository for the collection of this data and the ISO shall coordinate with the local NCIS office for analysis of crime trends.

c. The RSO shall compile crime statistics and trend analysis information from their installations on a quarterly basis. See Appendix G for examples of some crime reports and what they should contain. This information shall be provided to CNIC N3AT on both a quarterly basis and as an annual summary report. This analysis will allow for more efficient utilization of resources to combat crime.

0509. **Personal Firearms Safety, Control, and Accountability**

a. IAW reference (a) Change 1, 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 PPV housing), without first obtaining prior written approval of the CO. The provisions of this section do not apply to personnel residing in off-base Navy family housing, including off-base family PPV housing.

b. Personal firearms overseas are governed by applicable Status of Forces Agreements and host nation laws.

c. All personal firearms brought onboard a Navy installation will be registered with the installation security detachment. If another entity such as a Navy armory is designated to process personal firearms registration, the installation security detachment must be notified of such registration.

d. The REGCOM and CO will ensure a process is developed to provide strict control and accountability of personal firearms which include, at a minimum:

   (1) Types of firearms to be registered

   (2) Transportation/transiting procedures for firearms and ammunition on base

   (3) Location and storage procedures for properly registered and authorized personal weapons

   (4) Minimum registration and accountability requirements

   (5) Concealed handgun permit limitations which will include that state licenses or permits to carry concealed handguns are not recognized or valid on Navy installations

e. Violation of paragraph 0509 of this instruction and the applicable section contained in reference (a) Change 1 may subject military personnel to appropriate administrative and/or disciplinary action under the UCMJ. Civilian employees may be subject to disciplinary action or administrative action under applicable civilian personnel instructions. Violations by family members can lead to being barred from the installation.

f. When personnel permanently depart the installation all registered personal weapons must be administratively deregistered with the installation security detachment and the weapon removed from the installation.
g. Duly authorized civilian law enforcement personnel entering a Navy installation on official business may carry their assigned weapon(s).

0510. **Courthouse Security.** The CO is responsible for providing courthouse security.

0511. **Cell Phones and Texting**

a. In accordance with references (ll) and (mm) all military and civilian operators of vehicles on Navy installations and operators of government owned/leased vehicles (including rental cars while on Temporary Assigned Duty) on/off Navy installations shall not use cell phones unless the vehicle is safely parked or unless they are using a hands free device.

(1) This applies to all Navy personnel, civilian employees, family members, contractors, tenants, and visitors, except for fire, emergency, or law enforcement/security personnel operating government owned/leased vehicles using an official communication device on Navy installations.

(2) The prohibition against using handheld cellular phones does not include hands free cellular phone devices. Hands free devices include console/dash mounted or otherwise secured cellular phones with integrated features such as voice activation, speed dial, speakerphone or other similar technology for sending and receiving calls.

(3) Driver use of any portable, personal listening device worn inside the aural canal, around or covering the driver’s ear while operating a motor vehicle, except for fire and emergency response or law enforcement/security purposes, is prohibited. Listening devices include wired or wireless earphones and headphones (including Bluetooth® or similar technology), and do not include hearing aids or devices designed and required for hearing enhancement.

(4) Personnel performing NSF duties will not use personal communication devices when use of these devices interferes with the performance of their duties or creates a safety hazard.

b. Pursuant to the White House Executive Order, reference (mm), text messaging is prohibited for all operators of government owned/leased vehicles (including rental cars while on Temporary Assigned Duty) on/off Navy installations. In
addition, text messaging is prohibited by all military personnel, civilian employees, family members, contractors, tenants, and visitors, while driving on a Navy installation. Fire, emergency, or law enforcement/security personnel, while conducting official business, may utilize authorized computer type keyboards which are permanently installed as part of emergency vehicle equipment. Extreme caution will be used at all times. “Text Messaging” or “Texting” means reading from or entering data into any handheld or other electronic device, including for the purpose of SMS texting, e-mailing, instant messaging, obtaining navigational information, or engaging in any other form of electronic data retrieval of electronic data communications.

c. Enforcement. These procedures shall be enforced by installation security. Violations of this guidance will be subject to actions described in reference (cc) to include administrative actions; reprimand, assessment of points, and loss of on-base driving privileges, may be initiated against persons who violate this policy.

0512. Pre and Post Shift Activities

a. Inherent in the Law Enforcement profession is the pre- and post-shift activity of an officer. All shifts should be designed to allow for a pre-shift briefing commonly referred to as “Roll Call”, where NSF personnel receive law enforcement sensitive information concerning the latest activity on their installation. This may have safety and security implications. This, along with issuance of weapons, shall be considered part of the pre-shift activities.

b. Regions and installations will comply with the rules and regulations pertaining to pre- and post-shift activities for NCP/NSG.

c. Overtime is not to be construed as part and parcel of any shift work except authorized overtime that may result from pre- and post-shift activities. Overtime is reserved for extenuating circumstances where it is unavoidable and if not employed, poses a threat to the security of the installation.

d. The three (3) entities that comprise the NSF; MA, Department of the NCP and guards, and Contract Guard personnel require different guidelines.
(1) Military personnel are on duty 24/7 and overtime does not exist.

(2) NCP and guards are entitled to overtime when circumstances require it. Overtime is not to be construed as part and parcel of any shift work except authorized overtime that may result from pre- and post- shift activities.

(3) Contract Guards will be bound by what was negotiated and agreed upon during the contracting process.
0601. **Purpose.** To provide policy, assign responsibilities and define procedures concerning the administration and management of TOA for CNIC NSF ashore.

0602. **Definitions**

   a. **TOA.** A complete listing of CNIC approved equipment and materiel authorized as allowance for specific NSF units or regions at CNIC installations. The TOA format and codification will remain common for all TOAs developed by CNIC. The NSF TOA will only list materiel, equipment, and supplies identified by the NSF Mission Statement, ROC level IAW reference (c), which support NSF operational requirements.

   b. **Allowance Change Request (ACR).** The process/format used to submit proposed changes to the CNIC approved TOA.

   c. **Enterprise Safety Applications Management System (ESAMS).** A web based reporting system utilized for identifying, inventorying and reporting TOA items. ESAMS shall be the only validated source accounting for NSF TOA metrics values.

   d. **CNIC N3AT Program Director or designated N3AT TOA Program Manager.** Reports directly to CNIC via CNIC N3 Operations Officer and is overall responsible for NSF TOA program management. The Program Manager will be HQ primary liaison with Region Commanders, ESAMS Program Manager and other applicable entities that have an impact on the NSF TOA. N3AT Program Director shall assign a Program Manager to oversee the TOA program.

0603. **Background**

   a. CNIC has engaged the assistance of SPAWAR to develop and implement a standard allowancing system to support outfitting and sustainment of CNIC required AT equipment. CNIC intends to leverage existing SPAWAR infrastructure to rapidly implement an efficient, centralized process for management, procurement and distribution of material. Figure 6-3 outlines the “Material Management and Implementation Process”.

   b. CNIC N3AT is the NSF TOA system manager, responsible for development, modification, and documentation. CNIC N3AT designated representative or Program Manager shall be the
primary point of contact concerning all TOA matters, to include implementation of new requirements, enhancing the design and selection of material, tools and equipment, and other factors leading to the improvement and effectiveness of the NSF TOA. See Appendix E for the list of equipment. Note: This is a list of the basic recommended equipment and is not all inclusive. Any additions by regions, such as specific make and model of equipment, will require N3AT approval.

c. Recommended changes to the NSF TOA are initiated using the ACR form, (Figure 6-1). An ACR may be initiated to identify requirement recommendations based on field experience of NSF units, mission changes, or technology advancement.

d. State of the Art Technological Advances. ACRs involving technical advances or a system stock number change of an existing approved TOA can be approved by CNIC N3AT Program Director and/or TOA Program Manager if the following conditions are met:

   (1) Item does not involve a wholesale change of every like item in the TOA. Record of change will reflect only when new item is introduced as a suitable replacement or part of a phasing in process. Existing useable items will continue to be used until replaced at the end of its service life.

   (2) Change has no significant impact on training requirements.

   (3) Change has no significant cost impact.

0604. Responsibilities

   a. Commander Naval Installations Command N3AT.

   (1) CNIC will host annual NSF TOA conference to address issues, collect and compile ACRs.

   (2) CNIC will review for final approval all validated ACRs submitted via REGCOMs. Validated and approved ACRs will be submitted to the NSF TOA Program Manager for implementation and codification into the ESAMS program of record.

   (3) CNIC NSF TOA Program Manager will ensure that all approved NSF TOA items are accurate in terms of materiel identification, cost and any metric value identified in the ESAMS program. Any changes or modifications that are necessary
to maintain ESAMS integrity will be evaluated, presented to the REGCOM and resubmitted via the ACR process.

(4) The CNIC TOA Manager will analyze reports and provide recommendations to CNIC in all matters related to NSF TOA, including budget requests, risk analysis and other CNIC required reports.

b. Region Commander

(1) Region Commanders will validate all ACRs in accordance with this chapter.

(2) Region Commanders will identify in writing all POCs that will have NSF TOA management authority. Regional TOA managers are responsible for proper evaluation of equipment and materiel, proper inventory reporting by subordinate commands in their region via ESAMs and administrating ACR submission at the regional level.

(3) Regional NSF TOA POCs will participate in an annual review of NSF TOA or when necessary to provide input for their specific region.

c. ISO will maintain accurate NSF TOA inventories in accordance with this chapter. ESAMS will be the official reporting program to reflect current inventory, materiel identification, cost and all other metric values concerning the NSF TOA.

0605. Procedures for Initiating TOA Changes. All changes to CNIC TOAs shall be initiated as follows:

a. Format. ACRs shall be submitted with complete justification for each requested change in a format similar to “CNIC TOA Change Impact Analysis” (Figure 6-1).

b. Justification. Justification for changes shall be based on one or more of the following:

(1) Mission Capability Improvement and Modernization. The proposed change must improve the capability to perform the assigned mission. Proposed changes resulting from changes in a unit's mission should be specifically identified.

(2) ROC. Changes to the ROC may result in the unit's mission capability being substantially revised and should result
in an ACR being submitted to CNIC to conduct an analysis of the affected systems. This review shall identify any offsets or recapitalization of assets being replaced or no longer required.

(3) Cost Effectiveness. The proposed change should address manpower savings or reduce the inventory requirements and the perceived life cycle costs. A brief cost comparison must be included.

(4) Other. The proposed change should result in a non-quantitative improvement such as improved health, welfare, morale, quality of life, etc.

(5) Site Specific. Proposed changes that support site specific operations will be procured using unit O&MN or CNIC funds. Approved TOAs will not be changed to accommodate short term operation specific requirements.

c. Submission. Recommendations involving changes to authorized TOA allowances shall be submitted via the Chain of Command. CNIC will assign a tracking identification number. Additionally, once the tracking number has been assigned, CNIC will maintain the proposed changes on file and act as liaison for status updates. CNIC Program Manager will forward proposed changes to CNIC via REGCOM's for approval.

d. Processing Criteria. CNIC Program Manager shall systematically conduct a systems analysis for all recommended changes using criteria and processes as identified in the “Allowance Change Request” (Figure 6-2) and present all the facts with proposed options as an ACR project summary package. Before presenting the proposed options, the CNIC program manager shall consider:

(1) Reliability, Maintainability, and Flexibility. Technically suited items shall be selected to increase the overall reliability and maintainability of the TOA and minimize the amount of specialized equipment/materiel designed to serve only a limited function.

(2) Life Cycle Costs. Items shall be selected with consideration toward reducing total life cycle costs; including initial procurement, training, operations, interoperability, maintenance, and replacement costs.
(3) Interoperability. Allowances shall be maintained to ensure interoperability of equipment and components among commands within DoD.

(4) Stock Status. Recapitalization against other allowances and/or disposition of stock must be considered if the recommended change will result in excess of equipment or material.

e. TOA Approval. Approval authority for all TOAs rests with CNIC.
### CNIC TOA CHANGE IMPACT ANALYSIS

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Proposal Summary:</td>
</tr>
<tr>
<td>2.</td>
<td>Tracking Number:</td>
</tr>
<tr>
<td>3.</td>
<td>Start Date:</td>
</tr>
<tr>
<td>4.</td>
<td>Due Date:</td>
</tr>
<tr>
<td>5.</td>
<td>Current TOA Information</td>
</tr>
<tr>
<td>6.</td>
<td>Proposed TOA Information</td>
</tr>
<tr>
<td>Line Item</td>
<td>Line Item</td>
</tr>
<tr>
<td>Total Allowance:</td>
<td>Total Allowance:</td>
</tr>
<tr>
<td>Unit Cost:</td>
<td>Unit Cost:</td>
</tr>
<tr>
<td>Extended Cost:</td>
<td>Extended Cost:</td>
</tr>
<tr>
<td>7.</td>
<td>Mission (ROC/POE)</td>
</tr>
<tr>
<td>8.</td>
<td>Supporting Doctrine:</td>
</tr>
<tr>
<td>9.</td>
<td>Safety Considerations:</td>
</tr>
<tr>
<td>10.</td>
<td>Training Requirements:</td>
</tr>
<tr>
<td>11.</td>
<td>Maintenance Requirements:</td>
</tr>
<tr>
<td>Annual Man hours:</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>Test and Evaluation:</td>
</tr>
<tr>
<td>13.</td>
<td>Federal Supply System:</td>
</tr>
<tr>
<td>14.</td>
<td>ILS and Life Cycle Cost:</td>
</tr>
<tr>
<td>15.</td>
<td>Initial Outfit Cost:</td>
</tr>
<tr>
<td>16.</td>
<td>Phase Replacement Plan:</td>
</tr>
<tr>
<td>17.</td>
<td>DLR Cost (if applicable):</td>
</tr>
<tr>
<td>18.</td>
<td>Inter/Intra TOA Impacts:</td>
</tr>
<tr>
<td>19.</td>
<td>Funding Responsibility (resource sponsor):</td>
</tr>
<tr>
<td>20.</td>
<td>Other Options:</td>
</tr>
<tr>
<td>21.</td>
<td>PROS:</td>
</tr>
<tr>
<td>22.</td>
<td>CONS:</td>
</tr>
<tr>
<td>23.</td>
<td>Offsets (i.e., reduction in personnel, reutilization/capitalization)</td>
</tr>
<tr>
<td>Signature:</td>
<td>Approve/Disapprove Date</td>
</tr>
</tbody>
</table>

**Figure 6-1. CNIC TOA Change Impact Analysis**
<table>
<thead>
<tr>
<th></th>
<th>Allowance Change Request</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. FROM:</strong></td>
<td><strong>2. DATE/serial number</strong></td>
</tr>
<tr>
<td><strong>TO:</strong></td>
<td><strong>3. APL/AEL/TOA SECTION NUMBER</strong></td>
</tr>
<tr>
<td><strong>VIA:</strong></td>
<td><strong>4. REQUEST TYPE</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5. NATIONAL STOCK NUMBER (NSN) OR MANUFACTURER &amp; PART NUMBER</strong></td>
<td><strong>6. ESAM ITEM NOMEN-CLATURE</strong></td>
</tr>
<tr>
<td><strong>9. PRESENT QTY ALLOWED</strong></td>
<td><strong>10. QTY ON HAND</strong></td>
</tr>
<tr>
<td><strong>13. JUSTIFICATION (MANDATORY)</strong></td>
<td><strong>14. SIGNATURE:</strong></td>
</tr>
</tbody>
</table>

**Figure 6-2. Allowance Change Request**
Figure 6-3. Material Management and Implementation Process

Develop and promulgate baseline allowance documents and management policy

- Develop installation-specific allowances based on functional FP mission areas (IPE, ECP).
- Develop and promulgate policy and procedures for management, periodic review and allowance changes.

Validate allowance documents by region

- Review baseline allowances with each region to ensure regional and installation-specific peculiarities or concerns are addressed.
- Revise baseline document as necessary to reflect changes from regional reviews.

Establish long term sustainment plan

- Formulate budget to support achievement of allowances and sustainment of program.
- Establish permanent program management, procurement and distribution infrastructure.

Capture region and installation inventory posture via ESAMS

Execute procurement and distribution of known critical equipment shortfalls as funding becomes available

Execute procurement and distribution IAW long term plan

Resources/Priorities

SPAWAR

NAVSEA Contracting Warfare Centers
DOI - Acquisition Services

Equipment

FP Warehouse

Equipment (to Installations & Regions)

Distribution Plans/Priorities
0606. Uniform and Appearance Standards for DON Civilian Police/Security Guards

a. These standards apply to all Navy Civilian Police (083)/Security Guard (085) (NCP/SG) personnel employed by CNIC. When purchasing uniform items, members must ensure that all articles purchased conform in quality, design, fit, and color to the uniform standards and specifications prescribed in this instruction. As representatives of DON, NCP/SG personnel will conduct themselves in a professional and courteous manner at all times. Basic character traits of honesty, courtesy, tact, cooperation, personal appearance, and bearing are important factors required of NCP/SG.

b. Explanation of Terms.

(1) A uniform includes, but is not limited to, articles of clothing or insignias that an employee is required to wear for the purpose of identification while in the performance of official duties. In this instruction, a uniform means articles for which a uniform allowance is paid.

(2) Insignias worn on uniforms are to identify the type of duty performed by the NSF personnel.

(3) Badges, cap devices, holsters (web gear), and weapons are not articles of uniform. Such accessories are furnished by the government and remain the property of the government while in the custody of the employee. These are items which are accountable and will be returned to the security detachment when employment is terminated. Additionally, all professional web gear (holster, ammo pouches, PPE, oleoresin capsicum [OC] spray, baton, flashlight, and handcuffs) will be worn in a standardized manner. This equipment is also classified accountable and will be returned to the security detachment when employment is terminated.

c. Ballistic vests are considered part of the TOA for all armed employees identified within this instruction. Upon issue, these vests shall be worn by all armed uniformed personnel while on duty. National Institute of Justice (NIJ) Level IIIA vest, with the ability to accept Level IV plates, where required, is the standard. All other special clothing worn for protective reasons, safety clothing and equipment, and work clothing worn to protect uniforms or in place of ordinary clothing are not articles of the uniform within the content of this instruction.
d. Items such as socks and undergarments are not articles of the uniform for which uniform allowance will be paid even when color, quality, or type is prescribed.

e. All articles of uniforms visible to the public will be maintained in a serviceable condition. Frayed, faded, torn, or wrinkled uniforms are not acceptable and shall be replaced by the officer utilizing their clothing allowance.

0607. **Policy.** All NCP/SG will maintain a professional appearance at all times while performing duties on Navy installations. This instruction defines the basic policy for personal appearance and wearing of the NCP/SG uniform. For consistency purposes, all NCP/SG will wear the same uniform with the exception of specialized duties such as bike patrol, boat patrol, etc.

0608. **Personal Appearance.** No extreme personal grooming habits or uniforms will be allowed (e.g., fad hairstyles, fingernails that detract from a professional appearance). The ISO is the approving authority for any debated issue. Uniforms will be clean, pressed, and serviceable at all times without exception. As DON representatives, it is inherent that NCP/SG project a professional image which portrays good order and discipline. This includes shirts/blouses and trousers being pressed with single creases. No articles carried in the uniform pockets (wallets, combs, keys, etc.) will be protruding and or visible. Government issued two-way radios and cell phones may be attached to the uniform belt. Personnel will not wear personal cell phones, earphones, and or ear buds while in uniform at anytime. Personnel will not place their hands in the uniform pockets unless they are retrieving an item. All authorized metallic devices adorned on the uniform will be clean with luster and free of scratches. These items will be replaced when they no longer conform to these standards and are considered unserviceable. All shoes/boots will be clean and polished. Tattoos are allowed with the exceptions identified in paragraph 0610 of this instruction.

0609. **Hair, Grooming, and Appearance Standards**

a. Hair (General). Hair and grooming practices are specified below. Hairstyles must be neat, clean, and acceptable by the criteria described below. There will be no extreme or fad style haircuts or hairstyles. No lines or designs will be cut into the hair or scalp. If dyes, tints, or bleaches are
used, colors used must be natural to human hair and not present an extreme appearance. Personnel may wear a wig or hairpiece in uniform to cover natural baldness or physical disfiguration. When worn, it will conform to the standard haircut criteria as stated. Haircuts, without reference to style, will conform to the following standards.

(1) Males

(a) The hair on top of the head will be groomed and have a neat appearance. The length and bulk of the hair will not be excessive or present a ragged, unkempt, or extreme appearance. Hair will present a tapered appearance and when combed will not fall over the ears or eyebrows or touch the collar except for the closely cut hair at the back of the neck. The block cut fullness in the back of the head is acceptable in moderate degree as long as the tapered look is maintained. In all cases, the bulk or length of hair will not interfere with the normal wear of headgear.

(b) Sideburns will be trim, have a horizontal line, and will not have a flared appearance. Sideburns will not extend below the lowest part of the exterior ear opening.

(c) The face will be clean-shaven, with mustaches permitted. If a mustache is worn, it will be kept neatly trimmed and tapered and will not present a chopped-off appearance. Handlebar mustaches, goatees, and beards are not authorized. If appropriate medical authority prescribes beard growth, the length required for medical reasons also will be specified. For example, "A neatly trimmed beard is authorized. The length will not exceed 1/4-inch."

(2) Females

(a) Hair will be neatly groomed. The length and bulk of the hair will not be excessive or present a ragged, unkempt, or extreme appearance. Hair will not fall over the eyebrows or extend below the bottom edge of the collar. Hairstyles will not interfere with proper wearing of headgear.

(b) Hair holding ornaments (including, but not limited to, barrettes, pins, clips, bands), if used, must be unadorned and plain, must be similar in color to the hair, and must be inconspicuously placed. Beads or similar ornamental items are not authorized.
b. Cosmetics. NCP/SG are authorized to wear cosmetics applied conservatively (as determined by the ISO) and in good taste. Exaggerated or faddish cosmetic styles are inappropriate with the uniform and will not be worn.

c. Fingernails. All personnel will keep fingernails clean and neatly trimmed in order not to interfere with performance of duty, detract from the professional image, or present a safety hazard. If used, nail polish must be a natural or clear color to complement the uniform.

d. Wearing of Jewelry

(1) The wearing of a wrist watch, a wrist identification bracelet, including a conservative style Missing in Action/Prisoner of War identification bracelet (only one item per wrist), and not more than two rings (wedding set is considered one ring) is authorized for wear with NCP/SG uniforms unless prohibited for safety or health reasons as long as the style is conservative and in good taste.

(2) No jewelry, watch chains, or similar items will appear exposed on uniforms. Authorized exceptions are a conservative tie tack or tie clasp for wear with the full-length necktie.

(3) Females are authorized to wear prescribed earrings while in uniform. Males are not authorized to wear earrings while in uniform. Earrings may be screw-on, clip-on, or post-type earrings, in gold, silver, white pearl, or diamond. The earrings will not exceed 6 mm or 1/4” in diameter, and must be unadorned and spherical. When worn, the earrings will fit snugly against the ear. Females may wear earrings only as a matched pair, with only one earring per ear. No other jewelry, such as in eyebrows, lips, and nose will be visible while in uniform.

(4) Ankle bracelets, necklaces, faddish (trendy) devices, medallions, amulets, and personal talismans or COns are not authorized for wear with or on any uniform.

e. Wearing of eyeglasses, sunglasses, and contact lenses

(1) Eyeglasses and sunglasses.

(a) Conservative prescription eyeglasses are authorized for wear with all uniforms.
(b) Conservative prescription and nonprescription sunglasses are authorized for wear, except when in formation and while indoors. Prescription glasses of a photo-gray type material that automatically change from light to dark are authorized. Individuals, who are required by medical authority to wear sunglasses for medical reasons other than refractive error, may wear them, except when health and safety considerations apply.

(c) Restrictions on eyeglasses and sunglasses. Trendy eyeglasses or sunglasses or eyeglasses or sunglasses having lenses and frames with initials or other adornments are not authorized for wear. Personnel may not wear lenses with extreme or trendy colors, which include, but are not limited to, red, yellow, blue, purple, bright green, and orange. Lens colors must be traditional gray, brown, or dark green shades. Personnel will not wear lenses or frames so large as to detract from the appearance of the uniform. Personnel will not attach chains, bands, or ribbons to eyeglasses. Eyeglass restraints are authorized only when required for safety purposes. Personnel will not hang eyeglasses or eyeglass cases on the uniform, and may not let glasses hang from eyeglass restraints down the front of the uniform.

(d) Restrictions on contact lenses. Trendy or extreme colored contact lenses are not authorized for wear with the uniform. The only exception is for opaque lenses prescribed medically for eye injuries. Additionally, clear lenses with designs that change the contour of the iris are not authorized for wear with the uniform.

0610. Hygiene and Tattoos. All NCP/SG will maintain good hygiene and present a professional appearance at all times while on duty. Tattoos and branding prejudicial to good order and discipline are prohibited. The CO or designated representative will determine the acceptability of authorized tattoos. Personnel having unauthorized tattoos or brands prior to employment do not need to remove them; however, tattoos must not be visible while in uniform. The following are examples of unauthorized tattoos:

a. Tattoos depicting or symbolizing extremist philosophies, organizations, or activities. Examples would be advocating racial, gender, or ethnic hatred discriminating race, color, gender, ethnicity, religion, or national origins or advocating
violence which deprives individual rights under the U.S.
Constitution or federal or state laws.

b. Indecent tattoos or brands grossly offensive to modesty,
decency, or proprietary, which shock the moral sense and tend to
corrupt morals or incite libidinous thoughts.

0611. **Supervisory Responsibility.** All supervisors will take
necessary actions to ensure compliance with the provisions of
this instruction.

0612. **Honors.** All NCP/SG personnel will render proper respect
to military officers, thus improving the image of the security
force in the eyes of the military and the public. All military
officers identified by their uniform, military identification
card, and or the presence of a blue DD Form 2220 decal on their
vehicle will receive a hand salute. REGCOMs will provide
guidance on rendering the hand salute during periods of
increased traffic, such as morning and afternoon rush hours.
Additionally, NCP/SG will pay respect to the U.S. flag during
reveille and retreat by stopping inbound/outbound traffic and
rendering a proper hand salute in the direction of the flag or
the sound of the music. NSF personnel shall maintain situational
awareness at this time.

0613. **Uniform Allowance.** Payment of uniform allowance shall be
made to employees required to wear a uniform.

a. Initial and replacement allowance shall be IAW reference
(nn).

b. The effective date of the initial allowance is the date
the employee is placed in a position requiring wearing the
uniform. The period covered by the initial allowance is one
year and begins on the anniversary date of placement in the
position requiring wearing of the uniform.

c. In case of appointment or assignment to a police
position for a period of more than three months but less than
one year, the amount of the allowance will be determined by the
REGCOM in relation to the cost of the articles the employee will
be required to buy during the limited period of service. No
allowance shall be granted to an employee appointed or assigned
for three months or less.

d. IAW reference (nn), the initial allowance shall not
exceed $1,800. All NCP (083)/SG (085) employees hired after
February 22, 2007 may be eligible to receive an initial allowance not to exceed $1,800. RSO’s will determine and document the appropriate amount of initial uniform allowance paid to employees based on the cost of the minimum required uniform articles identified in paragraph 0614 of this instruction, as well as any additional uniform items the region deems necessary. Eligible employees, who received less than the determined initial allowance on or after 22 February 2007 shall be reimbursed the difference between what was received and the amount determined by the applicable Region, not to exceed the $1,800 maximum allowance.

e. Employees who are required to wear uniforms will be furnished the uniform at a cost not to exceed $800 per year or paid a uniform replacement allowance equal to the cost of the uniform or $800 per year, whichever is less.

f. Uniform allowance is not considered pay, salary, or compensation.

g. Payment of uniform allowances will be made by the Disbursing Officer on Voucher for Disbursement and/or Collection (NAVCOMPT 2277) prepared by the Security Detachment. Payment to more than one person may be authorized on the same voucher by inserting the word "various" in the payee space and listing each payee in the articles or services block of the voucher. Payment will be made in accordance with regulations provided in the Navy Comptroller Manual. A copy of NAVCOMPT Form 1034 will be maintained as record of payment by the Security Detachment. This record will show the amount of allowance paid, whether initial or replacement allowance, period covered by allowances payment, and employee's official position title.

h. An employee who receives an initial allowance in one position, and who then changes to another position with a different uniform requirement is entitled to an initial allowance for the new position. An employee who receives an initial allowance and then leaves the position is entitled to a further initial allowance upon return to the position if one year has elapsed since the expiration date of the last allowance paid. An employee who transfers to a similar position in DoD after receiving an initial allowance is entitled to only a replacement allowance at the expiration of the period covered by the initial allowance.

i. Entitlement to the replacement allowance for any particular year is conditional on the expectation that the
requirement for wearing the uniform will exist during one-third or more work days of the year.

j. The requirement for wearing the uniform is considered to exist during the period of annual or sick leave and while temporarily assigned to other duties for the purpose of determining eligibility for a replacement allowance. This should not be construed as requiring the wearing of the uniform during periods of annual or sick leave. Payment of the replacement allowance may be withheld if the employee is in non-pay status at the beginning of the year. If the period of absence in a non-pay status continues less than one-third of the year, the employee is entitled to a full yearly payment. If the non-pay status continues beyond one-third of the year, the allowance is prorated. If non-pay status continues beyond two-thirds of the year, no replacement allowance is allowed for the year.

k. Allowance for uniforms specifically applies to clothing which an employee is required to wear in the performance of official duties and shall be used for that purpose. Uniform allowance will be paid once a year.

l. This instruction does not direct the employee to purchase uniforms from any particular supplier as long as the requirement of this instruction is met.

0614. Authorized Uniforms. The uniform items for uniformed NCP/SG include, at a minimum, the following items: Gore-Tex™ gloves; pants; long sleeve shirts; cold weather duty jackets; light weight duty jackets; sweaters; all season trousers; summer duty shirts; winter duty shirts; raincoats; sheriff’s type hats; ties; shoes; leather boots; heavy duty coats; shoulder patches; and cloth badges.

a. Jacket. New generation, convertible-type, navy in color, constructed of nylon fiber featuring standard police department jacket details, modified for year-round use with a zip-in, 200-gram Thinsulate™ liner, heavy-duty nylon zipper, optional removable plush pile collar, Velcro™ sleeve cuffs, and treated to ensure water repellency. Jackets for NCP/NSG personnel will have silver-colored buttons. Jackets for shift supervisors will have gold-colored buttons. A windbreaker-style jacket is an optionally authorized item and may be worn when approved by the ISO. Windbreakers will have the means of attaching a badge and may have "Police" written across the back
of the jacket. All jackets will be kept buttoned or zippered at least three quarters of the way up at all times while on duty.

b. Trousers. Summer and winter specifications are identical. Trousers will be of the conventional police type, without cuffs, dark navy blue in color, with fabric constructed of 100% Dacron™ polyester or poly/rayon gabardine weave, weighing 10.5–11 ounces, plain seams, with 2-inch belt loops. Any flare will not exceed ¾ inches more than the narrowest part of the leg. Winter undergarments must not be visible.

c. Shorts. The only posts/patrols allowed to wear shorts are bike/harbor patrols while performing those specified duties. Type of shorts or uniform for these duties is based on the approval of the REGCOM.

d. Shirt. Dark navy blue, short sleeve, will be authorized for year-round wear. The long-sleeve shirt will be optional during cold weather or ceremonial use. For those supervisory level personnel working in an office environment, white shirts will be worn. Both short-sleeve and long-sleeve shirts will be constructed of 100% Dacron polyester or poly/rayon, two-ply fabric, weight of 7.25 ounces/linear yard, epaulets, sling badge tab, pleated pockets with scalloped flaps secured by Velcro at the corners, dark plastic or metal buttons, and a pencil division the left pocket flap. The long-sleeve shirt will have a convertible collar and a bar-tacked sleeve hem. A plain white or black tee shirt will be worn with the short-sleeve shirt.

e. Tie. Only plain black clip-on ties made of woven cotton, wool, silk, or synthetic fabrics are authorized. Clip-on ties are mandatory for officer safety reasons. The tie shall be worn whenever the long-sleeve shirt is worn and optional with the short-sleeve shirt as determined by the ISO.

f. Tie Tack or Tie Bar. When a tie is worn, a metal tack or bar will be worn to keep the tie neatly in place. These will be plain or conservative in design (silver in color for patrol officers and security guards, gold in color for shift supervisors).

g. Hat. The NCP/NSG hat will be of the type commonly referred to as the “sheriff” style hat. The wool type will be worn during winter months and the straw type will be worn during summer months. It will be navy blue in color with a black chinstrap and a clear rain cover for inclement weather. All personnel will wear the standard DON badge, in the appropriate
color, centered on the front of the sheriff hat. Supervisory personnel will wear gold-colored acorn devices. Non-supervisory personnel will wear silver-colored acorn devices. Non-supervisory NCP/NSG may wear the ball cap with the approval of the RSO in lieu of the sheriff hat. Supervisory personnel will always wear the “sheriff” style hat. Ball cap-style hats with the appropriate insignia will be navy blue and made of nylon, Dacron, and or polyester, either solid woven material or nylon mesh with adjustable band in the rear, with white lettering to indicate Police or Guard. Rank insignias will not be worn on the ball cap. Ball caps will not be blocked, folded, or rolled. The bill of the ball cap may have a slight curvature but will not be excessive. The ball cap will rest squarely on the head and not be tilted in any way. The black watch-cap may be worn during severe cold (below 35°F) weather. Hats will be worn at all times while on all posts.

h. Belt. The belt worn through the trouser belt loops will be of leather material 1–1½ inches in width, black in color, with or without a buckle. If a buckle is used, it will be conservative and will not be visible from under the pistol belt. Leather belts with Velcro closures may be worn. The trouser belt is not a government-issued item.

i. Insignia. Shoulder patches will be of the DON type and will be worn on both shoulders approximately 1 inch below the seam of the jacket and all shirts. (Figure 6-4)

---

Figure 6-4. DON Police and Guard Shoulder Patches
j. Collar Devices. Collar devices shall be worn by supervisory personnel with the rank of lieutenant or above using insignia’s described in paragraph l. below. Devices will be centered approximately 1 inch above the collar tips. Supervisory personnel will wear respective silver/gold-colored metal devices.

k. Epaulet Devices. Members of the rank of lieutenant and above will wear metallic insignias denoting their respective rank on each epaulet or shoulder strap of the jacket.

l. Rank Insignia. The rank insignia for NCP/SG supervisory personnel are as follows. The intent is standardization and shall be implemented within one year of signature to this instruction.

(1) Silver Oak Leaf – Senior Navy Civilian Police Officer (083). The insignia will be centered over the cross stitching of the epaulet or shoulder strap.

(2) Gold Oak Leaf – Navy Civilian Police Operations Officer. The insignia will be centered over the cross stitching of the epaulet or shoulder strap.

(3) Double-Linked Silver bars – Watch Commander. The insignia will be centered over the cross stitching of the epaulet or shoulder strap.

(4) Single Gold bar – Shift Supervisor. The insignia will be centered over the cross stitching of the epaulet or shoulder strap.

(5) Three chevron stripes – Shift Sergeant. Sergeants will wear official designated sergeant chevrons on both sleeves of the shirt and jacket. The top point of the chevron will be ½ inch below the shoulder patch and centered thereon.

m. Police/Security Badge. The standard DON badge (silver/gold) (Figure 6-5) shall be worn centered over the left breast portion of the shirt or coat. All supervisory positions will wear the gold color DON badge. All other positions will wear the silver color DON badge.
Figure 6-5. DON Police and Guard Badges

(1) Only DON patches and badges depicted in Figures 6-4 & 6-5 are authorized for use by NCP/NSG personnel assigned to CNIC regions and installations. No regional, installation or individual department designed patch or badge is authorized.

(2) Additionally, regional or installation Security Department designed and procured credential, consisting of a badge and ID card, will only be carried identifying oneself as:

(a) Navy Master-at-Arms
(b) DON Police
(c) DON Guard
(d) Criminal Investigator
(e) Antiterrorism Officer
(f) Physical Security Specialist

n. Shoes. Black in color, polished patent leather or high-gloss leather shoes and boots are the only authorized footwear permitted. All footwear will be conservative with no straps, buckles, or logos visible while the officer is in the standing
position. Harbor and bike patrols may wear shoe variations as directed and approved by the RSO/ISO.

o. Socks. Socks will either be navy blue or black in color.

p. Winter Gloves. Winter gloves must be solid black in color and made of good-quality, lightweight leather. A glove made of heavy material that interferes with the performance of duties is not authorized.

q. Name Plates with Double Service Bars. These will be of a metal construction, approximately 2¼ by ¼ inches in width. Placement on the uniform will be centered approximately ¼ inch above the top seam of the right pocket flap on both the short- and long-sleeve shirt. Finish may be gloss or non-gloss and will match the badge in color. Field Training Officers will also have "FTO" in front of their name.

r. Weapons Qualifications Badges. If authorized for wear by the REGCOM or CO, these badges will be of metal construction. These badges will be placed on the shirt centered approximately ¼ inch above the top of the nameplate double service bar.

s. Security Identification Badges. The RSO will prescribe the wear and location of any security identification badges to be worn in accordance with all applicable instructions.

t. Personal Protective and Reflective Clothing. All protective clothing and equipment will be issued and worn when applicable while on duty when approved and directed by the CO. These items include, but are not limited to, wet-weather gear, reflective traffic vests or raincoats, concealable body armor, OC or pepper spray, police baton w/holder, handcuffs w/holder, flak vest and helmet, etc. In addition, organizational clothing and equipment may be issued on approval of the CO. All of these items are accountable and will be returned to the installation after termination.

u. Modifications of the Uniform and Changes in Specifications. Changes and modifications will only be approved by the REGCOM. Items purchased by the employee which do not meet the specifications as determined by the ISO will not be worn.

v. Uniform Appearance. Employees are responsible for, and will bear the expense of regular cleaning, laundering, and
routine repair of uniforms. All employees shall be required to maintain their appearance in a neat and well-groomed manner while on duty. Employees will not be allowed to perform duties with an unkempt, dirty, shoddy, or disheveled appearance.

w. Wearing the Uniform. Employees subject to this instruction may wear the prescribed uniform to and from duty unless otherwise directed. However, at no time may employees conduct themselves in a LE capacity off the installation. Personnel will not wear their uniform or any part of the uniform to meetings, social events, or gatherings without prior approval from the ISO or higher authority.

x. Police Whistle (Optional). Officers of the Patrol Unit may wear the regulation police whistle and chain hooked to the right shoulder strap button of the uniform shirt. Whistle and excess chain shall be placed in the right pocket from the right side.

y. Bike Patrol uniform (if applicable) will consist of DOT approved bike helmet, Navy Blue polo shirt with all proper badges, name tags, rank insignias and collar devices, specialty bike shorts, cold weather reflective bike jacket, standard bicycle gloves and leather cross-trainer type shoes with white ankle socks.

z. Tactical Duty Uniform (TDU). The REGCOM may authorize the wear of the TDU for civilian NSF employees (NCP/NSG) and contractors providing direct support to NSF operations. The TDU shall conform to the same high standards of professional appearance as the NCP/NSG service uniform.
CHAPTER 7
TRAINING

0701. Background

a. CNIC shares a vision with CNO, USFF, Navy Education and Training Command, and CENSECFOR for a unified, consistent training program with commonality of training and resources. This is an ongoing, iterative process which constitutes the Navy Warfare Training System used for all operational Navy training and further captures the potential for consolidating resources and training efficiencies. A key to this training continuum is mutual goals for standardization and efficiency. It is essential to review how and where the Navy conducts protection training and to maximize and more efficiently use resources via training consolidation.

b. Prior to implementing the training requirements applicable to NCP/SG identified within Chapter 7, all regional program managers will ensure union notification and subsequent bargaining requirements have been satisfied. Moreover, all regional program managers will ensure that the training requirements are made part of position descriptions and notices on vacancy announcements.

c. Each region and installation will develop and maintain a comprehensive training plan and schedule which will be promulgated and reviewed by the Regional ATWG and approved by the REGCOM/CO as appropriate.

d. To support the Navy’s computer application reduction effort, CNIC has mandated regions and installations to track and schedule NSF training through ESAMS. ESAMS shall be updated monthly to include all qualifications such as, initial training, weapons qualifications, EVOC qualifications, patrolman qualifications etc. Regions and installations shall identify, at a minimum, one coordinator and one alternate to document training utilizing ESAMS.

e. CNIC N7 has formalized and standardized training and exercise for all Navy programs. For the purposes of this chapter, all protection training will be referred to as NSF training. Initial and sustainment training for NSF is the responsibility of the REGCOM through the N3. Regional Training Academies (RTA) will conduct initial training for all Navy Civilian Police (GS-0083) and Navy Security Guards (GS-0085). While attendance in the Regional Training Academy is the
preferred method of delivery; Apprentice training for NCP/SG may be conducted by use of mobile training teams (MTTs) from the RTA in order to meet requirements on a case by case basis. Installation training departments, where they exist, will conduct sustainment training for military, DON civilians, and contractors where specified through contract. Contract guard providers are required to ensure their personnel are trained to current Navy security standards prior to assuming duties.

f. CNIC N7 is responsible to facilitate the exercise component of the training and readiness initiative. All-hazards approach exercises will integrate all phases of sustainment training for security forces. In a coordinated effort, CNIC N3 and N7 shall establish requirements and NMETs, which provides a framework for the REGCOM and CO to meet mission readiness. REGCOM and CO shall ensure training is consistent with existing policy.

g. An RTA has been established at NRMA, NRSE, NRSW, NRNW and NRH. The RTA at NRMA will support NDW initial training requirements; NRSE RTA will support NRMW and NRH RTA will support JNRM. The RTA may deploy a MTT to conduct required training for regions / installations that have an unexpected hiring surge in the number of new CP/SG employees. The decision to conduct training at the RTA location or via MTT at an installation location is the responsibility of the supporting RSO. The RSO/ISO shall maximize the RTA/MTT course convenings by coordinating with Human Resources Office to link new employee hiring dates to the start date of a scheduled NSFTC or NSGTC. The convening of a NSFTC or NSGTC for less than 16 new hires shall be considered an ineffective use of resources. RSOs/ISOs are strongly encouraged to fill vacant course seats with recently hired CP/SG to achieve the minimum course convening size (min. 16 students). Installation training staffs are NOT authorized to conduct initial CP/SG training.

0702. Navy Security Force (NSF) Training

a. Per reference (a), all NSF personnel are required to complete apprentice training prior to assuming their duties and sustainment training on an annual basis. When additional requirements are levied for specialized positions, training will be in accordance with CNO, USFF, CNIC established requirements, and in some cases state and local requirements. Examples of specialized training include, but are not limited to, HSBs, the Military Working Dog Program, Criminal Investigators, etc. Per reference (a), all NSF personnel are required to be armed, and
IAW reference (o) shall qualify with their assigned duty weapons before they are authorized to carry weapons. Training in the Use of Force, to include the Use of Deadly Force, shall be required quarterly for all NSF personnel.

b. Training, exercise, and evaluation policy is prescribed in reference (a) and CNIC N7 Shore Response Training Plan. Effective training will establish readiness as reported in DRRS-N. Individual training is a commander's responsibility before any assignment to watches. Assigned forces must be capable of fulfilling prescribed measures effectively and IAW DoD and DON standards and requirements. Collective training will normally be the responsibility of the commander. Military and civilian security personnel must be familiar with the essential elements of their respective AT plans and procedures, including the necessary command and control (C2) organization and responsibilities, coordination, local alarms, PS equipment, and reporting requirements.

c. Reference (oo), the Presidential Directive that establishes procedures for the management of domestic incidents provides guidance to all agencies for a collective response capability.

d. All NSF personnel designated as First Responders will complete National Incident Management System (NIMS) and Incident Command System (ICS) training. Minimum training required to comply with both NIMS and ICS are as follows.


(3) FEMA IS-100.a - Introduction to Incident Command System (ICS).  http://training.fema.gov/EMIWeb/IS/IS100a.asp


e. CNIC, Center for Security Forces (CENSECFOR), and NECC developed a standardized PQS for the NSF. This PQS will be used in conjunction with NAVEDTRA AT Common Core and Security Force Weapons along with other applicable PQS.
f. Qualifications for position: Once NSF personnel have completed their PQS for patrolman, watch commander etc., they must be able to pass an oral board, with the chairman being the ISO or Deputy ISO. This may not be delegated. Once personnel have qualified he/she will receive a qualification letter signed by the ISO. Qualifications must be documented in ESAMS. Upon transfer to another command he/she must re-board at the new command.

0703. **Harbor Security Boat Training and Reporting**

a. The purpose is to establish HSB minimum training and reporting requirements for coxswains and to reinforce compliance with HSB mishap reporting for regions and installations. All personnel assigned to a HPU shall be coxswain and crew served weapons qualified.

b. Three elements exist to the HPU training solution. The following identify these elements and the methods to attain HPU coxswain qualification as stated in reference (pp)

1. **Level I - Basic Coxswain or boat “drivers license”**

   a. Attend Commander Surface Combat Systems (CSCS) 7M RHIB Coxswain COI (K-062-0625) and complete PQS IAW NAVEDTRA 43152-F, or

   b. Perform under instruction of the installation/region HSB TRASUP or PQS qualifier using CSCS 7M RHIB courseware (K-06200625) and complete PQS IAW NAVEDTRA 43152-F, or

   c. Attend Shore Installation Management Basic Boat Coxswain Course (SIMBBC) and complete SIMBBC PQS NAVEDTRA 43153

2. **Level II - Tactical (Mission) qualifications:**

   Attend Level II Coxswain Operations and Tactics COI (A-062-0050) and complete PQS IAW NAVEDTRA 43467-1 under the instruction of a HSB TRASUP, or

3. **HSB TRASUP - Training management, oversight and standardization**

   a. Designated in writing by the Commanding Officer as a HSB TRASUP

   b. Complete the HSB TRASUP Course (A-062-0049)
(c) Have a minimum of 100 underway hours of tactical experience documented by parent command

(d) Complete NAVEDTRA 43467-1

(e) Successfully complete the Level II Coxswain Operations and Tactics Course (A-062-0050)

c. HSB mishaps will be reported IAW reference (ii). When providing information regarding the mishap, include the DTG of OPREP message and IC “Incident Number”.

0704. **Nonlethal Weapons (NLW)**

a. In conjunction with other services, the Navy continues to research the use of increased capabilities with regard to NLW. Currently, CNIC policy allows the employment of the following NLW types and tactics; OC spray, straight baton, expandable baton, handcuffs/flexi-cuffs, and hand-to-hand techniques and will evaluate other means of non lethal force as technology matures. All security force personnel will attend and satisfactorily complete NLW training IAW reference (a).

b. The use of the human electro-muscular incapacitation (HEMI) devices are prohibited for use by Region or installation security personnel.

0705. **Security and Auxiliary Security Force (ASF) Training**

a. Region NGS RTA, Installation NGS Site Managers, and OCONUS AT Training Supervisors will deliver NSF Sentry (NSFS) (A-830-2216)/Security Reaction Force Team Member Basic (SRFTM-B) (A-830-2217) courses within their respective areas of responsibility to maintain adequate Security and ASF end-strength. Qualified instructors (minimum of two per course) must be graduates of the following courses in order to deliver NSFS/SRFTM-B COI’s:

   (1) Anti-Terrorism Training Supervisor (A-830-0034) (NEC 9501) and/or;

   (2) Small Arms Marksmanship Instructor (SAMI) (A-041-0148) (NEC 0812) or appropriately qualified Government Civilian employee meeting the instructor training requirements delineated in reference (o).
b. NSFS (A-830-2216)/SRFTM-B (A-830-2217) are the only authorized courses for Armed Sentry Region/Installation Between the Lifelines (BTL) delivery. Students will receive classroom and hands-on instruction in NLW, firearms, watch standing, basic reaction force tactics and communications. Graduates will possess knowledge of proper employment techniques with the baton, will be certified to carry and employ Oleoresin Capsicum (OC) spray, will be qualified on M9 service pistol, M16 rifle, and shotgun, and will be able to perform as a force protection team member. Training must be conducted and reported in accordance with paragraph f.(1).

c. Prerequisites. Commands are responsible for validating prerequisites and screening students prior to course convening.

(1) No domestic violence convictions.

(2) Physically fit/has passed last Physical Fitness Assessment.

(3) No light duty.

(4) Must be medically prescreened to participate in NLW training, specifically for OC Level 1 direct exposure.

d. Equipment. No additional equipment will be provided. Installations are encouraged to maximize existing resources within the security training program.

e. Prior to instructing a course, the AT Training Supervisor shall check NKO to verify the most current curriculum is being taught. Course material for NSFS (A-830-2216)/SRFTM-B (A-830-2217) can be found under the CENSECFOR curriculum page. AS/SRF-B (A-830-0018) is no longer authorized for delivery.


(1) Upon completion of NSFS (A-830-2216)/Security SRFTM-B (A-830-2217), regions/installations will report via Navy message to TRASUPPCEN Hampton Roads (TSC HR). Messages will info the following addresses: CNIC/N7, REGCOM/N7, and CENSECFOR NORFOLK VA/N5.

(2) An example of the required message follows:

R XXXXXXXZ JAN 11
FM NAS NEVERSAIL VA/
TO TRASUPPCEN HAMPTON ROADS DAM NECK VA/
INFO CNIC WASHINGTON DC//N7/
COMNAVREG XXXXX//N03T/N7/
CENSECFOR NORFOLK VA//N5/
UNCLASS FOUO
MSGID/GENADMIN/NAS NEVERSAIL/-/MAY/
SUBJ/FOUO-PRIVACY SENSITIVE-REPORT OF TRAINING NAVY SECURITY
FORCE SENTRY (NSFS) (A-830-2216)/SECURITY REACTION FORCE TEAM
MEMBER BASIC (SRFTM-B) (A-830-2217)
REF/A/DOC/CNIC/FEB 2011/
AMPN/REF A IS CNIC ASHORE PROTECTION PROGRAM INST 5530.14/
POC/DOE, JOHN/MAC/PUBLIC SAFETY STOREFRONT NEVERSAIL/-/TEL: 999-
999-9999/
RMKS/1. IAW REF A, THE FOLLOWING COMMAND LEVEL DELIVERY OF ARMED
SENTRY TRAINING IS SUBMITTED.
A. CIN/CDP/CLASS CONVENING: A-830-2216/08M5/5-9 DEC 2011
B. CIN/CDP/CLASS CONVENING: A-830-2217/08M6/12-23 DEC 2011
C. TRASUP AND SAMI CONDUCTING COURSE: GS-12 JOHN DOE/MAC JANE
SMITH
D. STUDENT GRADUATION/COMMAND INFO:
COMMAND         UIC    NAME/RATE          SSN (Last 4)
NAS NEVERSAIL   99999  JONES, DAVY BMC    9999
E: FOUO - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED
DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES.//
BT
NNNN

(3) Convene/graduation date: Course delivery will be a
minimum of three weeks for class sizes greater than 10 students.
Course delivery may be reduced to two weeks for smaller class
sizes of less than 10 personnel.

(4) TRASUPPCEN Hampton Roads will enter course
completions into the Corporate enterprise Training Activity
Resource System (CeTARS) for Navy-wide tracking and entry into
personnel Electronic Training Jackets (ETJ). For additional
information, contact TRASUPPCEN Hampton Roads at 757-421-
8105/8109.

g. Commands will conduct ASF training during a consecutive
three week period in an uninterrupted training environment to
facilitate completion of training requirements. Students should
be in a non-duty status during delivery of this training.

h. Additionally, each student scheduled to attend NSFS (A-
830-2216)/SRFTM-B (A-830-2217) will have their ETJ screened
utilizing the Fleet Training and Management Planning System (FLTMPS). If the student has attended any of the following courses, they meet requirements for Armed Sentry Training and are not required to repeat the course.

(1) Graduate of MA "A" School (A-830-0011) after Sept 2006. All graduates of MA "A" School prior to Sept 2006 must complete Armed Sentry Training to be qualified for watch standing assignments while performing Force Protection and or Law Enforcement duties.

(2) NSFS (A-830-2216)/ SRFTM-B (A-830-2217) (Must have both course completions in ETJ to meet Armed Sentry requirements).

	ri. For personnel who indicate they have attended but do not show attendance in their ETJ for Armed Sentry Training, RTA and Installation AT Training Supervisors (E-7 and above or CIV equivalent) will verify student attendance by having the individual provide a copy of their graduation certificate from any of the COI’s listed above. The RTA or Installation AT Training Supervisor is then required to submit a course attendance message to update personnel ETJ’s in the following format:

R XXXXXXXZ JAN 11
FM NAS NEVERSAIL VA//
TO TRASUPPCEN HAMPTON ROADS DAM NECK VA//
INFO CNIC WASHINGTON DC//N7//
COMNAVREG XXXXX/N03T/N7//
CENSECFOR NORFOLK VA//N5//
UNCLAS FOOU
MSGID/GENADMIN/NAS NEVERSAIL/~/MAY//
SUBJ/FOOU-PRIVACY SENSITIVE-REPORT OF TRAINING BETWEEN THE LIFELINES (BTL) ARMED SENTRY TRAINING//
REF/A/DOC/CNIC/12NOV2008(update when Instruction is signed)//=
AMPN/REF A IS CNIC ASHORE PROTECTION PROGRAM INST 5530.14//=
POC/DOE, JOHN/LT/PUBLIC SAFETY STOREFRONT NEVERSAIL/~TEL:999-999-9999//=
RMKS/1. THE FOLLOWING PERSONNEL HAVE BEEN VERIFIED AS GRADUATES OF BTL ARMED SENTRY TRAINING.
A. SECURITY PERSONNEL VERIFYING COURSE ATTENDANCE: LT JOHN DOE/GS-07 JANE ANDERSON/MAC BILL CODY
B. (READ IN FIVE COLUMNS: RANK/NAME/SSN/COURSE/GRAD DATE)
0706. **Training Standards for Navy Civilian Police and Security Guards NCP/SG**

a. CNIC N7, in conjunction with CNIC N3AT has developed a standardized curriculum for CNIC NCP officers. The course title is “Navy Security Forces Training Course” (S-540-1006). This will be the only course authorized for initial training of NCP within CNIC. The COI is nine (9) weeks in length. Failure to pass this COI will result in dismissal as a NCP officer. All new hires and those who have not attended a regional academy will be required to attend the CNIC “Navy Security Forces Training Course” (S-540-1006). Priority of attendance will be new hires followed by the least senior NCP who has not attended the Navy Security Forces Training Course (S-540-1006). This course will not be grandfathered; however, regions that have previously conducted police academies shall conduct a review of previously provided initial training compared against the DoD/DoN standards. Those current NCP who have received training equal to the established standards may have the requirement to attend the course waived. The approval authority for this waiver is the RSO. A copy of all approved waivers will be provided to CNIC N3AT and include the subjects taught, number of hours of training, comparison to current standards and waiver justification. In addition to the topics listed in Figure 7-1, the new curriculum will also consist of:

1. Training Course Control Document (TCCD)
2. Instructor Guides
3. Student Guides
4. Presentations to support each terminal and enabling objective
(5) Practical exercise scenarios

(6) Weapons qualification (9mm Pistol, 12 Gauge Shotgun, M-16 Rifle)

(7) Emergency Vehicle Operator Course (EVOC)

b. Minimum training standards have been established for all NCP/SG. All regions will ensure the minimum standards are met for initial training of NCP/SG employees.

c. Initial training and certification standards. Each individual who performs NCP/SG guard tasks or duties will, prior to assignment, be trained and qualified to perform assigned duties. The following policy concerning basic NCP/SG training is provided:

(1) NCP. All newly hired NCP (083) personnel shall attend a Regional Training Academy for initial training, regardless of previous law enforcement training received prior to being hired.

(a) The RSO will ensure all NCP graduate from a Regional Training Academy and complete the Field Training Officer (FTO) Navy formal training program prior to assignment of duties. NCP also must attend and complete an in-service sustainment training program to maintain certification. The RSO is responsible for programming and funding initial training requirements.

(b) The CO is responsible for programming and funding in-service sustainment training requirements.

(c) NCP will not be assigned duties which require them to be armed until all initial training, use of force training and weapons qualification have been successfully completed.

(2) Navy Security Guards (NSG).

(a) All contract and 0085 Security Guards must successfully complete a NSG training program prior to assignment to NSG duties utilizing the NSFS course (A-830-2216) as the standard in addition to DoD/DoN and local requirements. Once development of the Navy Security Guard Training Course (NSGTC) is complete, all GS-0085 Security Guards and contract guards must successfully complete the NSGTC ILO the NSFS prior to
performing duties as a SG. The NSGTC will meet all DoD and DON training requirements. Local requirements may be included after successful completion of the NSGTC.

(b) NSG will not be assigned duties which require them to be armed until all initial training, use of force training and weapons qualification have been successfully completed.

(c) The RSO will ensure all NSG graduate from a Regional Training Academy prior to assignment of duties.

(d) The RSO is responsible for programming and funding initial NSG training requirements.

(e) The CO is responsible for programming and funding in-service sustainment training requirements.

d. Minimum Training Standards for GS-0083, Civilian Police Personnel. Table 7-1 lists the minimum training standards for Series 0083 or equivalent civilian police.
<table>
<thead>
<tr>
<th>Activities/Duties</th>
<th>Series 0083 or Equivalent Civilian Police Minimum Training Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Security Forces/Military Law Enforcement History and Culture</td>
</tr>
<tr>
<td></td>
<td>NSF Duties and Functions</td>
</tr>
<tr>
<td></td>
<td>Standards of Conduct</td>
</tr>
<tr>
<td></td>
<td>Area Familiarization</td>
</tr>
<tr>
<td></td>
<td>Organization</td>
</tr>
<tr>
<td></td>
<td>- Chain of Command</td>
</tr>
<tr>
<td></td>
<td>- Functions</td>
</tr>
<tr>
<td></td>
<td>Operations</td>
</tr>
<tr>
<td></td>
<td>- Concept and Principles</td>
</tr>
<tr>
<td></td>
<td>- General LE/Security Force Operations</td>
</tr>
<tr>
<td></td>
<td>- LE/Security Force Roles and Missions</td>
</tr>
<tr>
<td></td>
<td>- Community Policing</td>
</tr>
<tr>
<td></td>
<td>Ethics/LE Code of Conduct</td>
</tr>
<tr>
<td></td>
<td>Judgmental Training</td>
</tr>
<tr>
<td></td>
<td>Interpersonal Skills</td>
</tr>
<tr>
<td></td>
<td>AT Level 1</td>
</tr>
<tr>
<td></td>
<td>PS Safeguards</td>
</tr>
<tr>
<td></td>
<td>Force Protection</td>
</tr>
<tr>
<td></td>
<td>- FP OPSEC</td>
</tr>
<tr>
<td></td>
<td>- Threat Levels/FPCONs</td>
</tr>
<tr>
<td></td>
<td>- Threats to Installations and Resources</td>
</tr>
<tr>
<td></td>
<td>Concept and Principles/Threat Spectrum</td>
</tr>
<tr>
<td></td>
<td>- Terrorism/AT</td>
</tr>
<tr>
<td></td>
<td>Active Shooter</td>
</tr>
<tr>
<td></td>
<td>Physical Fitness and Nutrient</td>
</tr>
<tr>
<td>Legal</td>
<td>Posse Comitatus Act/Military Authority</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction and Authority</td>
</tr>
<tr>
<td></td>
<td>Criminal Law</td>
</tr>
<tr>
<td></td>
<td>- Military Law (UCMJ, Assimilative Crimes Act)</td>
</tr>
<tr>
<td></td>
<td>- Civil Law (18 U.S.C.)</td>
</tr>
<tr>
<td></td>
<td>Introduction to Court Testimony</td>
</tr>
<tr>
<td></td>
<td>- Captain's Mast/Courts-Martial</td>
</tr>
<tr>
<td></td>
<td>Advise Persons of Their Rights</td>
</tr>
<tr>
<td></td>
<td>Rules of Evidence</td>
</tr>
<tr>
<td></td>
<td>Federal Tort Law</td>
</tr>
<tr>
<td>Search</td>
<td>Search and/or Seizure Authorization</td>
</tr>
<tr>
<td></td>
<td>Employ Search Procedures</td>
</tr>
<tr>
<td></td>
<td>Search Individuals</td>
</tr>
<tr>
<td></td>
<td>Search Vehicles</td>
</tr>
<tr>
<td></td>
<td>Search Buildings</td>
</tr>
<tr>
<td></td>
<td>Search Areas</td>
</tr>
<tr>
<td>First Aid</td>
<td>First Responder First Aid</td>
</tr>
<tr>
<td></td>
<td>Blood-Borne Pathogens</td>
</tr>
<tr>
<td></td>
<td>Cardiopulmonary Resuscitation</td>
</tr>
<tr>
<td>Activities/Duties</td>
<td>Series 0083 or Equivalent Civilian Police Minimum Training Standards</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Apply Force</td>
<td>DoD Force Continuum (Use of Force)</td>
</tr>
<tr>
<td></td>
<td>Use of Deadly Force</td>
</tr>
<tr>
<td></td>
<td>Use of Less than Deadly Force</td>
</tr>
<tr>
<td></td>
<td>Apply LE Techniques</td>
</tr>
<tr>
<td></td>
<td>- Nonlethal Weapons</td>
</tr>
<tr>
<td></td>
<td>- Employ OC Pepper Spray</td>
</tr>
<tr>
<td></td>
<td>- Employ Expandable Baton</td>
</tr>
<tr>
<td></td>
<td>- Use Unarmed Self-Defense Techniques</td>
</tr>
<tr>
<td></td>
<td>- Use Straight Baton to Subdue a Suspect</td>
</tr>
<tr>
<td>Weapon(s)</td>
<td>Qualify Semiannually with Assigned Weapon</td>
</tr>
<tr>
<td>Communications</td>
<td>Use and React to Visual Signaling Techniques</td>
</tr>
<tr>
<td></td>
<td>Communications Discipline</td>
</tr>
<tr>
<td></td>
<td>Tactical Communication</td>
</tr>
<tr>
<td>Reports/Report Writing</td>
<td>Prepare Evidence Tag</td>
</tr>
<tr>
<td></td>
<td>Visitor/Vehicle Pass</td>
</tr>
<tr>
<td></td>
<td>Prepare Visitor Register Log</td>
</tr>
<tr>
<td></td>
<td>Prepare Statement of Suspect, Witness, or Complainant</td>
</tr>
<tr>
<td></td>
<td>Prepare Authority to Search and Seize</td>
</tr>
<tr>
<td></td>
<td>Prepare Consent for Search and Seizure</td>
</tr>
<tr>
<td></td>
<td>Prepare Incident Report</td>
</tr>
<tr>
<td></td>
<td>Prepare Receipt for Inmate or Detained Person</td>
</tr>
<tr>
<td></td>
<td>Prepare Field Interview Card</td>
</tr>
<tr>
<td>Patrol/Post Activities</td>
<td>Patrol Procedures (Vehicle and Boat)</td>
</tr>
<tr>
<td></td>
<td>Objectives of Patrol</td>
</tr>
<tr>
<td></td>
<td>Types of Patrol</td>
</tr>
<tr>
<td></td>
<td>Record Police Information</td>
</tr>
<tr>
<td></td>
<td>Apprehend a Subject</td>
</tr>
<tr>
<td></td>
<td>Transport Offenders</td>
</tr>
<tr>
<td></td>
<td>Perform Vehicle Preventive Maintenance Checks and Services</td>
</tr>
<tr>
<td></td>
<td>Introduction to Capabilities and Use of Military Working Dogs</td>
</tr>
<tr>
<td></td>
<td>Movement Techniques</td>
</tr>
<tr>
<td></td>
<td>- Enter a building</td>
</tr>
<tr>
<td></td>
<td>- Clear a Building</td>
</tr>
<tr>
<td></td>
<td>- Use Cover and Concealment</td>
</tr>
<tr>
<td></td>
<td>- Clear areas</td>
</tr>
<tr>
<td></td>
<td>Installation Patrol</td>
</tr>
<tr>
<td></td>
<td>Conduct Building and Repository Checks</td>
</tr>
<tr>
<td></td>
<td>- Respond to Alarms</td>
</tr>
<tr>
<td></td>
<td>- React to Weapons Fire</td>
</tr>
<tr>
<td></td>
<td>Vehicle Stops</td>
</tr>
<tr>
<td></td>
<td>- High Risk</td>
</tr>
<tr>
<td></td>
<td>- Unknown Risk</td>
</tr>
<tr>
<td></td>
<td>Driver Training/Emergency Vehicle Operator Course</td>
</tr>
<tr>
<td></td>
<td>Officer Survival/Safety</td>
</tr>
<tr>
<td>Activities/ Duties</td>
<td>Series 0083 or Equivalent Civilian Police Minimum Training Standards</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Patrol/Post Incidents | Introduction to Responding to Calls for Service Preplanned Response Procedures (Small Boat, Suspicious Packages, etc.) Protocols  
- Secure Crime Scenes  
- Process Crime Scenes  
- Crime Scene Search  
- Crime Scene Search Patterns  
- Hostile Intent Determination (Small Boat)  
Identify Evidence/Contraband (Including Drugs)  
- Collect Evidence  
- Interview Persons  
Introduction to Emergency Response Protocols  
- Bombs/Bomb Classifications  
- Improvised Explosive Device  
- Means of Detonation  
- Means of Delivery  
- Bomb Threat  
- Bomb Threat Procedures  
- Evacuation/Evacuation Planning  
- Search Procedures  
- Sabotage and Wrongful Destruction  
Introduction to Incident Management  
- Identify Offense of Sexual Assault/Rape  
- Identify Offense of Burglary  
- Identify Offense of Housebreaking  
- Identify Offense of Larceny or Wrongful Appropriation of Property  
Identify Offense Involving Controlled Substances  
- Collect Physical Evidence at a Crime Scene  
- Interrogate Suspect(s) and Subject(s)  
- Maintain Accountability of Evidence in an Evidence Room |
| Civil Disturbance | Introduction to Crowds/Crowd Behavior  
Introduction to Use a Riot Baton/Riot Shield/Use of Gas Mask  
Introduction to Position Yourself in Riot Control Formation  
Introduction to Conduct Squad-Size Riot Control Formations |
| CBRNE | Basic LE First Responder Skills  
Basic LE Individual Protection  
National Incident Management System (NIMS)  
Incident Command System (ICS) |

e. Civilian Security Guard Standards. Table 7-2 lists the Series 0085 NSG or contract SG minimum training standards.
<table>
<thead>
<tr>
<th>Activities/Duties</th>
<th>Series 0085 or Contract Security Guard Minimum Training Standards</th>
</tr>
</thead>
</table>
| General                | NSF Duties and Functions  
                         | Security Forces/Military LE History and Culture  
                         | Organization  
                         | ▪ Chain of Command  
                         | ▪ Functions  
                         | Ethics/LE Code of conduct  
                         | Interpersonal Skills  
                         | AT Level 1  
                         | Force Protection  
                         | ▪ FP OPSEC  
                         | ▪ Threat Levels/FPCONs  
                         | ▪ Threats to Installations and Resources  
                         | ▪ Concept and Principles/Threat Spectrum |
| Legal                  | Types of Jurisdiction                                                                                                           |
| Search                 | Employ Search Procedures  
                         | ▪ Search Individuals  
                         | ▪ Search Vehicles  
                         | ▪ Search Buildings |
| First Aid              | Cardiopulmonary Resuscitation  
                         | First Responder First Aid  
                         | Blood-Borne Pathogens |
| Apply Force            | DoD Force Continuum (Use of force)  
                         | Use of Deadly Force  
                         | Use of Less than Deadly Force  
                         | Apply LE Techniques  
                         | Nonlethal Weapons  
                         | ▪ Employ OC Pepper Spray  
                         | ▪ Employ Expandable Baton  
                         | Use Unarmed Self-Defense Techniques  
                         | Use Straight Baton to Subdue a Suspect |
| Weapon(s)              | Qualify Semiannually with Assigned Weapon                                                                                       |
| Communications         | Communications Discipline                                                                                                         |
| Patrol/Post Activities | Perform Vehicle Preventive Maintenance Checks and Services  
                         | Conduct Building and Repository Checks  
                         | Officer Survival/Safety |
| Patrol/Post Incidents  | Secure Crime Scenes  
                         | Bombs/Bomb Classifications  
                         | Improvised Explosive Device  
                         | Bomb Threat  
                         | Bomb Threat Procedures  
                         | Evacuation/Evacuation Planning |
| Reports/Report Writing | Visitor/Vehicle Pass  
                         | Prepare Visitor Register Log                                                                                                    |
| CBRNE                  | Basic LE First Responder Skills  
                         | Basic LE Individual Protection                                                                                                  |
f. Each region and installation will establish a Cycle of Training, to include at a minimum, topics and drills listed in Appendix F.

g. All regions will establish a certification program that requires NCP/SG to:

(1) Successfully complete a standardized training program, including initial and sustainment training.

(2) Meet approved medical and physical fitness standards.

(3) Qualify with assigned weapons IAW reference (o).

h. Physical Agility Test (PAT). The PAT serves to provide a measure of the individual’s preparedness to successfully accomplish the essential functions of the position. In order to meet the condition of employment standard, the individual tested must successfully pass the established standard for each of the two elements of the PAT.

(1) Background.

(a) The U.S. Navy has directed the implementation of a PAT for NCP and NSG IAW reference (qq). CNIC has implemented the U.S. Army PAT. The U.S. Army is the Executive Agent for establishing minimum training standards for DoD civilian police and security guards. The purpose of the test is to ensure the capability of our NCP/SG to satisfactorily perform the physical aspect of the full range of essential job duties. Minimum physical agility standards relate to the individual's job requirements by providing relative measures of the individual's preparedness to perform physically demanding tasks in unusual or emergency situations.

(b) All NCP/SG personnel will meet the minimum standards of the performance-based PAT for NCP/SG. The PAT is based on occupational tasks. Tests will be conducted at least annually. Personnel require medical screening and clearance prior to testing.

(c) The procedures below direct the conduct and administration of the PAT for NCP/SG.
(d) A minimum of four months must elapse before an individual who passed the PAT in one calendar year is required to take the PAT again in the next calendar year. Job descriptions and performance plans/performance standards will contain the PAT requirement.

(e) New hires must be advised in writing at the time of initial employment they are required to pass a PAT within 30 days of being medically screened and cleared to initially take the PAT. New hires must pass the PAT prior to graduation from the Regional Training Academy. New hires must sign a statement acknowledging they have been advised of the initial PAT and that it will also be required annually as a condition of their employment.

(f) Current NCP/SG employees are required to take an initial PAT within 30 days of being medically screened and cleared, and must pass the PAT within one year from the date of their medical clearance; thereafter, an annual PAT will be required for all NCP/SG. It is a condition of employment that individuals tested must successfully pass the established standard for each of the elements of the PAT. If the NCP/SG fails the PAT, he/she will be required to pass the retest within 90 days. If the NCP/SG fails the second PAT, the ISO may request a waiver from the RSO for a third attempt. If granted, the PAT will be conducted by personnel from the Region. After failure of a second (or third if a Regional waiver is granted), the ISO will contact the Human Resources Office or Human Resources Service Center for advice on termination.

(g) The RSO/ISO shall designate physical screening personnel to schedule NCP/SG for their medical physical at the installation medical treatment facility (MTF). Upon satisfactory completion of physical and when proper documentation is forwarded to the training department, they will conduct the PAT annually for all NCP/SG personnel. The medical physical will ensure personnel are cleared to participate in the PAT.

(2) PAT Standards. All NCP/SG will be required to meet the following minimum physical agility test standards.

(a) Execute 19 push-ups in two minutes.

(b) Run 1.5 miles in 17:30 minutes.

(3) PAT Test Procedures
(a) The PAT will be scheduled and participants notified of the PAT test date at least one month in advance. A suitable location will be identified in advance, and all required equipment available at the test site when the PAT is administered. The procedure and order for testing are as follows:

1. Conduct warm up for 3 minutes
2. Perform push ups
3. Rest for 10 minutes
4. Conduct cardio warm-up for 2-3 minutes
5. Perform the run
6. Conduct cardio cool-down for 5 minutes

(b) Execute 19 push-ups in two minutes. This event demonstrates core strength and capacity used in defensive tactics and is important for rescues and use-of-force situations.

1. The following guidance will be adhered to by the graders and the person performing the PAT push-ups. The push-up event measures the endurance of the chest, shoulder, and triceps muscles.

2. On the command “Get set,” the NCP/SG will assume the front-leaning rest position by placing their hands where they are comfortable and feet may be together or up to 12 inches apart. When viewed from the side, the body should form a generally straight line from shoulders to ankles. On the command “Go,” the NCP/SG will begin the push-up by bending at the elbows and lowering their entire body as a single unit until upper arms are at least parallel to the ground. Then, they will return to the starting position by raising the entire body until arms are fully extended. The body must remain rigid in a generally straight line and move as a unit while performing each repetition. At the end of each repetition, the scorer will state the number of repetitions that have been completed correctly.

3. If the person fails to keep the body generally straight, to lower the whole body until upper arms are
at least parallel to the ground, or to extend arms completely, that repetition will not count, and the scorer will repeat the number of the last correctly performed repetition. If the first five push-ups are not done correctly, the scorer will tell the person to go to his or her knees and will explain what the mistakes are. The person will then be retested after a 10-minute wait. After the first five push-ups have been performed and counted, however, no restarts are allowed. The test will continue, and any incorrectly performed push-ups will not be counted.

4. An altered, front-leaning rest position is the only authorized rest position. That is, the person may sag in the middle or flex the back. When flexing the back, knees may be bent but not to such an extent they support most of the body weight with the legs. If this occurs, performance will be terminated. After resting, the person must return to, and pause in the correct starting position before continuing. If the person rests on the ground or raises either hand or foot from the ground, performance will be terminated. Feet and hands may be repositioned during the test as long as they remain in contact with the ground at all times. Correct performance is important. The person has two minutes to complete 19 push-ups.

(c) Run 1.5 miles (2.41 km) in 17:30 minutes. This event serves to assess cardio-respiratory and leg-muscle endurance.

1. Equipment: Two stopwatches are required for the event supervisor and a clipboard with all runners’ names. Two stopwatches are used in the event one fails.

2. Facilities: The running area must be generally level with no more than a 3° slope on which a measured course has been marked. An oval track of a known length may be used. If a road course is used, the start, finish, and ½ mile increments must be marked.

3. The event supervisor is the timer. As the runners near the finish line, the event supervisor calls out the times so the runners and the graders clearly hear the finish time.

4. Although the person being tested can walk, it is discouraged. Runners may not be physically helped in any way. They may be encouraged by other persons, but they cannot be physically touched while on the running course.
(4) Alternate PAT Events. Alternate PAT events are permitted for NCP/SG with long-term medical restrictions or disabilities that cannot perform the run or push-up events but can otherwise perform the essential functions of the job. The NCP/SG must perform all the regular PAT events his/her medical restriction permits and also complete any identified alternate event in the time period specified. Alternate events are as follows:

(a) The 2.0-mile walk is an authorized alternate event for the 1.5-mile run. This event uses the same course as the 1.5-mile run. Scorers must observe the person during the entire event and must ensure the person maintain a walking stride. Those who break into any type of running stride will be terminated from the event and given a "no go." When the event is over, scorers record the time in the scorecard, initial the appropriate block, and note in the comment block that the time is for a 2.0-mile walk and whether or not the testee received a "go" or "no go." To successfully pass this event, the individual must walk 2.0 miles in 32:30 minutes.

(b) The 25-foot dummy drag is an authorized alternate event for the push-up. The dummy must be of average proportionate height and weight of an adult and weigh 140–150 pounds. The individual stands behind the dummy and holds it under its arms, bending at the knees to protect lower back. At the starting line, participants must move the dummy in a controlled manner for 25 feet and place the dummy on the ground safely at the completion of the event (dummy's feet must pass the 25-foot line). To pass, the event must be completed in 15 seconds and without dropping the dummy.

(5) Temporary Medical Conditions. NCP/SG who are temporarily medically restricted from performing the functions of their job, including taking the PAT, will be exempt from taking the PAT for the duration of the temporary medical restriction. Once the temporary medical restriction has been lifted and the individual has been medically cleared to return to duty, he/she will have 90 days to take the PAT.

0707. **AT Level 1 Awareness Training.** IAW references (b) and (d), the REGCOM and CO shall ensure all assigned personnel receive Level 1 AT Awareness Training annually. This includes military personnel, DoD employees, contractors, and accompanying family members to locations outside of the United States. AT
Awareness Training will be completed on NKO or under the instruction of a qualified Level I AT Awareness instructor.
CHAPTER 8
EXERCISES AND READINESS

0801. General. An exercise and evaluation standard will be explicitly reviewed, evaluated, and tested on different specific response capabilities. Exercises are used to coordinate requirements and plans in a scenario-based environment so units can train with realistic conditions. The program will also be used to assess lessons learned and validate plan revisions, as deemed appropriate. Regional/Installation AT exercises must, where possible, provide for the potential range of AT capabilities that are required by the command. Training events and exercises should be executed to meet and/or exceed minimum requirements. During execution, performance data, key issues and lessons learned will be observed and collected. Training participants will be encouraged to provide evaluations and training feedback. At a minimum, individual and team-related activities such as the ICS, together with appropriate NMETs and FPCON measures, shall be exercised. Appropriate AT command, control, and communications functions should also be exercised.

0802. Overview. Commanders will conduct several training exercises annually to test individual tasks and capabilities on a performance-based scale, which will require hands-on demonstration, real-world application, and the detailed evaluation of lessons learned. Testing will validate individual preparedness, planning, and training to determine whether the program is capable of completing the desired task and mission. Real-world applications of protection exercises such as no-alert drills (no-alert drills must conform with all the requirements regarding safety and high-risk training) and field training exercises (FTXs) and USFF’s Navy Security Operations Exercise Program (NSOXP) are designed to validate personnel knowledge, personnel abilities, equipment use, and equipment performance in achieving and completing the critical tasks. All supporting elements of these programs must participate and evaluate in realistic exercises, including multidisciplinary and multijurisdictional events with federal, state, local, other services, and/or private (host-nation) interaction to validate actions, plans, essential skills, improve integration, and promote interoperability.

0803. Goals

a. The goals of the exercise and evaluation program are to test preparedness, planning, and training; to enhance the increase of proficiency; and to validate/test the capability of
an installation to prepare for, mitigate, respond to, and initiate recovery from all natural and man-made hazards identified within the hazard assessment. The protection exercise and evaluation program provides information needed to validate the program and identify or establish future training requirements. Exercises are a means to ensure that the components of the plan are executable and the resources needed are available, adequate, and trained to standards.

b. Regional headquarters/assigned unit AT exercise must, where possible, provide for the potential range of AT capabilities that may be required by the organization. As a minimum, individual and team-related activities will ensure the NMETs together with appropriate FPCON measures and appropriate AT command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) functions are exercised. Other related details on exercises can be found in reference (pp), the SRTP Toolbox.

c. All training and exercises will be NMETS based and will be assessed and entered in Navy Training Information Management Systems (NTIMS). Training will be NMET based and developed using a collection plan within the execution module of NTIMS. Once training is completed, the training assessment will be entered in NTIMS via the collection plan. Once all NMETS associated with the sub event are completed, then a sub event collection plan is submitted. Both collection plan submissions are in order to document the training exercise or unit level training assessment and populate the DRRS-N “T” pillar to reflect the current training readiness of a command. NTIMS input/population shall be made by N7 with input from N3AT at the Region and installation level.

0804. Exercise Planning. Integrated exercises are the culmination of individual and team/unit training. Training will be coordinated with the N7. Participation in Installation Training Teams (ITT) and Regional Training Teams (RTT) are an integral part of all training exercises and should be part of all exercise planning. Vital planning begins with exercise objectives being identified by the CO. Major planning milestones for the exercise process are the Concept Development Conference (CDC), Initial Planning Conference (IPC), Mid-Planning Conference (MPC) and Final Planning Conference (FPC). The major phases of the exercise process are Design, Development, Conduct, and Evaluation. Additionally, exercises will incorporate Operational Risk Management (ORM) strategies as an integral part of planning and execution for all participating
personnel, military and civilian. Planning assistance is available through the CNIC N72 and additional planning information is contained in reference (pp).

0805. **Exercise Schedule**

a. The SRTP provides the framework for REGCOM’s and CO’s to execute the Shore Response Plan (SRP) in meeting routine Navy operations, surge requirements and NCC war fighting tasks. The Shore Response Training Plan (SRTP) serves as the linkage to create a consistent, standardized and reliable approach to conduct planning and execution of exercises and training events.

b. CNIC approach for shore training follows the Navy Warfare Training System (NWTS) cycle of Requirements, Planning, Execution, and Assessment of all training events associated with the Shore Enterprise. These events range from individual training, unit level and multi-unit integrated training events using a variety of training and exercise venues.

c. CNIC has provided policy and guidance to installations that they will participate in monthly Unit Level and integrated training exercises. Installations will participate in four integrated training events each year: two installation-wide integrated training events and two major exercises (one enterprise wide exercise such as Citadel Shield, and one region directed exercise, such as Citadel Gale or Citadel Rumble). See Table 8-1 below.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Periodicity</th>
<th>Type</th>
<th>ROC Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>Monthly</td>
<td>Drills, FTX</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>Integrated</td>
<td>Monthly</td>
<td>TTX, FTX</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>Reliant Series</td>
<td>Minimum Two Per Year</td>
<td>TTX, FTX, CPX</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>Citadel Series</td>
<td>Minimum Two Per Year</td>
<td>TTX, FTX, CPX</td>
<td>1,2,3,4</td>
</tr>
</tbody>
</table>

d. Training drills and exercises will be exercised based on installation scheduled unit level training, and monthly integrated training via the installation PB4T.

e. Unit Training Requirements. Operations based exercises such as drills and FTX are designed to validate personnel and
equipment performance in achieving critical tasks. Unit level training will be conducted and documented into NTIMS as required.

f. Assessment of Unit Level Training will be done under the Reliant Series sub events within the execution module curricula tree. All training should be assessed and documented via NTIMS collection plan to provide DRRS-N T-Pillar Training Readiness (Tr) data.

**0806. Exercise Design**

a. Training exercises should be realistic and address the full spectrum of natural and man-made emergencies and incidents, in addition to CBRNE and terrorist attack. Incorporating various federal, state and local agencies establishes common procedures which increase interoperability and exercises procedures used during actual events. Establishes common operating procedures and ensures synchronization and focus of effort. It also establishes common operating procedures and ensures synchronization and focus of effort.

b. Exercise design and evaluation shall be performed per CNIC N7 guidance. N7 exercise program is aligned with Homeland Security Exercise and Evaluation Program (HSEEP). Regions and ROC 1 installations should receive external, objective exercise design and evaluation support due to the increased scope and complexity of their assigned mission and capabilities. This exercise design and evaluation function may be completed using contract support, regional personnel, other service, or U.S. Government support or a combination of these options. ROC 2 installations shall request regional assistance in design and evaluation of their assigned exercises. ROC 3 installations shall use a template design for their annual Tabletop Exercise (TTX) requirements and conduct a self-evaluation. Regions shall program accordingly.

**0807. Exercise Types**

a. Drills, TTXs, operations center exercises, and AT exercises are required types of exercises, determining whether or not a unit is validated or requires additional training.

b. Exercises will be organized by the REGCOM or CO and should increase in complexity over time, depending on turnover ratio. All training will use practical exercises to present
real-life scenarios that challenge security force participants with realistic and increasingly complex situations designed to reinforce and require application of the principles and techniques learned in the classroom.

c. Commanders have the discretion to implement any mode or type of exercise they see fit, but each exercise will build on previous exercises using more sophisticated techniques and requiring more preparation time, personnel, and planning.

d. The exercises the REGCOM/CO mandates do not limit or modify existing exercise requirements of existing programs, such as Fire and Emergency Services and Navy Medicine. Regions and installations will continue to conduct regularly scheduled annually and semiannually exercises mandated for existing programs while ensuring that these exercises support the federal, state, and local PS and LE agencies and programs.

e. Table 8-2 provides a comparative overview of exercise types.
### Table 8-2

#### Exercise Component Overview

<table>
<thead>
<tr>
<th></th>
<th>Orientation</th>
<th>Drill</th>
<th>Tabletop Exercise</th>
<th>Command Post Exercise</th>
<th>Field Training Exercise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Format</strong></td>
<td>Informal discussion in group setting various presentation methods</td>
<td>Actual field or facility response, actual equipment</td>
<td>Narrative presentation, problem statements or simulated messages, group discussion, no time pressures</td>
<td>Interactive, complex, players respond to messages (events/problems) provided by simulators, realistic but no actual equipment, conducted in real time, stressful</td>
<td>Realistic event announcement, personnel gather at assigned site, visual narrative (enactment), actions at scene serve as input to Regional Operations Center/Emergency Operations Center (EOC)/Incident Command Post (ICP) simulation</td>
</tr>
<tr>
<td><strong>Leaders</strong></td>
<td>Facilitator</td>
<td>Manager, supervisor, department head, or designer</td>
<td>Facilitator</td>
<td>Controller</td>
<td>Controller(s)</td>
</tr>
<tr>
<td><strong>Participants</strong></td>
<td>Single agency/department, or cross-functional</td>
<td>Personnel for the function being tested; may include coordination, operations, response personnel</td>
<td>Anyone with a policy, planning, or response role for the type of situation used</td>
<td>Players (policy, coordination, and operations personnel), simulators, evaluators</td>
<td>All levels of personnel, (policy, coordination, operations, field), evaluators</td>
</tr>
<tr>
<td><strong>Facilities</strong></td>
<td>Conference room</td>
<td>Facility, field, Regional Operations Center, Installation EOC, Medical Treatment Facility (MTF) EOC, or other facility</td>
<td>Large conference room</td>
<td>All C2 nodes, (Regional Operations Center, Installation EOC, MTF EOC, Dispatch Center, EOC) (multiple rooms)</td>
<td>Realistic setting, all C2 nodes</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>1–2 hours</td>
<td>1–2 hours</td>
<td>1–4 hours</td>
<td>3–8 hours or longer</td>
<td>2 hours to 1 or more days</td>
</tr>
<tr>
<td><strong>Preparation</strong></td>
<td>2 weeks</td>
<td>1 month, participants need orientation</td>
<td>1 month, preceded by orientation and one or more drills</td>
<td>4-6 months, preceded by simpler exercises</td>
<td>6 months to 1 year, including preparatory drills, tabletops, functional exercises</td>
</tr>
</tbody>
</table>
0808. **Drill.** A drill is a creative, coordinated, and a supervised exercise activity (see Table 8-3). All drills can be tested within each mode, Alert or No Alert. Typically, most drills are used to test a single specific operation or function set by the commander. With a drill, there is no coordination with higher or lower support organizations. It is primarily used as practice event to give leadership a chance to validate one small part of the response plan. Small, individual drills help prepare for more extensive exercises in which several functions will be coordinated and tested in their entirety.

**Table 8-3**

**Drill Overview**

<table>
<thead>
<tr>
<th>Format</th>
<th>A drill is an actual field or facility response to a tested PS/LE operation. It will be as realistic as possible and employ all pertinent equipment and personnel for the function being tested.</th>
</tr>
</thead>
</table>
| Applications | Drills are used to test a specific operation. They are also used to provide training with new equipment, develop and practice new policies or procedures, or practice and maintain current skills. Drills are a routine part of the daily job and are held in the field, facility, or operations centers. Some examples of drills run by different organizations are:
  -- Operations Centers: Alert/procedures
  -- NSF: Locating/placing road barriers
  -- Selected Responders: Alert/mobilization/deploy drill
  -- SROE/Arms-carrying personnel |
| Leadership | A drill can be led by a manager, supervisor, department head, or exercise designer. Staff must have a good understanding of the single function being tested. |
| Participants | The number of participants depends on the function being tested. Coordination, operations, and response personnel could be included. |
| Facilities | Drills can be conducted within a facility, in the field, or at the EOC or other operating center. |
| Time | 1-2 hours is usually required, then a detailed after-action review follows, with a detailed log of three sustains and three improvements. |
| Preparation | Preparation may take as little as 5 minutes or about a month. Participants usually need a short orientation beforehand. |

0809. **Tabletop Exercise (TTX).** A TTX is a facilitated analysis of a PS or LE breach that is situated in an informal, stress-free environment (see Table 8-4). It is designed to elicit constructive discussion as participants examine and resolve problems based on existing operational plans and identify where those plans need to be refined when any such breach happens within the PS of a region or installation.
### Table 8-4
#### Tabletop Exercise Overview

| Format | - The exercise begins with the reading of an exercise scenario, which sets the stage for the hypothetical emergency. Then, the facilitator may stimulate discussion in two ways:  
  -- Problem statements: Problem statements (describing major or detailed events) may be addressed either to individual participants or to participating departments or agencies. Recipients of problem statements then discuss the actions they might take in response.  
  -- Simulated messages: These messages are more specific than problem statements. Again, the recipients discuss their responses.  
- The discussion generated by the breach of security or incident focuses primarily on how the participants would respond during a real-world incident, the plans, the coordination, the effect of decisions on other organizations, and similar concerns. Often maps, charts, and packets of materials are used as references to add to the realism of the exercise. |
| Applications | - TTXs have several important applications:  
  -- Lend themselves to low-stress discussion of coordination and policy.  
  -- Provide a good environment for problem solving.  
  -- Provide an opportunity for key personnel to interact and share their interrelated roles, respective responsibilities, and suggestions. |
| Leadership | - A facilitator leads the discussion. This person calls on others to participate, asks questions, and guides the participants toward sound decisions, while providing subject matter experts to mediate between different agencies and their practiced methods. |
| Participants | - The objectives of the exercise dictate who should participate. The TTX may involve many people and many organizations. Essentially anyone who can learn from or contribute to the planned discussion items. Participation may include all entities that have a policy, planning, or response role. |
| Facilities | - A TTX requires a large conference room or hanger where participants can surround a table or a large open area where a sand table can be created. |
| Time | - Usually lasts 1–4 hours. Discussion times are open-ended, and participants are encouraged to take their time in arriving at in-depth decisions without time pressure. |
| Preparation | - It typically takes about a month to prepare for a TTX. Preparation also usually requires at least one orientation seminar or an Intermediate Progress Review and one or more drills. |

**0810. Command Post Exercise (CPX).** A CPX is a fully simulated interactive exercise that tests the capability of an organization and its supporting federal, state, and local PS/LE agencies to respond to a simulated event, short of moving real people and equipment to an actual site (see Table 8-5). The exercise tests multiple functions of the organization's operational plan and strategic planning capabilities and how well they can coordinate a response to the situation/incident in a time-pressured, realistic simulation.
Table 8-5
Command Post Exercise Overview

| Format | This is an interactive exercise—similar to an FTX without the equipment. It simulates an incident in the most realistic manner possible short of moving resources to an actual site. A CPX is:
| Format | -- Geared for policy, coordination, and operations personnel - the "players" in the exercise - who practice responding in a realistic way to carefully planned and sequenced messages given to them by "simulators." The messages reflect ongoing events and problems that might actually occur in a real emergency.
| Format | -- A stressful exercise because players respond in real time, with on-the-spot decisions and actions. All of the participants' decisions and actions generate real responses and consequences from other players, which are all logged and evaluated.
| Format | -- Complex - Messages must be carefully scripted to cause participants to make decisions and act on them. This complexity makes the CPX more difficult to design than a TTX.
| Applications | CPXs make it possible to test several functions and exercise several agencies or departments without incurring the cost of a full-scale exercise. In some instances, taking part in a CPX may serve as a full-scale exercise for a participating organization (e.g., a Military Working Dog Team may conduct its own FTX as part of a regional/installation CPX).
| Participants | CPXs are complex in their organization of leadership and the assignment of roles. The following general roles are used:
| Participants | -- Controller: Manages and directs the exercise, should be Incident Commander.
| Participants | -- Players: Participants who respond as they would in a real emergency. (Players should include policy makers; may include coordinators and operational personnel directing field activities.)
| Participants | -- Simulators: Assume external roles and deliver planned messages to the players.
| Participants | -- Evaluators: Observers assess and log the performance of an individual and the supporting agency.
| Facilities | Usually conducted in the Regional Operations Center, Installation EOC, MTF EOC, Regional/Installation Dispatch, the EOC, Security detachment, and/or other operating centers. Players and simulators are often seated in separate areas or rooms. Realism is achieved by the use of telephones, radios, televisions, computers, and maps.
| Time | Requires 3–8 hours, although it can run a full day or even longer.
| Preparation | Plan on 4-6 months to prepare for a CPX, for several reasons:
| Preparation | -- Staff members need considerable experience with the functions being tested.
| Preparation | -- The exercise should be preceded by lower-level exercises, as needed.
| Preparation | -- Controller, evaluators, and simulators require training.
| Preparation | -- The exercise may require a significant allocation of resources and a major commitment from organizational leaders.

0811. Field Training Exercise (FTX). The FTX is an event in which all resources, all leadership, and all strategic assets are used to validate each supporting agency’s performance capabilities during an operational breach of PS or an LE incident (see Table 8-6). The exercise examines and relates to a real-world event as closely as possible in a highly stressful environment that simulates actual response conditions. The
coordination and mobilization of actual LE personnel, equipment, and resources is a must. The FTX tests and evaluates most functions of the regional and/or installation PS and LE plans.

<table>
<thead>
<tr>
<th>Format</th>
<th>The exercise begins with a no-warning alert or warned alert with a description of the event communicated to responders in the same manner as would occur in a real event. Personnel must report to their assigned locations, where mock incident/ scenario has been created. Actions taken at the scene serve as input to the simulation taking place at the Regional Operations Center, Installation EOC, MTF EOC, Regional/Installation Dispatch Center, and/or EOC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>FTXs are the ultimate in functional area evaluation. Because they are expensive and time-consuming, it is important that all viable resources can and will be used in support of this very important performance-validating operation.</td>
</tr>
<tr>
<td>Participants</td>
<td>One or more controllers manage the exercise, and evaluators are required at every station. All levels of personnel and supporting agencies take part in the FTX: policy, coordination, operations, and personnel</td>
</tr>
<tr>
<td>Facilities</td>
<td>The event unfolds at the Regional Operations Center, in a realistic setting. The Installation EOC, Security detachment, Regional/Installation Dispatch Center, and EOC are activated, and supporting federal, state, local, other service, private (and/or host-nation) command centers support the exercise.</td>
</tr>
<tr>
<td>Time</td>
<td>A full-scale exercise may be designed to be as short as 2–4 hours or to last as long as two or more days.</td>
</tr>
<tr>
<td>Preparation</td>
<td>Preparation for an FTX an extensive investment of time, effort, and resources, usually six months to a year to develop a complete exercise package. This time frame includes multiple drills and a preparatory TTX and CPX. In addition, personnel and equipment from participating agencies must be committed for a prolonged period of time.</td>
</tr>
</tbody>
</table>

**Table 8-6**

Field Training Exercise Overview

0812. **Regional Training Teams and Installation Training Teams.** In coordination with CNIC N7, NSF personnel will establish and participate in exercises that meet NMET requirements and ensure this data is recorded in DRRS-N. Exercises will range from AT-centric to all hazards. RSOs, ISOS, and ATOs will coordinate with respective N7 Regional and Installation Training Officers (ITO).

0813. **Orientation Seminar.** An orientation seminar (see Table 8-7) is an introductory event that familiarizes personnel and civilian participants with roles, plans, procedures, or equipment. It also can be used as Intermediate Progress Review to help resolve questions of coordination and assignment of responsibilities within the different personnel and different agencies that are participating.
Table 8-7
Orientation Seminar Overview

| Format | The orientation seminar is a very low-stress event, usually presented as an informal discussion to familiarize and coordinate between different participating personnel and agencies. A variety of seminar formats can be used: lecture, discussion, slide or video presentation, computer demonstration, panel discussion, guest lecturers. |
| Applications | The orientation seminar can be used for a wide variety of purposes, including: -- discussing a topic or problem in a group setting -- introducing new policies and plans -- explaining existing plans to personnel new and old who require an explanation of the regional/installation protection program and their role at their assigned location -- orientation to operational plans as they relate to incidents and emergencies -- introducing a cycle of exercises |
| Leadership | Orientations are led by a facilitator, who presents information and guides discussion. |
| Participants | A seminar may be cross-functional, involving one or two participants for each function or service being discussed (e.g., regional/installation leadership, policy, coordination, and operations staff). |
| Facilities | A conference room or any other fixed facility may be used, depending on the purposes of the orientation. |
| Time | Orientations should last a maximum of 1–2 hours. |
| Preparation | An orientation is quite simple to prepare (two weeks' preparation time is usually sufficient) and conduct. |

0814. Evaluation. Evaluation is an important functional element of the exercise program (e.g., ensuring accurate assessment and subsequent identification of issues discovered during an exercise, training event or real-world incident). This evaluation provides the data required to determine lessons learned and best practices which will be fed back into the exercise planning process. This feedback is provided through accurate reporting of the observations and recommendations (O&Rs) in an after action report (AAR). AAR submission at the installation level or higher is the primary source for data entry into the Shore Lessons Learned Program (SLLP), established for the collection and dissemination of O&Rs generated by exercises, training events and real-world incidents. Negative O&Rs deemed systemic across the CNIC enterprise are entered and tracked within the Shore Issue Resolution Process (SIRP) to enhance Shore Force readiness.

a. The SLLP resides within the Joint Lessons Learned Repository (JLLR) and provides regions and installations access to all shared information maintained within the repository. Knowledge gained from review and thorough understanding of
previous lessons learned will assist Commanders to improve situations, techniques, and/or processes to better perform assigned tasks and/or missions. The overall quality of information within the SLLP will always be directly linked to the quality of submissions received via AARs and the rigor of the SIRP.

b. The AAR shall be a composite product based on input provided by nonpartisan evaluators that are either trained or are subject matter experts (SME) within the specific area they are evaluating. AARs shall be maintained for a minimum of three years at the installation and/or regional level for AT and other FP mission related exercises, training events and real-world incidents. AARs should result in lessons learned that are prioritized based on CNIC guidance and incorporated into existing programs. The AAR shall be submitted in accordance with the following guidelines: Regions will submit a naval message AAR(s) to CNIC N3 and N7, using the AAR format provided in paragraph (c) below, not later than 30 days following an exercise, or as directed for real-world events.

c. All AAR’s prepared should use the following format and when necessary be classified at the appropriate level depending upon the detail and granularity of the AAR:

(1) Overview. Provide a general description of the exercise or event; exercise objectives; key dates; location of exercise, and participants.

(2) Topic/Issue. Provide a short title of the issue observed.

(3) Observation. Provide a factual description of the observed issue or success. Explain what procedure or process conducted inside the exercise/event caused the observation. Define how your command reacted to the procedure or process. Further explain why and how this observation has either a positive or negative impact to operational readiness. Identify if this observation is systemic across the CNIC enterprise or an isolated incident. Limit each submission to a single issue, or action.

(4) Discussion. Provide amplification of facts and details relating cause of the observation that answers who, what, where, when, why and how elements about the observation. In this amplification, link the observation elements (i.e. flow of events, facts, TTP, PPR, analysis and assessment results) to
the instruction, regulation, operational plan (OPLAN) or operational order (OPORD) guidance, which were used to determine that these problems/issues were valid deficiencies. When citing these references, include the version date, series or edition used chapter, page and paragraph. Describe how guidance is either adequate or inadequate. If no higher level guidance exists, describe how that affected the observation.

(5) Recommendation. If it is a negative observation and the guidance is inadequate, provide detailed verbiage to improve the current guidance in the instruction/regulation/OPLAN/OPORD. If it is a positive observation, provide recommended procedures/policies, as a best practice, to reiterate across the CNIC enterprise as a lesson learned. It may suggest a new way of doing something, or a way of doing something in spite of the problem causing the issue (e.g., new TTP, PPR, process, or equipment setting). If it is a materiel issue, recommend a solution and describe why it should receive resource priority. Identify if your command intends to submit resource allocation module input to address the observation.

(6) Implications. Provide a statement to reflect what happens if your recommendation is not adopted.
0901. **Mission.** CNIC has developed the MPV-P to be utilized when funding protection positions in connection with reference (a). The MPV-P consists of several parts used in tandem to complete the assessment process. Each part is designed for a specific purpose and contributes to the ultimate end state which is the predictive staffing requirement for a region, installation (precinct), or non-contiguous fence lines of an installation (entity). The MPV-P replaces the Security Post Validation calculation and is a method to determine each region’s and installations actual requirement of limited resources. The MPV-P is intended to provide CNIC with an improved capability to distribute manpower resources for the CNIC Navy security workforce to maximize NSF mission and functional capability within budgeted resources.

0902. **Concept.** The Microsoft Access® based model generates region and installation level staffing templates that aggregate numerous considerations and factors, specifically assets and risk in the form of ROCs, Capability Performance Levels (CPLs), FPCONs, geographical location, workload, workforce mix, productivity factors, and AT work factors and staffing standards. An Excel® spreadsheet called the Data Collection Workbook (DCW) is populated by the precinct and submitted for import into the model. MPV-P is a flexible model that allows greater accuracy and granularity of installation staffing at all FPCONs.

0903. **Process.** The model uses staffing levels developed using the following criteria.

   a. NSF Workweek Factor. The MPV-P assumes a 24-hour work day as the basis for calculating the required hours for a 24 hours per day, seven days per week post requirement. CNIC determined that in large part the civilian workforce was either (1) being paid overtime for this time as required by law or (2) had the shift differential subsumed in alternative shifts of greater than 8 hours. Even when post personnel were relieved by other NSF personnel to take a meal break (and thus worked and were paid for only 8 hours), relief personnel were often already on watch as part of that shift (perhaps a rover or supervisor) and merely swapped posts (with the patrol "on call" while taking a meal). For military, it was assumed that shift differential time was similar to any other watch turnover at any station and was effectively part of their required work day.
b. Productive Workweek Factor. The MPV-P uses a productive workweek factor (PWF) of 34.38 for military, 33.68 for federal civilian, and 40.00 hours for contract watch standers. These revised MPV-P figures are calculated pursuant to reference (rr) and are based on training requirements, leave and other diversions as time not available in the standard workweek. IAW reference (rr) guidance for watch standers (e.g., firefighters), the MPV-P does not subtract holidays as non-available time when calculating the PWFs. The resourcing impact of the revised NSF workweek and the various PWFs is that a 24/7 post requires approximately five (or fewer for contractors) full-time equivalents.

c. The number of security patrol units required to support the AT mission is determined by considering the following indicators: assets to be protected, workload, performance (required response times) and minimum capabilities.

(1) Calls for service are used to determine the additional patrols required, however, a detailed analysis of calls for service is conducted by the MPV-P team. The analysis encompass not just one aggregate number, but examines the calls by numbers and frequency of calls in three categories: major crimes against person or property (rape, murder, burglary, breaking and entering, etc.), lesser crimes or noncriminal offenses (suicide and attempted suicide, destruction of property, disorderly conduct, etc.) and more routine offenses or complaints (vehicle accidents, abandoned vehicles, misuse of government property, lockouts, housing complaints, etc.). This analysis is considered as part of the Risk Assessment for establishing mobile patrols, particularly backup patrols for lower ROCs and outlying areas with minimal assets to protect.

(2) The MPV-P considers that patrol zones in populated areas should provide an average response time of 15 minutes to emergent situations. For non-populated areas, the MPV-P provides appropriate response to the asset (i.e. 15 minutes for AA&E). The MPV-P includes risk analysis in the overall determination of patrol staffing.

(a) The current OPNAV procedure defines response time speed as “safe speed” and eliminates a set speed limit for code calls. For the sake of initial planning, the patrol zone is drawn as a circle with an 8.8 mile diameter (estimating a 35 MPH speed). This can be adjusted based on actual geography and likely speeds under normal conditions. The patrols are first
based on assets but may be based on geography to provide full coverage of the installation/fence line. Based on these criteria, bases of similar size and ROC level can have a different number of patrols simply because of differences in speed limits on the respective installations.

(b) The MPV-P assumes patrols will respond to emergencies based on speeds commensurate with type of emergency, weather conditions, time of day, traffic conditions, and other factors, and an exact patrol size cannot be determined.

(3) The MPV-P considers supervisors as backups and does not staff a patrol and backup for each patrol zone. Based on ROC level, however, a backup patrol may also be validated to provide support for multiple simultaneous incidents.

d. Staffing for other mobile patrols which include additional mobile patrols that provide coverage to areas including controlled industrial areas, off-base housing, and overseas schools, is utilized in the calculation as applicable.

e. ECP resourcing. Every installation with a gate and perimeter fencing or barrier will have at least one primary external vehicle access control point automatically resourced for 24 hours a day, 7 days per week. Any secondary external vehicle access control points will be resourced by workload. Vehicle gates in operation with a usage of 29 or less vehicles per hour will not be resourced.

(1) Vehicle gates and pedestrian gates are considered separately even when co-located.

(2) Each post will be individually assessed and resourced to support the workload and security requirements of the post.

(3) The MPV-P considers peak coverage hours, normally for ingress and also includes cover sentries for external perimeter ECPs during increased FPCONs.

f. Commercial Vehicle Inspection Team (CVIT) staffing covers the commercial vehicle inspection requirement (OUTUS). It is based on the commercial vehicle workload (i.e. numbers and types of vehicles) and, where volume and traffic flow dictate, traffic engineer analysis and requirements. The CVIS will not normally be validated where throughput is less than 30 commercial
vehicles per day. Mobile Vehicle Inspection Teams (MVIT) can be used to satisfy the CVIS requirement for those installations.

(1) Vehicle inspection types are administrative, intermediate and complex.

(2) Resourcing will consider the three levels of inspections based on the ROC, COL, and FPCON for the installation.

g. MVIT standards are consistently being accomplished at ECPs and the CVIT entrance. These two levels of inspection substantially satisfy much of the FPCON measures required and mitigate the need for the high staffing for MVIT/ECP vehicle inspections at FPCON BRAVO. Absent overriding circumstances, the MPV-P resources FPCON BRAVO with one three-person team, for 40 hours per week at all installations. FPCONs CHARLIE and DELTA are based on gate operating hours. However, of particular note, the MVIT in CONUS, HI, and CJR Marianas fall under non-guard services contract and are not generated from the model. In these cases the guard authorization is input directly into the precinct/entity validation based on the input from the NGS Program Manager.

h. Harbor protection and flight line security patrols are resourced separately from security and other mobile patrols.

(1) Harbor protection resourcing will be based on assets being protected; fields of fire, patrol boats assigned, and automated ECPs when piers are enclaved. Average pier loading and type of asset is considered in determining posts for pier access control.

(2) Patrol boats will be assigned to installations required to protect afloat assets. The number of patrol boats assigned and the personnel required to man them will be based on type of assets to be protected and waterfront area to be patrolled. Basic crew up to FPCON BRAVO is two personnel (coxswain and crew member).

(3) Pier access points that are not automated will be staffed with at least one Armed Sentry (AS).

(4) When flight lines are enclaved, all automated entry control system-enabled and closed-circuit television (CCTV) systems are monitored, no staffing is resourced. Monitoring of CCTV is performed by dispatch personnel.
(5) ECPs into flight lines will have a single AS during normal work hours. The DCW provides all hours of operation of flight line control points, and MPV-P estimates staffing based on those hours of operation.

i. Investigators will be resourced based on number and complexity of cases averaged annually.

(1) All investigations will be coded as complex, intermediate or simple in accordance with reference (a).

(2) A 12-month period of data will be utilized.

(3) Investigators will be resourced commensurate with the total aggregate investigation hours for the entire 12 months.

(4) Commands not meeting the minimum workload for full-time investigators shall train collateral duty investigators.

j. Military Working Dogs (MWD) staffing includes explosive detection and drug detection dog (EDD/DDD) teams. There are also special staffing requirements for regional kennels and for deployable support.

(1) Regional kennel requirements are built into the MPV-P.

(2) Although EDD and DDD use separate matrices, input for MWDs are provided by the Navy MWD Program Manager (NECC). These requirements are input directly into the Working Dogs section of MPV-P. NECC MWD PM also provide the requirement for Kennel Staffing (Kennel Master, trainers).

(3) Canines used exclusively as Patrol Dogs are not included in the matrix.

k. Emergency Operation Centers. ROC 2 installations will be staffed to operate an operation center on a 24 hour/7 day basis, with the number of personnel based on the number and complexity of installed systems (telephones, area notification system, Non-secure/Secure Internet Protocol Router Network, etc.).

l. Other staff resourcing for administrative and support staff (i.e. Pass and ID and Armory/Range Operation) requirements
are so divergent that each location will be resourced by trained CNIC manpower personnel using workforce staffing delineated in paragraphs 0903 a and b above based on the unique region/installation requirements for OCONUS installations. CONUS, Hawaii and Guam NGS personnel requirements are provided by the NGS Program Manager.

m. No dedicated surveillance detection (SD) personnel will be resourced at CONUS installations. Staffing for overseas installations will be determined by the other staffing matrix on a case-by-case basis. SD in CONUS will be handled as a RAM, and all security personnel are expected to maintain situational awareness at all times.

n. Reaction Force resourcing will be determined in accordance with reference (a).

o. The MPV-P considers both reimbursable and non-reimbursable posts in the calculations.

0904. **Data Collection Workbooks**

a. Regions and installations will be provided with DCW to be completed based on their unique requirements. A minimum of two weeks of data are required for resource determination. This data is directly imported into MPV-P to establish initial protection points. Regions/installations are highly encouraged to continue to collect data as feasible since more data will increase the accuracy of the generated results.

b. After completion, the aggregate data will be analyzed by the MPV-P team and forwarded to CNIC N1 for creation of revised Statement of Manpower Requirements (SMR) that reflects resource funding. The RSO is responsible for ensuring all shore installations have a current post validation conducted. The post validation process establishes and validates the resources necessary to provide sufficient protection for the shore installation as mandated by higher headquarters, including the CNO, Navy Component Commanders, and CNIC.

c. Establishment of any new security positions following a valid post validation must be approved by the RSO and in some instances, CNIC N3AT. Some factors in determining the size of the security force include the following:

   (1) Size and location of the activity.
(2) Criticality of assets to be protected.

(3) Number of posts and the number of hours that each is validated.

(4) Degree of supervision that is appropriate considering the training and experience of security force members.

(5) Number, type, and size of restricted areas, including the number of separate ECPs.

(6) Use of alternative security support measures and effectiveness of mechanical or electronic security measures.

(7) Security force support provided by other agencies, including local, state, and federal support.

(8) Total daily population of the installation or activity and its composition, which affects the DCW workload.

d. Regional coordination and integration of security force requirements and employment to avoid unnecessary duplication of effort and confusion within the chain of command. A clear and simple chain of command must be established and accepted by all levels in the chain of command from the CO to the REGCOM.

0905. Determination of Posts

a. Guarding and security patrolling of areas must be commensurate with the importance of the area/assets being guarded and the threat. Since no two activities will present the same degree of risk or contain identical situations, it is impractical to set fixed rules to apply to all activities. However, the RSO must ensure every effort is made to establish uniformity and consistency in policy, gear (equipment, individual protective equipment, and security uniforms), vehicles, etc. across the region.

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

c. The security staffing standards as described in the MPV-P process are the approved and accepted standards for determining the manpower equation and rule of thumb in estimating the precise number of personnel required for a particular post.

d. The RSO must ensure a continuing review of the Protection Program is established for the region and installations. The review should be a systematic assessment, with specific goals and purposes, including the following:

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

(2) A Terrorism Threat Assessment is conducted at least annually by NCIS.

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

(4) Preparation of protection plans.

(5) Host/tenant coordination and agreements concerning efficient, dissimilar employment of mutually supportive PS resources and procedures.

(6) Preparation of Terrorism Incident Preplanned Responses Plan. Preplanned responses should be reviewed and exercised regularly.
CHAPTER 10
INTELLIGENCE SUPPORT

1001. Purpose. Commanders require timely and actionable intelligence/information, and when necessary/able, the preservation of an evidentiary foundation in order to ensure effective command decisions and action. Under the authority of the Secretary of the Navy, the NCIS has primary investigative and counterintelligence jurisdiction within the DON for offenses and incidents, on and off naval installations and aboard ships IAW reference (kk). This jurisdiction is grounded in federal statutes, Executive Orders, and DoD and Secretary of the Navy policy. To the extent possible and where there is a need for the region and installation antiterrorism and law enforcement personnel to compliment a fusion of threat information, the following procedures shall be implemented by REGCOM and CO.

1002. Overview. NCIS formulates Navy centric terrorist threat intelligence collection plans in order to answer terrorism specific Commander’s Critical Information Requirements (CCIR), and directs, coordinates, or requests U.S. and/or Host Nation (HN) intelligence and LE agencies to provide terrorist threat information based on the Commanders Priority Intelligence Requirements (PIR). In coordination with Public and Civil Affairs, directs, coordinates, or requests the provision of answers to HN related Friendly Forces Information Requirements (FFIR). In addition, they convert raw terrorist threat information into forms of intelligence suitable to support the Commander, provide timely terrorist threat intelligence in appropriate formats to the Commander, ATO, ISO/RSO and other Navy units and organizations based on the “responsibility to provide” IAW reference (kk).

   a. Occasionally the ATO or ISO/RSO may be required to provide their own threat assessment or other intelligence products due to time constraints and/or lack of resident NCIS capability.

   b. When an installation or region does not have adequate intelligence support to meet the requirements of this instruction, the regional RSO/ATO and installation ISO/ATO will inform the appropriate COC to include CNIC N3/N3AT and assume responsibility to provide intelligence support, to their utmost ability, until relieved. These procedures will be codified in the regional and installation AT Plan.
1003. **Intelligence Support Concept**

a. Intelligence provided in support of AT efforts attempts to ascertain the disposition and intentions of asymmetric actions potentially desiring to harm U.S. Navy facilities, personnel and/or mission. Detecting terrorist activities and methods require a high level of situational understanding, informed by current and precise intelligence. The terrorist threat drives the need for predictive intelligence based on analysis of information from intelligence sources, LE, security activities, and the observations of the population not only aboard CNIC installations but in the surrounding areas of the installation.

b. Antiterrorism intelligence will employ analytical methodologies and tools to provide situational understanding and to predict the adversary’s actions. Time event charts, association matrixes, activity matrixes, link diagrams, and overlays will be created to monitor the actions of the adversary.

c. NCIS provides U.S. Navy installations and regions with intelligence that supports AT decision making IAW reference (b). Region and installation staffs are obliged to apply this intelligence to their local protection posture. However, ATOs and RSO/ISOs have to be prepared to request specific targeted intelligence support from higher authority when necessary. This includes knowing what intelligence products provide what type of information. If intelligence gaps continue to exist, region and installation staffs are required to submit requests to their local NCIS office and/or the MTAC, with a courtesy copy of the request to CNIC N3AT.

d. Terrorist threat assessments will include “ground truth” evaluations of HN and local LE and intelligence agencies’ capabilities in accordance with the Commander’s FFIR.

e. Terrorist threat intelligence operations support the commander’s decisions concerning the creation and maintenance of major subordinate command AT Plans, installation AT Plans, FPCON execution, execution of RAM and the execution of other security related measures.

f. Most routine intelligence support requirements, primarily for planning, can and should be accomplished with the TWG IAW reference (d). TWG membership at a minimum shall include the ATO, the Commander (or a designated representative), members of
the staff, NCIS or other intelligence sources, RSO/ISO and senior NSF personnel, and appropriate representation from direct hire, contractor, local, state, federal, and host nation law enforcement agencies and others as needed.

g. An optional forum that is intelligence support related and highly effective when used properly is the Operations/Intelligence Fusion Cell. This cell combines intelligence analysis information and events of the previous period, usually monthly or quarterly, that predicts what will happen in the upcoming period. Operations personnel (N3, NSF, etc) then propose actions to mitigate the effect on the command by known or suspected upcoming events, such as demonstrations, civil disobedience, attacks, etc. Intelligence personnel then advise whether those actions could possibly compromise their sources. In most cases events are generally allowed to happen to a certain degree that has minimal effect on the command. The Operations/Intelligence Fusion Cell at the Installation and Region level generally consists of the N3, NCIS or other intelligence source, NSF, local/HN LE and intelligence personnel, civil affairs, public affairs, etc, and others that may contribute at any given time.

1004. Planning and Direction

a. NCIS will review PIR and FFIR developed by the ATO/RSO/ISO to determine intelligence requirements, including the requirements of subordinate commanders, to prepare a collection plan, issue orders, and formulate requests to information collection agencies. NCIS will monitor the performance of collection agencies in order to correlate their products, conduct analysis, and produce assessments which explain the “so what” for Navy Commands.

b. Commander’s Critical Information Requirements (CCIR) process.

(1) Standing CCIR’s are developed, disseminated, and answered during operational phase one Pre-Incident AT operations.

(2) Crisis specific CCIR’s are developed and tasked from the onset of a terrorist incident and for the duration of the emergency incident response during operational phase two, installation/command-level emergency incident response, Consequence Management (CM).
(3) Reevaluation of standing CCIR is conducted during operational phase-five, after action tasks. New standing CCIR’s will be developed, published, and tasked.

c. Priority Intelligence Requirements (PIR). To provide terrorism information that enables the Commander to make risk and planning decisions concerning the Command AT Program, and for commanders at subordinate Commands to formulate and periodically update Command AT Plans.

d. Friendly Forces Information Requirements (FFIR). IAW reference (ii) FFIR is defined as information the commander and staff need to understand the status of friendly force and supporting capabilities. It provides a “ground truth” view of HN and local capabilities to combat terrorism. The U.S. military community has made assumptions about HN/local capabilities that may or may not be accurate. The Navy relies on the HN/local LE/intelligence for terrorism related information as a development tool of AT Plans. To this end, HN and local capabilities must be realistically assessed and, if required, courses of action developed to mitigate deficiencies.

e. Essential Elements of Friendly Information (EEFI). This is information enemy forces want to know about friendly forces in order to plan and execute an attack. Essentially, these are the enemy commander’s PIR.

f. New intelligence requirements. Provide specific guidance for new intelligence requirements during each operational phase of AT operations.

g. CCIR development and support for major crisis. The support for incident response operations at the various Operation Centers include vertical and horizontal flow of information. Procedures and tasks will be documented in the OC SOP, which is formulated and maintained by the N3.

h. Production. NCIS develops internal policies and procedures to analyze and report collected intelligence information, by all collection sources, in support of the AT mission. This includes multidiscipline reports which fuse information from multiple sources. Reference appropriate regulations, directives, and standing operating procedures specifying U.S.-only, and multinational reporting procedures. Identify the production effort, including any intelligence and counterintelligence products, required to support this instruction.
i. Dissemination. NCIS ensures the widest possible dissemination of terrorist threat information to commanders, staffs, and units. If the RSO/ISO is not receiving sufficient NCIS support an internal SOP will be developed which will document procedures and criteria to satisfy expanded requirements for vertical and lateral dissemination of finished intelligence products and SPOT reports. Alternate means will be established to ensure the required intelligence products are provided during all operational phases of the AT mission. The SOP will include:

(1) Intelligence reports required from commanders of installations and units.

(2) Formats for intelligence reports.

(3) Distribution of intelligence products.

(4) Requirements for release of terrorist threat intelligence to HN and local agencies.

(5) Requirements for secondary imagery dissemination.

1005. **Tasks.** To insure intelligence information is accurately collected and disseminated requires certain commands, departments and individuals to be responsible to the task at hand. The following information will describe primary task responsibilities of NCIS and in order to enhance this information, the tasks become the responsibility of the RSO/ISO if applicable.

a. The NCIS responsibilities include, but are not limited to.

(1) (FOUO) Formulate and execute a collection plan to task or “ask” collection requirements to organizations in accordance with terrorism related standing PIR’s. Standing PIR’s are developed during operational phase one by the region or installation Operations Officer N3 in collaboration with other primary staffs and approved by the commander.

(2) (FOUO) Office of Primary Responsibility (OPR) to plan, coordinates, and executes Navy centric, antiterrorism intelligence operations. Coordinate and establish lines of communications to receive terrorist threat information with
NCIS, Navy intelligence and other U.S. Military service components’ LE and intelligence agencies.

(3) (FOUO) Establish lines of communications to receive terrorist threat information from HN/local LE and intelligence agencies.

(4) (FOUO) Use all legal means to determine the presence, organization, activities, capabilities, equipment, weapons, area of operations, objectives, likely pre-strike activities, indicators, likely targets, the most likely courses of action, and the most dangerous courses of action of potential terrorist threats.

(5) (FOUO) The end state of this effort will be Navy centric, location specific and “outside the wire” terrorist threat assessments that will be used by commanders to formulate AT programs, AT Plans, FPCON execution, RAM execution, security budgets, and commander’s assumption of risk.

Note: “Navy centric” does not mean Navy only. TTP used worldwide must be studied because terrorist TTP successfully executed in one region of the world are inevitably used in other regions and may manifest in Navy Areas of Operation.

(6) Is the OPR to facilitate the TWG IAW reference (d)

(7) During emergency incident response and FPCON CHARLIE/DELTA, is a member of the Crisis Intelligence Cell as part of the installation EOC/region ROC.

(8) Executes collection of the commanders CCIR, counterintelligence, counter surveillance, and surveillance detection operations in support of this instruction and IAW reference (d).

(9) Provide terrorist threat assessments and ensure the widest possible dissemination to all personnel with a valid “need to know”.

(10) (FOUO) Formulate a collection plan for PIR and HN related FFIR during AT training exercises, an actual terrorist attack, and during the execution of FPCON CHARLIE and DELTA.

(11) Ensure dissemination of HN centric threat assessments to warn Navy REGCOM and CO of specific, credible threats.
(12) (FOUO) With assistance of the ATO and Security Officer, develop a process to identify potential internal threats to the command. This may be caricaturized as being a “loner” or displaying behavior that indicates a possible radicalization. Prior to travel and during an individual’s pre-departure brief on the localized threat in the area he/she is going, determine if the individual is going to an area that is frequented and/or occupied by radical elements and if any radical event is happening during the time period they will be there. Upon return to the command, conduct a thorough debriefing to determine if the individual can answer any PIRs or IRs related to the area visited, and if the individual had or possibly had any contact with radical elements.

(13) Is the OPR for Navy collection activities in support of PIR and HN/local related FFIR.

(14) Document RFI procedures for each operational phase of the AT mission in an internal SOP that will include RFI to higher, adjacent, and cooperating units.

(15) Develop, within their internal SOP, procedures for the distribution of intelligence products that includes the conditions, dates, and periodicity. These SOPs will include keeping the ATO, RSO/ISO and command informed of any legitimate threats.

(16) Develop and maintain, through the Crisis Intelligence Cell/Threat Working Group (CIC/TWG), the intelligence collection plan for installation/region.

(17) Assume intelligence collection lead in development of terrorist threat information collection for installation/region. Serve as member of the CIC/TWG.

(18) Assume intelligence lead in coordinating intelligence requirements with national intelligence agencies (CIA, NSA, DIA, etc.) consistent with DoD and U.S. Government guidelines.

(19) Develop PIRs with information requirements (IRs) and specific information requirements (SIRs) consistent with standard intelligence collection practices. Utilize PIRs, IRs, and SIRs in the installation/region intelligence collection plan as needed.
(20) Develop additional PIR’s as required for clarity, simplicity, specific situations, or other operational requirements. If additional PIR’s are developed, list the specific overlay.

(21) Advise and assist the CIC/TWG and other intelligence production activities in the development and review of terrorist threat intelligence requirements. Provide updates as needed.

(22) Review, at least annually, the Threat Information Collection Plan for installation/region. Update as needed.

(23) Serves as the lead coordinating agency for development and dissemination of law enforcement information. The RSO/ISO will work in concert with NCIS. Consequently, unless specifically identified as foreign intelligence, all threat information will be handled as “Law Enforcement Sensitive” until further classified. In cases of questions or uncertainties, NCIS will make a disposition determination consistent with existing law, regulations, and directives.

(24) (FOUO) Develop, maintain and review at least annually, through the CIC/TWG, the surveillance detection plan for installation/region.

(25) (FOUO) Assume information fusion lead in development of surveillance detection information fusion for installation/region. Serve as a member of the CIC/TWG.

(26) (FOUO) Serves as the lead coordinating agency for development and dissemination of foreign intelligence information. Within CONUS, unless otherwise directed, no information developed through this plan will be considered foreign intelligence.

(27) (FOUO) Provide counterintelligence (CI) awareness briefings to installations, regions and tenant commands on an annual basis.

(28) Advise the REGCOM/CO and appropriate installation/region subordinate commanders on matters affecting the security of the installation/region.

(29) Collect threat information to provide installations/regions with early warnings of threats.
(30) Report threat data and security hazards promptly to the N3/RSO/ISO/ATO, or designee, providing evaluation and analysis within capabilities.

(31) Refer CI matters involving civilian employees of installation/region to the FBI for investigation and disposition, in accordance with the "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation".

(32) Maintain direct contact with the FBI to obtain information on terrorist related incidents, and other matters concerning the security of installation/region and its activities.

(33) Develop and maintain, through the CIC/TWG, the intelligence fusion plan for installation/region.

(34) (FOUO) Assume intelligence fusion lead in development of terrorist threat information fusion for installation/region. Serve as a member of the CIC/TWG.

(35) (FOUO) Assume intelligence lead in coordinating intelligence fusion with national intelligence agencies (CIA, NSA, DIA, etc. and host nation intelligence activities where applicable), consistent with DoD and US Government guidelines.

(36) Forward all information requests of suspected terrorist threats, or acts of terrorism involving DoD personnel or assets through national intelligence networks (and host nation intelligence activities where applicable), consistent with DoD and U.S. Government guidelines.

(37) Forward timely requests for information to intelligence collection and production activities when local information indicates intelligence gaps.

(38) Advise and assist the CIC/TWG and other information fusion activities in the development and review of terrorist threat information fusion requirements. Facilitate the flow of information between the RSO/ISO, ATO, N3 and the national intelligence agencies regarding criminal and terrorist threats. EXTREME caution and care must be taken to ensure complete compliance with intelligence oversight directives while providing support to the installation AT Program. Provide updates as needed.
(39) Review, at least annually, the Threat Information Fusion Plan for installation/region. Update as needed.

(40) (FOUO) NCIS’s Threat Management Unit (TMU) will be an integral part of the Threat Assessment process. They will provide quarterly briefs/assessments to the RSO/ISO and ATOs on the internal threats to their regions/installations. These briefs and/or assessments will include not only current threats but any trends that are present. They will also provide current indicators which can be used to assist in identifying individuals who routinely have access to the installation that could potentially do harm to CNIC personnel. These indicators will be provided to NSF personnel especially those at ECP.

b. ATO tasks include the following:

(1) OPR to develop, periodically update, and seek command approval of terrorism specific Standing CCIR in support of AT Program.

(2) Coordinate and periodically update Standing CCIR with NCIS. Ensure CCIR’s are sent to NCIS.

(3) Develop and periodically update terrorism related PIR in coordination with other primary staff officers. Upon approval by the commander, PIR are submitted to NCIS for collection.

(4) Coordinates with all staff sections to develop and periodically update FFIR in support of the AT mission.

(5) Assume operational lead with the RSO/ISO in development of terrorist threat information requirements for installation/region.

(6) Advise and assist the CIC/TWG and other intelligence production activities in the development and review of terrorist threat information requirements. Provide updates as needed.

c. The ISO/RSO tasks include the following:

(1) Where applicable due to NCIS other commitments, the ISO/RSO are the lead coordinating individuals for development and dissemination of law enforcement information. Consequently, unless specifically identified as foreign intelligence, all threat information will be handled as “Law Enforcement Sensitive” until further classified.
(2) Assist NCIS with developing and maintaining the information collection plan for installation/region.

(3) Assume law enforcement lead (with NCIS) in coordinating information requirements with state and local law enforcement agencies consistent with DoD and U.S. Government guidelines.

(4) Assist NCIS with development of additional PIR’s as required for clarity, simplicity, specific situations, or other operational requirements.

(5) Review, at least annually, the Threat Information Collection Plan for installation/region. Assist NCIS with updates as needed.

(6) Assume operational lead as installation point-of-contact for surveillance detection information fusion.

(7) Forward all intelligence requests of suspected terrorist threats, or acts of terrorism involving DoD personnel or assets through NCIS, consistent with DoD and U.S. Government guidelines.

(8) Forward all law enforcement information requests of suspected terrorist threats, or acts of terrorism involving DoD personnel or assets through NCIS to local FBI, state police, or local law enforcement agency as appropriate, consistent with DoD and U.S. Government guidelines.

(9) Forward timely requests for intelligence to NCIS when local information indicates intelligence gaps.

(10) Forward timely requests for law enforcement information to state or local law enforcement agencies as appropriate, consistent with DoD and U.S. Government guidelines.

(11) Provide input to the installation/regional TWG.

(12) Advise and assist the CIC/TWG and other information production activities in the development and review of surveillance detection requirements. Provide updates as needed.

(13) (FOUO) Facilitate the flow of information between NCIS, N3, and both national and local law enforcement agencies regarding criminal and terrorist threats. Provide updates as
needed. EXTREME caution and care must be taken to ensure complete compliance with Intelligence Oversight directives while providing support to the installation/region AT program.

(14) (FOUO) Coordinate requests for specialized surveillance detection assets by forwarding requests through the chain of command.

(15) (FOUO) Coordinate and establish partnerships with local authorities to develop intelligence and information sharing relationships to improve security for the installation/region and the military community at large.

(16) (FOUO) Serve as coordinator for surveillance detection information sharing between installation/region and local law enforcement agencies, consistent with approved memoranda or agreement and DoD policy.

(17) Review, at least annually, the surveillance detection plan for installation/region. Update as needed.

(18) Submit CI requests to NCIS.

(19) When received from NCIS, ensure information on terrorist related incidents, and other matters concerning the security of installation/region and its activities are forwarded up the Chain of Command.

(20) Take corrective action on security deficiencies and hazards reported by NCIS.

(21) Provide NCIS with necessary administrative personnel actions and logistics support as required or directed.

(22) Assume operational lead as installation/region point of contact for fusion of terrorist criminal threat information.

(23) Forward all intelligence requests of suspected terrorist threats, or acts of terrorism involving DoD personnel or assets through NCIS, consistent with DoD and U.S. Government guidelines.

(24) Advise and assist the CIC/TWG and other information production activities in the development and review of terrorist threat information requirements. Provide updates as needed.
(25) Advise and assist the CIC/TWG and other information fusion activities in the development and review of terrorist threat information fusion requirements. Facilitate the flow of information between NCIS, the N3 and local law enforcement agencies regarding criminal and terrorist threats. Provide updates as needed. EXTREME caution and care must be taken to ensure complete compliance with Intelligence Oversight directives while providing support to the installation AT program.


(27) Be prepared to support the N3 for establishing and maintaining an emergency operations center as an installation/region command post for managing AT operations and the fusion of terrorist threat information.

(28) Review, at least annually, the Threat Information Fusion Plan for installation/region. Update as needed.

d. The Operations Officer (N3) tasks include the following:

(1) Assist NCIS with development of additional PIR’s as required for clarity, simplicity, specific situations, or other operational requirements.

(2) Integrate threat information requirements with the installation/region AT personnel, to the extent allowed by law, policy, or regulation.

(3) Review, at least annually, the Threat Information Collection Plan for installation/region. Assist NCIS with updates as needed.

(4) Advise and assist the CIC/TWG and other intelligence production activities in the development and review of terrorist threat information requirements. Provide updates as needed.

(5) Review current FPCONs, threat levels, and surveillance detection requirements.

(6) Advise the installation/region commander, in conjunction with the ISO/RSO regarding implementation of FPCONs or additional physical security measures for both installation/region and deployed personnel.
(7) Provide input to the installation/region TWG.

(8) Advise and assist the CIC/TWG and other intelligence production activities in the development and review of surveillance detection requirements. Provide updates as needed.

(9) Review current FPCONs, threat levels, and terrorist threat information fusion requirements. Coordinate with NCIS and the CIC/TWG as required for implementation of these measures.

(10) Assist other intelligence production activities in the development and review of threat information fusion requirements. Provide updates as needed.

(11) Establish and maintain an emergency operations center as an installation/region command post for managing terrorist threat information.

e. CIC/ TWG tasks include the following:

(1) The CIC/TWG will meet at least quarterly, but are subject to attend on call of the chairperson. Typically, the CIC will convene to deal with specific issues arising from evolving crises, developing intelligence affecting the area.

(2) (FOUO) The CIC/TWG will coordinate the collection and dissemination of intelligence information vital to the security of CNIC personnel and facilities.

(3) (FOUO) The CIC/TWG also reviews the status of active Terrorism Attack Indicators and PIR/IR to determine their status as Red, Amber or Green.

(4) At a minimum the CIC/TWG will stand up at least twice annually for exercises. At a minimum once will be for an AT exercise. The second time may be for a table top exercise.

(5) Have knowledge about the area and have authority to make commitments.

(6) Complete a CNIC approved intelligence support to AT course such as those taught at United States Army Military Police School (USAMPS) or Federal Law Enforcement Training Center (FLETC).
(7) Gather, analyze, and disseminate terrorism threat information.

(8) Develop and maintain a threat collection plan.

(9) Forward threat intelligence and information to the AT TWG.

(10) Gather, analyze, and disseminate terrorism surveillance detection information and forward to the AT TWG through the COC.

(11) Be prepared to support NCIS and ISO/RSO with implementation and execution of this plan.

(12) Monitor local and global events that may impact the safety of assigned personnel. Primary sources of information include open source and classified reporting by law enforcement organizations and intelligence agencies.

(13) During an incident coordinate the intelligence, investigative and criminal information needs of the installation/region and On-Scene Commander.

(14) Assist hostage negotiation team investigation cell.

f. Subordinate and tenant commanders and security zone commander tasks include the following:

(1) Implement the information collection plan for installation/region as directed or tasked.

(2) Ensure subordinates are aware of threat information requirements, and how to report threat information through proper channels.

(3) Ensure threat information reported through the chain of command is promptly reported to ISO/RSO and NCIS, as required.

(4) Assist the CIC/TWG and other intelligence production activities in the development and review of terrorist threat information requirements. Provide updates as needed.

(5) Forward all information relating to suspected terrorist threats, or acts of terrorism involving DoD personnel or assets through the COC.
(6) Serve as, or delegate as appropriate, information point of contact regarding AT responsibility for assigned personnel and assets.

(7) Forward timely requests for information to intelligence collection and production activities through NCIS when local information indicates intelligence gaps.

(8) Provide representatives to the CIC/TWG as required.

(9) Advise assigned personnel to report suspicious activity on a continuing basis.

(10) All installation/regional agencies will cooperate to the maximum extent possible on development of terrorist threat information requirements and related information.

(11) Ensure personnel understand limitations and restrictions on CI activities conducted by DoD personnel.

(12) Incorporate CI training into unit activities where appropriate.

(13) Be prepared to support NCIS and ISO/RSO with implementation and execution of this instruction.

(14) Be prepared to assist the N3 for establishing and maintaining an emergency operations center as a base command post for managing terrorist threat information.

g. ATWG tasks include the following:

(1) Synchronize and implement installation/region physical security, FPCON, and RAM as directed by the COC.

(2) Provide recommendations to the CIC/TWG for improving surveillance detection processes.

(3) Be prepared to support NCIS, REGCOM, CO and ISO/RSO with implementation and execution of this instruction.

(4) Be prepared to assist the N3 for establishing and maintaining an emergency operations center as an installation/regional command post for managing terrorist threat information.
h. Installation or Region SJA shall provide advice on procedures that govern the permissible techniques, the permissible targets, and the appropriate official who may approve CI activities within the limitations of law and policy.

1006. **Coordinating Procedures**

a. To enhance the process of intelligence information and its dissemination, the necessity of how some official reports and requirements are facilitated and who is responsible are delineated as follows:

b. Friendly Forces Information Requirements (FFIR). Upon approval by the Commander, HN/local related FFIR are submitted to the NCIS for collection. N1 and other primary staff sections answer FFIR concerning Navy or other U.S. military forces.

c. Essential Elements of Friendly Information (EEFI) process may include the Security Officer/N3 coordinating with primary staff sections and operational forces to develop HN/local centric EEFI.

1007. (FOUO) **Intelligence Products.** Intelligence products are produced locally and may come from all levels of command; NCIS, other intelligence sources, such as local/HN LE, Fusion Cells, etc. All products except those produced locally require further analysis and answer the question of “What does this mean for me?” The following are minimal requirements of specific products, tools and plans.

a. (FOUO) Threat Assessments. In AT operations, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target an installation, facility or unit. A comprehensive threat analysis will review the factors of a terrorist group’s existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attacks and results in a threat assessment. The threat assessment will be completed at least annually or when there is a significant change in the threat. Additional factors for consideration include:

(1) Staging Areas

(2) Area of Operations
b. Unlike the conventional threat, the terrorist threat in most cases will be difficult to determine and identify. When attempting to determine and identify the terrorist threat, identify the threat in terms of the four categories terrorists, criminals, saboteurs, and foreign intelligence.

1008. **Threat Models**

a. CNIC regions and installations shall have a specific Threat Model that can be part of their threat assessment. These models shall include the familiar factors of Mission, Enemy, Terrain and Weather, Troops, Time Available and Civil Considerations (METT-TC).

   (1) Mission. From the adversary’s perspective, assume intent to identify, close with, and neutralize the war fighting capability of blue forces. With that intent, the model contemplates how the adversary would collect and update or
validate information, and in what manner would the adversary attack?

(2) Enemy. From the adversary’s perspective, blue forces are the “enemy.” The adversary will collect information as we would, to create a target information packet (or folder). This will include, for example, a thorough analysis of guard post procedures, foot patrol routes, surveillance cameras and systems employed and lengths of chains on guard dogs. Then the adversary will determine a variety of methods of attack.

(3) Terrain and Weather. Terrain is used to describe ground features, but also includes subterranean aspects and manmade features. Subterranean aspects include caves, mines, sewers, subway systems, and underground railroads. In the urban environment, in-depth analysis of manmade features is critical to successful terrain analysis. Knowing the location and status of key structures greatly assists in planning and execution the commands AT plan. Disseminate the results of terrain analysis to all installation staff elements and units for their planning considerations. Terrain and weather analysis are inseparable and like terrain, weather affects both the adversary and the blue forces. During weather analysis, evaluate the effects of each military aspect of weather. However, focus on the aspects that have the most bearing on the situation.

(4) When considering troops, do not just consider the major threat within your AO, consider the lesser threats and the possibility of threats outside the AO who may have an impact on AT operations. As part of the model, consider mercenaries, support from other terrorist groups, criminal elements that are aligned with the threat, and specialized consultants. These do not have to be shooters and operatives. Examples are cyber attackers (paid hacker) and counterfeitors. Likewise, one must consider the threat’s organizational structure and capabilities as part of the “troops” component.

(5) Time available. In the case of fixed facilities, the adversary can afford to select when, where, and in what strength to conduct the attack. Documents recovered from various adversarial sites suggest that collection against some targets preceded the actual attack by up to two years. One should therefore presume an adversary that is patient, deliberate, methodical, organized, trained, and disciplined in the conduct of such attacks.
(6) Civil considerations. A thorough analysis of the population OCONUS is critical to the execution of the AT plan. Consider the impact the local populace may have on the threat and friendly forces, as well as their location in the AO and AOI.

1009. **Analytical Methodologies and Tools Applied Against Terrorist Operations**

   a. Analytical methodologies produce intelligence that meets the commander’s requirements for planning or implementing appropriate operations and programs.

   b. Analytical tools assist in the processing of relevant information so the analyst may develop products that can enhance the probability of successful operations. Tools assist in deriving a logical and correct solution to complex situations. Tools themselves are not products of intelligence and not intended to be used to brief the commander. RSO/ISOs and ATOs will be familiar with the capabilities of these tools used.

1010. **Four Basic Tools**

   a. There are four basic tools used in analyzing relevant information.

   (1) Time event chart is a chronological record of individual or group activities and is designed to store and display large amounts of information in as little space as possible.

   (2) Association matrix is used to show that a relationship between individuals exists. It shows associations within a group or similar activity, and is based on the assumption that people involved in a collective activity know one another.

   (3) Activities matrix is used to determine connectivity between individuals and anything other than persons (interest/entity).

   (4) Link diagram is a depiction of the linkages between interests or entities, individuals, events, organizations.

1011. **Terrorist Threat Database.** Terrorist Threat Databases are a NCIS function. However, RSO/ISOs and ATOs will be familiar
with the type of information that should be in the database so they know what type of information is available.

1012. **Products and Plans**

a. The intelligence community produces numerous products that AT planners use to produce plans that are relevant to countering a current threat that the AT operational forces (NSF, NCIS, Emergency Management personnel, commanders, etc) are able to use as a training tool/guide. AT operational forces further use these products and plans to counter an attack. Should this fail, the AT operational forces use the products and plans to respond to an attack in an effective manner within their capabilities. Some of these products are part of the installation/region AT Plan and will be reviewed and updated at least annually. Other products are situational. While primarily NCIS responsibility, Security Officers and ATOs will be familiar with these products to ensure they know what to ask for and what they receive is complete. This will ensure a minimal level of quality control, and in certain situations produce the products themselves when necessary. These products/plans include but are not limited to:

1. Threat Assessments (For Special Events and AT Plans)
2. Threat Information Collection Plan (AT Plans)
3. Counter Surveillance Plan (AT Plans)
4. Counterintelligence Plan (AT Plans)
5. Threat Information Fusion Plan (AT Plans)
6. Briefings
7. Intelligence summary which is primarily situational but may be periodic
8. Intelligence report
9. Spot reports
10. Quarterly trends reports
11. After Action Reports (AARs)
12. Others such as alerts, updates, etc.
1013. **Information Dissemination/Briefing Requirements**

a. NSF members

(1) All members of the NSF will receive a threat briefing from a member of the TWG, preferably NCIS intelligence representative, at least quarterly. NSF members will receive critical updates at guard mount, when necessary, by the NSF COC. These briefs will focus on what NSF may encounter while on duty and provide situational awareness, not only what is occurring on their specific installation, but also areas that directly affect not only their installation but also their region.

(2) NSF members will further receive an annual threat brief which is all encompassing of information gathered from the previous year, with the necessary background information, from a member of the TWG.

b. ISO/ATO

(1) ISOs and installation ATOs will receive a threat briefing from a member of the TWG, preferably NCIS intelligence representative, at least quarterly or more frequently if a significant threat surface. These briefs will be all encompassing and provide situational awareness of not only what is occurring on their specific installation but also other areas that directly affect not only their installation but also their region.

(2) ISOs and installation ATOs will further receive an annual threat brief that is all encompassing of information gathered from the previous year, with the necessary background information.

(3) ISOs and installation ATOs will conduct liaison with local and host nation LE activities (at the local and in some cases state and national level including Fusion Cells) at least quarterly (preferably monthly) to promote cooperation, promulgate MOUs/MOAs, develop a working relationship and to solidify information flow of what is going on off base to on base.

(4) ISOs and installation ATOs will not only forward critical local developed intelligence/information to their region and NCIS but also to CNIC N3AT.
c. RSO/ATO

(1) RSOs and regional ATOs will receive a threat briefing from a member of the Regional TWG, preferably NCIS intelligence representative, at least quarterly. These briefs will be all encompassing and provide situational awareness of not only what is occurring in their specific region but also adjacent regions.

(2) RSOs and regional ATOs will further receive an annual threat brief, which may be the fourth quarterly brief, that is all encompassing of information gathered from the previous year with the necessary background information and include current trends.

(3) RSOs and regional ATOs will conduct liaison activities with local and host nation LE activities, including Fusion Cells, at least quarterly (preferably monthly) to promote cooperation, promulgate MOUs/MOAs, develop a working relationship and solidify information flow of what is going on off base to on base.

(4) RSOs and regional ATOs will not only forward critical local developed intelligence/information to the effected installation and NCIS but also to CNIC N3AT and the respective operational commander.

(5) Will periodically assess the effectiveness of intelligence support at the installation level and provide feedback and recommendations to CNIC N3AT and the local NCIS field office.

d. CNIC N3AT staff

(1) All members of the CNIC N3AT staff will receive a threat brief from a member of the CNIC TWG, preferably NCIS, at least quarterly. These briefs will be all encompassing and provide situational awareness of the ongoing threats throughout the command.

(2) The CNIC N3AT staff will further receive an annual threat briefing, which may be the fourth quarterly brief, that is all encompassing of information gathered from the previous year with the necessary background information and include current trends.

(3) Will periodically assess the effectiveness of
intelligence support at the regional level and provide feedback and recommendations to NCIS.

e. All CNIC military/civilian personnel

(1) All CNIC personnel will receive a threat brief, prior to going on leave or TAD, from the ATO, ISO, or preferably from a member of the TWG (NCIS). This brief will include current criminal, terrorist, health, etc. threats present in the location of leave or TAD and the risks of the modes of travel.

(2) All CNIC personnel will further receive a brief of the Combatant Commands PIR for the area the individual will be going on leave or TAD. During this brief it will be emphasized the individual is not to go out of their way to gather information but to note it and if legal, take pictures of it when they observe it during their travels.

(3) Upon return to the command from leave or TAD all CNIC personnel will be appropriately debriefed by the ISO, ATO and/or a member of the TWG. This debrief will include not only the area Combatant Commands PIR but also any foreign contacts the individual had while on leave or TAD.

(4) All CNIC personnel will receive an initial threat brief within thirty days of being assigned and annually thereafter. This brief will be all encompassing and will be at the classification level commensurate with the level held by the individual. It will be given by a member of the TWG. A system will also be outlined in the commands AT Plan to provide critical updates as needed.

Note: Figures 10-1 thru 10-5 depicted on the following pages are examples of (1) Concept, (2) Information Flow, (3) the Ideal Look, and (4) Participants, CONUS & (5) Participants, OCONUS for informational purposes only.
Figure 10-1. Concept

**Concept**

<table>
<thead>
<tr>
<th><strong>MTAC</strong></th>
<th><strong>STRAATEGIC</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REGIONS</strong></td>
<td><strong>OPERATIONAL</strong></td>
</tr>
<tr>
<td><strong>INSTALLATIONS</strong></td>
<td><strong>TACTICAL</strong></td>
</tr>
</tbody>
</table>

**MTAC:** Worldview "Big Picture" Participates in high level "Fusion" Venues

**REGIONS:** Regional View. May be Transnational or National in nature depending on Region. Participates in National and/or Regional "Fusion" Venues

**INSTALLATIONS:** Local View. May be State/Provincial, or County/City/Town in nature. Focus's on Suspicious Persons and potential targets that effect the Installations mission. Conducts Liaison with local authorities and Participates in any "Fusion" venues the locals have available.
Figure 10-2. Information Flow
Figure 10-3. Ideal Look
PARTICIPANTS - CONUS

Figure 10-4. Participants (CONUS)
PARTICIPANTS - OCONUS

Figure 10-5. Participants (OCONUS)
APPENDIX A
REFERENCES

(a) OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program, 28 Jan 09
(b) OPNAVINST 3300.53C, Navy Antiterrorism Program, 26 May 09
(c) OPNAVINST 3400.12, Required Operational Capability Levels for Navy Installations and Facilities, 29 Oct 08
(d) DoDI 2000.16, DoD Antiterrorism Standards, 02 Oct 06
(e) DoDD 2000.12, DoD Antiterrorism (AT) Program, 18 Aug 03 (certified current 13 Dec 07)
(f) CJCS Instruction 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force SROE/SRUF for U.S. Forces, 13 Jun 05
(g) SECNAV M-5214.1, DON Information Requirements (Reports) Manual, 01 Dec 05
(h) SECNAV M-5210.1, DON Records Management Manual, 16 Nov 07
(i) 50 U.S.C., Section 797, Jan 03
(j) Naval Ashore Vision 2035, 01 Apr 2008
(k) OPNAVINST. 3500.38B, Universal Naval Task List, 30 Jan 07
(l) CJCSI 2700.01C, International Military Agreements for Rationalization, Standardization and Interoperability between the United States, its Allies and Other Friendly Nations, 08 Feb 08
(m) NTTP 3-07.2.3, Law Enforcement and Physical Security for Navy Installations, 29 Jan 09
(n) NTTP 3-07.2.1, Antiterrorism, Sep 06
(o) OPNAVINST 3591.1F, Small Arms Training and Qualification, 12 Aug 09
(p) CNICINST 3440.17, Navy Installation Emergency Management Program, 22 Jul 05
(q) Commander United States Fleet Forces Command (CUSFFC) OPORD 3300-09, 16 Jun 09
(r) Lautenberg Domestic Violence Amendment to the Gun Control Act of 1968, Sep 96
(s) SECNAVINST 6320.24A, Mental Health Evaluations of Members of The Armed Forces, 16 Feb 99
(t) OPNAVINST 6110.1H, Physical Readiness Program, 15 AUG 05
(u) DoDI 1308.3, DoD Physical Fitness and Body Fat Programs Procedures, 05 Nov 02
(w) OPNAVINST F3300.56, Navy Antiterrorism (AT) Strategic Plan, 01 Nov 06
(x) Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control, 02 Dec 09
(y) CNICINST 1752.1, Policy for Sex Offender Tracking, Assignment, and Installation Access Restrictions, 7 Feb 2011
(z) SECNAV memo of 7 Oct 08, Policy for Sex Offender Tracking and Assignment and Access Restrictions within the Department of the Navy (NOTAL)
(aa) UFC 4-022-01, Security Engineering: Entry Control Facilities/Access Control Points, 25 May 05
(bb) OPNAVINST 5380.1A, Voluntary Services in the Department of the Navy, dtd 26 Feb 07
(cc) OPNAVINST 11200.5D, Motor Vehicle Traffic Supervision, 22 May 06
(dd) Directive-Type Memorandum (DTM) 08-003, Next Generation Common Access Card (CAC) Implementation Guidance, 01 Dec 08
(ee) 33 CFR 1.01-30, Captains of the Port, 27 Dec 94
(ff) OPNAVINST C8126.1C, Navy Nuclear Weapons Security
(gg) OPNAVINST 4780.6F, Policy for Administering Service Craft and Boats in the U.S Navy, 25 Jan 06
(hh) DoD Instruction 5200.8, Security of DoD Installation and Resources, 10 Dec 05
(ii) OPNAVINST F3100.6J, Special Incident Reporting (OPREP-3 PINNACLE, OPREP-3 NAVY BLUE, AND OPREP-3 NAVY UNIT SITREP) Procedures, 22 Dec 09
(jj) DoDI 5525.13, Limitation of Authority to Deputize DoD Uniformed Civilian Personnel by State and Local Government, 28 Sep 07
(kk) SECNAVINST 5430.107, Mission and Functions of the Naval Criminal Investigative Service, 28 Dec 05
(ll) OPNAVINST 5100.12H Change Transmittal 1, Navy Traffic Safety Program, 25 Jun 08
(mm) White House Executive Order, Federal Leadership on Reducing Text Messaging While Driving, 01 Oct 09
(nn) DoDI 1400.25, Volume 591, DoD Civilian Personnel Management System: Uniform Allowance Rates for DoD Civilian Employees, 12 Apr 09
(oo) Homeland Security Presidential Directive/HSPD-5, Management of Domestic Incidents, 28 Feb 03
(pp) CNIC Shore Response Training Plan (SRTP) Toolbox
(qq) DoDI 5210.90, Minimum Training, Certification, and Physical Fitness Standards for Civilian Police and Navy Security Guards in the Department of Defense, 09 Jul 07
(rr) OPNAVINST 1000.16K, Navy Total Force Manpower Policies Procedures, 22 Aug 07
(ss) JP 1-02 Department of Defense Dictionary of Military and Associated Terms, 12 Apr 01, amended 17 Oct 08
APPENDIX B
DEFINITIONS/ACRONYMS

Administrative Control (ADCON). The direction or exercise of authority over subordinate or other organizations with respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. ADCON is synonymous with administration and support responsibilities identified in Title 10, USC. This is the authority necessary to fulfill Military Department statutory responsibilities for administration and support. ADCON may be delegated to and exercised by CDRs of Service forces assigned to a CCDR at any echelon at or below the level of Service component command. ADCON is subject to the command authority of CCDRs. ADCON may be delegated to and exercised by CDRs of Service commands assigned within Service authorities. Service CDRs exercising ADCON will not usurp the authorities assigned by a CCDR having COCOM over CDRs of assigned Service forces. (JP-1)

Area of Responsibility (AOR). The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. In naval usage, a predefined area of enemy terrain for which supporting ships are responsible for covering by fire on known targets or targets of opportunity and by observation. (JP-1-02)

Assess. Accurately identify adversary capabilities that can be used against friendly personnel, physical assets, or information and precisely derive adversary courses of action planned or employed with the intent to destroy or disrupt operational readiness.

Calls For Service. The activities directing the unit to support the security mission, including such activities as responding to alarms, crimes in progress, security checks and gate inspections, relief, etc. Self-directed activities such as traffic enforcement, field interviews, and others are not calls for service but are often captured as patrol workload.

Combatant Command (COCOM). Nontransferable command authority established by Title 10, United States Code, Section 164, exercised only by commanders of unified or specified COCOM’s unless otherwise directed by the President or the Secretary of Defense. COCOM command authority cannot be delegated and is the
authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. COCOM command authority should be exercised through the commanders of subordinate organizations. Normally, this authority is exercised through subordinate joint force commanders and service and/or functional component commanders. COCOM command authority provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in COCOM command authority. (JP 1-02)

Commander. Any flag officer or other command authority or civilian supervisor in a comparable position.

Critical Infrastructure. Facilities, systems and functions that is highly sophisticated and complex. They include human assets and physical and cyber systems that work together in processes that are highly interdependent. They also consist of key nodes that, in turn, are essential to the operation of the critical infrastructures in which they function.

Critical Infrastructure Protection (CIP). (1) Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions may include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc. (DoDD 3020.40, 19 Aug 2005) (2) The identification, assessment, and security of physical and cyber systems and assets so vital to the Nation that their incapacitation or destruction would have a debilitating impact on national security, national economic security and/or national public health and safety.

Consequence Management (CM). Those measures taken to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of a chemical, biological, nuclear, and/or high-yield explosive situation. For domestic consequence management, the primary authority rests with the states to respond and the federal government to provide assistance as required. (JP 3-28)
**Defend.** Resist hostile actions directed against friendly personnel, physical assets, or information to preserve operational readiness.

**Detect.** To collect and obtain timely, unambiguous, and accurate data regarding adversary capabilities, actions planned, or employed against friendly resources (personnel, physical assets, or information). Focus is the adversary's capabilities as well as actions.

**Deterrence.** The range of DoD efforts and capabilities to discourage aggression or coercion by potential adversaries.

**Enrollment.** The process at which time a person requiring access is vetted for a credential other than a temporary pass that authorizes access to installations.

**Foundational Capabilities.** A set of capabilities under force protection, law enforcement, fire and emergency services, emergency management, and safety required providing the basic acceptable level of detection, assessment, warning, response, and recovery of mission-essential tasks at Navy installations worldwide. These capabilities are both materiel and non-materiel solutions that can be provided organically or by the community.

**Hostile Act.** An attack or other use of force against the United States or U.S. forces, which includes force used directly to preclude or impede the mission and/or duties of U.S. forces and the recovery of U.S. personnel and vital U.S. government property. In certain circumstances, the use of force against U.S. nationals, their property, U.S. commercial assets, and/or other designated non-U.S. forces, foreign nationals, and their property is also a hostile act. (JP 3-28)

**Hostile Intent (HI).** The threat of imminent use of force against the United States or U.S. forces, which includes the threat of imminent use of force that would preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital U.S. government property. In certain circumstances, hostile intent is the threat of imminent use of force against U.S. nationals, their property, U.S. commercial assets, and/or designated non-U.S. forces, foreign nationals, and their property.

**Information.** Facts, data, or instructions in any medium or form.
Initial Response. The first actions taken by patrolman at a scene of an incident is to secure the scene, prevent the incident from becoming worse, look for victims, and detain possible suspects. A high priority is to the victim and providing needed medical attention. (JP 3-07.2)

Intelligence. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.

Metric. A standard of measurement; a means of specifying values of a variable or position of a point.

Mission Profile Validation-Protection (MPV-P). An Excel-based model generates region and installation-level staffing templates that aggregate numerous considerations and factors, specifically assets and risk in the form of Required Operational Capabilities, Common Output Levels Standards, Force Protection Conditions, geographical location, workload, workforce mix, productivity factors, and specific security/force protection-related work factors and staffing standards. It is a flexible model that allows greater accuracy and granularity of installation staffing at all FPCON’s.

Operational Control (OPCON). Inherent in COCOM and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. (JP-1)
**Patrol Zones.** Patrol zones define a certain geographic area assigned for specific asset protection for which an individual patrolman is responsible during his/her watch.

**Patrol Response.** Responses are categorized as emergencies and non-emergencies as determined by the severity to threaten life and property, ability to aid individuals who are in danger of physical harm, and ability to identify and stop a potential for an incident becoming a serious problem by security personnel.

**Prevent/Deter.** Deter, dissuade, or restrict an adversary from conducting hostile actions against friendly personnel, physical assets, or information.

**Protection.** Protection consists of five groups of activities: hardening of positions, protecting personnel, assuming mission-oriented protective posture, using physical defense measures, and reacting to attack. In space usage, active and passive defensive measures to ensure that U.S. and friendly space systems perform as designed by seeking to overcome an adversary's attempts to negate them and to minimize damage if negation is attempted. (JP 3-11)

**Reaction Force.** A task-organized force of armed Security Personnel designed to quickly respond to threats and/or incidents on an installation or ship.

**Recover.** Recovery and reconstitution includes actions taken prior to, during, and following an attack by an enemy to minimize the effects of the attack and maximize the combat potential of the remaining forces and supporting activities.

**Registration.** The process at which time a person requesting access is vetted for a temporary pass that authorizes access to an installation.

**Region Commander (REGCOM).** The individual assigned as commander of a designated Navy geographic region. (SECNAVINST 5530.4D)

**Rental Car.** A passenger vehicle (automobile), rented from a commercial company for short periods of time (ranging from a few hours to a few weeks) for a fee.

**Response Organization.** Proficient, cohesive, task-organized, and networked teams using common procedures and relevant information capable of responding rapidly to plan and execute a broad range of military operations.
**Restrict.** To confine, restrain / deter that limits actions of an adversary.

**Required Operational Capabilities (ROC) level.** The classification from 1 to 5 of each installation is based on the criticality of assets assigned and functions performed and supported. The names and locations of these installations are classified.

**Security.** Measures taken by a military unit, activity, or installation to protect itself against all acts designed to or which may impair its effectiveness. A condition that results from the establishment and maintenance of protective measures that ensures a state of invulnerability from hostile acts or influence. (JP 3-04)

**Sex Offender.** Any individual convicted of a criminal offense who is required to register as a sex offender under the Sex Offender Registration and Notification Act of 2006 (SORNA) Title 42 U.S.C. §§ 169110 – 16929 [Department of Justice, Office of the Attorney General, The National Guidelines for Sex Offender Registration and Notification of 2 Jul 08 (Pages 38030 – 38070 of Volume 73, Number 128, Federal Register)]. The SORNA web address, at http://www.nsopw.gov/, will be utilized to verify if an individual is a registered sex offender.

**SORNA Check.** The investigative query of the SORNA database at enrollment or registration of an individual prior to granting installation access.

**Status of Forces Agreement (SOFA).** An agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or form part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials. (JP 3-16)

**Single Source Coordinator (SSC).** A government entity presently conducting business on an installation that maintains oversight responsibility for the local command’s or Region’s regulated taxicab, limousine or shuttle services as defined by this instruction.
**Tactical Control (TACON).** Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. (JP-1)

**Warning.** Responsively react to actionable intelligence regarding adversary plans and actions directed against friendly personnel, physical assets, or information by disseminating warnings or predictions in a timely, accurate, and unambiguous manner. Specifically, warning includes the acknowledgement and communication of dangers implicit in a wide spectrum of activities by potential adversaries ranging from routine defense measures to substantial increases in readiness and force preparedness and to acts of terrorism or political, economic, or military provocation; operating procedures, practices, or conditions which may result in injury or death if not carefully observed or followed. (JP 3-04)

**Vulnerability.** In antiterrorism, a situation or circumstance that, if left unchanged, may result in the loss of life or damage to mission-essential resources. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that may be exploited to gain unauthorized access to information or an information system. (JP 3-60)
# List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-76</td>
<td>Commercial Activities/Competitive Source Program</td>
</tr>
<tr>
<td>AA</td>
<td>Airfield Assessment</td>
</tr>
<tr>
<td>AA&amp;E</td>
<td>Arms, Ammunition, and Explosives</td>
</tr>
<tr>
<td>AAR</td>
<td>After-Action Report</td>
</tr>
<tr>
<td>ACR</td>
<td>Allowance Change Request</td>
</tr>
<tr>
<td>ADCON</td>
<td>Administrative Control</td>
</tr>
<tr>
<td>AIVA</td>
<td>Airfield Integration Vulnerability Assessment</td>
</tr>
<tr>
<td>AO</td>
<td>Area of Operations</td>
</tr>
<tr>
<td>AOR</td>
<td>Area of Responsibility</td>
</tr>
<tr>
<td>AS</td>
<td>Armed Sentry</td>
</tr>
<tr>
<td>ASF</td>
<td>Auxiliary Security Force</td>
</tr>
<tr>
<td>AT</td>
<td>Antiterrorism</td>
</tr>
<tr>
<td>ATEP</td>
<td>Antiterrorism Enterprise Portal</td>
</tr>
<tr>
<td>ATO</td>
<td>Antiterrorism Officer</td>
</tr>
<tr>
<td>ATWG</td>
<td>Antiterrorism Working Group</td>
</tr>
<tr>
<td>BOS</td>
<td>Base Operating Support</td>
</tr>
<tr>
<td>BPAO</td>
<td>Base Processing Authorizing Official</td>
</tr>
<tr>
<td>BSAT</td>
<td>Biological Select Agents and Toxins</td>
</tr>
<tr>
<td>BSO</td>
<td>Budget Submitting Office</td>
</tr>
<tr>
<td>BTL</td>
<td>Between the Lifelines</td>
</tr>
<tr>
<td>C2</td>
<td>Command and Control</td>
</tr>
<tr>
<td>C4ISR</td>
<td>Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance</td>
</tr>
<tr>
<td>CAC</td>
<td>Common Access Card</td>
</tr>
<tr>
<td>CAT</td>
<td>Crisis Action Team</td>
</tr>
<tr>
<td>CBRNE</td>
<td>Chemical, Biological, Radiological, Nuclear, and High-yield Explosives</td>
</tr>
<tr>
<td>CCI</td>
<td>Command Criminal Investigators</td>
</tr>
<tr>
<td>CCIR</td>
<td>Commander’s Critical Information Requirements</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-circuit television</td>
</tr>
<tr>
<td>CDC</td>
<td>Concept Development Conference</td>
</tr>
<tr>
<td>CENSECFOR</td>
<td>Center for Security Forces</td>
</tr>
<tr>
<td>CeTARS</td>
<td>Corporate enterprise Training Activity Resource System</td>
</tr>
<tr>
<td>CI</td>
<td>Counterintelligence</td>
</tr>
<tr>
<td>CIC</td>
<td>Crisis Intelligence Cell</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td>CLEOC</td>
<td>Consolidated Law Enforcement Operations Center</td>
</tr>
<tr>
<td>CM</td>
<td>Consequence Management</td>
</tr>
<tr>
<td>CNIC</td>
<td>Commander, Navy Installations Command</td>
</tr>
<tr>
<td>CNO</td>
<td>Chief of Naval Operations</td>
</tr>
<tr>
<td>CNOIIVA</td>
<td>Chief of Naval Operations Integrated Vulnerability Assessments</td>
</tr>
<tr>
<td>COC</td>
<td>Chain of Command</td>
</tr>
</tbody>
</table>
COCOM  Combatant Command
COI    Course of Instruction
COL    Common Output Level
COMNAVFACENGCOM  Commander, Naval Facilities Engineering Command
CONUS  Continental United States
COOP   Continuity of Operations
COPT   Captain of the Port
CPL    Capability Performance Level
CPX    Command Post Exercise
CSCS   Commander Surface Combat Systems
CTL    Criminal Threat Level
CVAMP  Core Vulnerabilities Assessment Management Program
CVIT   Commercial Vehicle Inspection Team
CVS    Contractor Verification System
DBT    Design Basis Threat
DCW    Data Collection Workbook
DDD    Drug Detection Dog
DHS    Department of Homeland Security
DIACAP Defense Information Assurance Certification and Accreditation Process
DoD    Department of Defense
DoN    Department of Navy
DOS    Department of State
DONCJIS Department of the Navy Criminal Justice Information System
DRRS-N Defense Readiness Reporting System-Navy
DSCA   Defense Support to Civil Authorities
DTRA   Defense Threat Reduction Agency
DUI    Driving Under the Influence
EA     Executive Agent
ECP    Entry Control Point
EDD    Explosive Detection Dog
EEFI   Essential Elements of Friendly Information
EM     Emergency Management
EOC    Emergency Operations Center
EPG    Electronic Procurement Generator
ERT    Emergency Response Team
ESAMS  Enterprise Safety Application Management System
ETJ    Electronic Training Jackets
EVOC   Emergency Vehicle Operator Course
FFIR   Friendly Forces Information Requirements
FLTMAPS Fleet Training and Management Planning System
FOUO   For Official Use Only
FP     Force Protection
FPC    Final Planning Conference
FPCON  Force Protection Condition
FPPD  Force Protection Program Director
FTO  Field Training Officer
FTX  Field Training Exercise
GCC  Geographic Combatant Commander
HEMI  Human Electro-Muscular Incapacitation
HHA  Higher Headquarters Assessment
HN  Host Nation
HQ  Headquarters
HSB  Harbor Security Boat
HSEEP  Homeland Security Exercise and Evaluation Program
IA  Information Assurance
IATP  Individual Antiterrorism Plan
IAW  In Accordance With
CO  Installation Commanding Officer
ICS  Incident Command System
ICP  Incident Command Post
IDS  Intrusion Detection System
IED  Improvised Explosive Device
IPAC  Installation Protection Assessment Cell
IPC  Initial Planning Conference
IR  Information Requirement
ISD  Installation Security Detachment
ISIC  Immediate Superior In Command
ISO  Installation Security Officer
ITO  Installation Training Officer
ITT  Installation Training Team
IVA  Integrated Vulnerability Assessment
JLLR  Joint Lessons Learned Repository
JSIVA  Joint Staff Integrated Vulnerability Assessment
KO  Contracting Officer
KTR  Contractor
LE  Law Enforcement
LVA  Local Vulnerability Assessment
MA  Master-at-Arms
MEO  Most Efficient Organization
METT-TC  Mission, Enemy, Terrain and Weather, Troops, Time Available and Civil Considerations
MEVA  Mission-Essential Vulnerable Assets
MMC  Merchant Mariners Credential
MMD  Merchant Mariner’s Documents
MOA  Memorandum of Agreement
MOU  Memorandum of Understanding
MPC  Mid-Planning Conference
MPV-P  Mission Profile Validate-Protection
MTAC  Multiple Threat Alert Center
MTF  Medical Treatment Facility
MTT  Mobile Training Team
MVIT Mobile Vehicle Inspection Team
MWD Military Working Dog
MWR Morale/Welfare/Recreation
NACLC National Agency Check with Local Agency and Credit Check
NAVFAC Naval Facilities Engineering Command
NAVSEA Naval Sea Systems Command
NC3VC Non-Common Access Card Credentialing for Vendors/Contractors
NCACS Navy Commercial Access Control System
NCC Naval Component Commanders
NCIC National Crime Information Center
NCIS Naval Criminal Investigative Service
NCP Navy Civilian Police
NECC Navy Expeditionary Combat Command
NGS Non-Guard Security
NHTSA National Highway Traffic Safety Administration
NIJ National Institute of Justice
NIMS National Incident Management System
NKO Navy Knowledge Online
NLETS National Law Enforcement Telecommunications System
NLW Nonlethal Weapon
NMCI Navy Marine Corps Internet
NMET Navy Mission Essential Task
NOSSA Naval Ordnance Safety and Security Activity
NOTAL Notice to All
NQC Navy Quick Credentials
NR Navy Reserve
NSF Navy Security Forces
NSFS Navy Security Forces Sentry
NSG Navy Security Guard
NSGTC Navy Security Guard Training Course
NSOXP Navy Security Operations Exercise Program
NTIMS Navy Training Information Management Systems
NWTS Navy Warfare Training System
O&R Observations and Recommendations
OC Oleoresin Capsicum
OCONUS Outside the continental United States
OIC Officer in Charge
OPCON Operational Control
OPLAN Operational Plan
OPN Other Procurement Navy
OPNAV Office of the Chief of Naval Operations
OPORD Operational Order
OPR Office of Primary Responsibility
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSEC</td>
<td>Operational Security</td>
</tr>
<tr>
<td>ORM</td>
<td>Operational Risk Management</td>
</tr>
<tr>
<td>PA</td>
<td>Port Assessment</td>
</tr>
<tr>
<td>PACOM</td>
<td>Pacific Command</td>
</tr>
<tr>
<td>PACS</td>
<td>Physical Access Control System</td>
</tr>
<tr>
<td>PAT</td>
<td>Physical Agility Test</td>
</tr>
<tr>
<td>PESTOF</td>
<td>Personnel, Equipment, Supplies, Training, Ordnance, and Facilities</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PIR</td>
<td>Priority Intelligence Requirements</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identification Verification</td>
</tr>
<tr>
<td>PIVA</td>
<td>Port Integrated Vulnerability Assessment</td>
</tr>
<tr>
<td>POC</td>
<td>Point of Contact</td>
</tr>
<tr>
<td>POM</td>
<td>Program Objective Memorandum</td>
</tr>
<tr>
<td>POV</td>
<td>Privately Owned Vehicle</td>
</tr>
<tr>
<td>PPR</td>
<td>Preplanned Response</td>
</tr>
<tr>
<td>PPV</td>
<td>Public-Private Venture</td>
</tr>
<tr>
<td>PS</td>
<td>Physical Security</td>
</tr>
<tr>
<td>PSB</td>
<td>Port Security Barriers</td>
</tr>
<tr>
<td>PSVA</td>
<td>Personal Security Vulnerability Assessment</td>
</tr>
<tr>
<td>PVTL</td>
<td>Political Violence Threat Level</td>
</tr>
<tr>
<td>PWF</td>
<td>Productive Workweek Factor</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Antiterrorism Measures</td>
</tr>
<tr>
<td>RAO</td>
<td>Regional Authorizing Official</td>
</tr>
<tr>
<td>REGCOM</td>
<td>Region Commander</td>
</tr>
<tr>
<td>RIC</td>
<td>Regional Investigative Coordinator</td>
</tr>
<tr>
<td>RM</td>
<td>Risk Management</td>
</tr>
<tr>
<td>ROC</td>
<td>Required Operational Capability</td>
</tr>
<tr>
<td>ROC</td>
<td>Regional Operations Center</td>
</tr>
<tr>
<td>ROE</td>
<td>Rule(s) of Engagement</td>
</tr>
<tr>
<td>ROMO</td>
<td>Range of Military Operations</td>
</tr>
<tr>
<td>RRP</td>
<td>Rules, Regulations, and Procedures</td>
</tr>
<tr>
<td>RSF</td>
<td>Regional Security Force</td>
</tr>
<tr>
<td>RSO</td>
<td>Regional Security Officer</td>
</tr>
<tr>
<td>RTA</td>
<td>Regional Training Academy</td>
</tr>
<tr>
<td>RTT</td>
<td>Regional Training Team</td>
</tr>
<tr>
<td>RUF</td>
<td>Rules for the Use of Force</td>
</tr>
<tr>
<td>SAMI</td>
<td>Small Arms Marksmanship Instructor</td>
</tr>
<tr>
<td>SD</td>
<td>Surveillance Detection</td>
</tr>
<tr>
<td>SG</td>
<td>Security Guard</td>
</tr>
<tr>
<td>SIMBBC</td>
<td>Shore Installation Management Basic Boat Coxswain Course</td>
</tr>
<tr>
<td>SIPRNET</td>
<td>Secret Internet Protocol Router Network</td>
</tr>
<tr>
<td>SIR</td>
<td>Specific Information Requirement</td>
</tr>
<tr>
<td>SIRP</td>
<td>Shore Issue Resolution Process</td>
</tr>
<tr>
<td>SLLP</td>
<td>Shore Lessons Learned Program</td>
</tr>
<tr>
<td>SME</td>
<td>Subject Matter Expert</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SMR</td>
<td>Statement of Manpower Requirements</td>
</tr>
<tr>
<td>SOFA</td>
<td>Status of Forces Agreement</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SORNA</td>
<td>Sex Offender Registration and Notification Act</td>
</tr>
<tr>
<td>SRFTM-B</td>
<td>Security Reaction Force Team Member Basic</td>
</tr>
<tr>
<td>SRP</td>
<td>Shore Response Plan</td>
</tr>
<tr>
<td>SRTP</td>
<td>Shore Response Training Plan</td>
</tr>
<tr>
<td>SSC</td>
<td>Single Source Coordinator</td>
</tr>
<tr>
<td>STAAT</td>
<td>Security Training, Assistance, and Assessment Team</td>
</tr>
<tr>
<td>STEP</td>
<td>Selective Traffic Enforcement Program</td>
</tr>
<tr>
<td>SWF</td>
<td>Strategic Weapons Facility</td>
</tr>
<tr>
<td>SWFLANT</td>
<td>Strategic Weapons Facility, Atlantic</td>
</tr>
<tr>
<td>SWFPAC</td>
<td>Strategic Weapons Facility, Pacific</td>
</tr>
<tr>
<td>SYSCOM</td>
<td>System Command</td>
</tr>
<tr>
<td>TACON</td>
<td>Tactical Control</td>
</tr>
<tr>
<td>TAD</td>
<td>Temporary Additional Duty</td>
</tr>
<tr>
<td>TCCD</td>
<td>Training Course Control Document</td>
</tr>
<tr>
<td>TCCM</td>
<td>Theater and/or Country Clearance Message</td>
</tr>
<tr>
<td>TMU</td>
<td>Threat Management Unit</td>
</tr>
<tr>
<td>TOA</td>
<td>Table of Allowances</td>
</tr>
<tr>
<td>Tr</td>
<td>Training Readiness</td>
</tr>
<tr>
<td>TRASUP</td>
<td>Training Supervisor</td>
</tr>
<tr>
<td>TT/N</td>
<td>Travel Tracker/Notifier</td>
</tr>
<tr>
<td>TTL</td>
<td>Terrorist Threat Level</td>
</tr>
<tr>
<td>TTP</td>
<td>Tactics, Techniques, and Procedures</td>
</tr>
<tr>
<td>TTX</td>
<td>Tabletop Exercise</td>
</tr>
<tr>
<td>TWG</td>
<td>Threat Working Group</td>
</tr>
<tr>
<td>TWMS</td>
<td>Total Workforce Management System</td>
</tr>
<tr>
<td>UCMJ</td>
<td>Uniform Code of Military Justice</td>
</tr>
<tr>
<td>UFC</td>
<td>Unified Facilities Code</td>
</tr>
<tr>
<td>USFF</td>
<td>U.S. Fleet Forces Command</td>
</tr>
<tr>
<td>USNORTHCOM</td>
<td>United States Northern Command</td>
</tr>
<tr>
<td>VA</td>
<td>Vulnerability Assessment</td>
</tr>
<tr>
<td>VCC</td>
<td>Visitor Control Center</td>
</tr>
<tr>
<td>WRA</td>
<td>Waterside Restricted Area</td>
</tr>
</tbody>
</table>
## APPENDIX C
### CRIME PREVENTION CHECKLIST EXAMPLES

#### Residential Crime Prevention Checklist

<table>
<thead>
<tr>
<th>Resident's Name</th>
<th>Residence Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Inspector's Name</td>
</tr>
<tr>
<td>Are all outside doors in the house of metal or solid wood construction?</td>
<td>Y</td>
</tr>
<tr>
<td>Are door frames strong enough and tight enough to prevent forcing or spreading?</td>
<td>Y</td>
</tr>
<tr>
<td>Are door hinges protected from removal from the outside?</td>
<td>Y</td>
</tr>
<tr>
<td>Are there windows in any door or within 40 inches of the locks?</td>
<td>Y</td>
</tr>
<tr>
<td>Are all door locks adequate and in good repair?</td>
<td>Y</td>
</tr>
<tr>
<td>Are door strikes and strike plates adequate and properly installed?</td>
<td>Y</td>
</tr>
<tr>
<td>Can the locking mechanism be reached through a mail slot, delivery port, or pet entrance at the door?</td>
<td>Y</td>
</tr>
<tr>
<td>Is there a screen or storm door with an adequate lock?</td>
<td>Y</td>
</tr>
<tr>
<td>Are all entrances lighted with at least a 40-watt light?</td>
<td>Y</td>
</tr>
<tr>
<td>Can front entrances be observed from the street or public area?</td>
<td>Y</td>
</tr>
<tr>
<td>Does the porch or landscaping offer concealment from view from the street or public area?</td>
<td>Y</td>
</tr>
<tr>
<td>If there is a sliding glass door, is the sliding panel secured from being lifted out of its track?</td>
<td>Y</td>
</tr>
<tr>
<td>Question</td>
<td>Y</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Is the “charley-bar” or a key-operated auxiliary lock used on sliding glass doors?</td>
<td></td>
</tr>
<tr>
<td>Are all entrances to the living quarters from a garage or basement of metal or solid wood construction?</td>
<td></td>
</tr>
<tr>
<td>Does the door from the garage to the living quarters have locks adequate for exterior entrances?</td>
<td></td>
</tr>
<tr>
<td>Does the door from the basement to the living quarters have an adequate lock operated from the living quarter's side?</td>
<td></td>
</tr>
<tr>
<td>Do all windows have adequate locks in operating condition?</td>
<td></td>
</tr>
<tr>
<td>Are windows capable of being locked or pinned in an open position?</td>
<td></td>
</tr>
<tr>
<td>Do windows have screens or storm windows that lock from the inside?</td>
<td></td>
</tr>
<tr>
<td>Do any windows open into areas that may be hazardous or offer special risk to burglary?</td>
<td></td>
</tr>
<tr>
<td>Do windows that open into hazardous areas have security screens or grills?</td>
<td></td>
</tr>
<tr>
<td>Are exterior areas of windows free from concealing structure or landscaping?</td>
<td></td>
</tr>
<tr>
<td>Is the exterior adequately lighted at all window areas?</td>
<td></td>
</tr>
<tr>
<td>Are trees and shrubbery kept trimmed back from ground floor as well as upper floor windows?</td>
<td></td>
</tr>
<tr>
<td>Are ladders kept outside the house where they are accessible?</td>
<td></td>
</tr>
<tr>
<td>If there is a door from the outside to the basement, is it adequately secure for an exterior door?</td>
<td></td>
</tr>
<tr>
<td>Is the outside basement entrance lighted by an exterior light of at least 40 watts?</td>
<td></td>
</tr>
<tr>
<td>Is the outside basement door concealed from the street or neighbors?</td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Y</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Are all basement windows adequately secured against entrance?</td>
<td></td>
</tr>
<tr>
<td>Is the automobile entrance door to the garage equipped with an adequate locking device?</td>
<td></td>
</tr>
<tr>
<td>Is the garage door kept closed and locked at all times?</td>
<td></td>
</tr>
<tr>
<td>Are the garage windows secured adequately for ground floor windows?</td>
<td></td>
</tr>
<tr>
<td>Is the outside utility entrance to the garage as secure as required for any ground floor entrance?</td>
<td></td>
</tr>
<tr>
<td>Are tools and ladders kept in the garage or locked shed?</td>
<td></td>
</tr>
<tr>
<td>Are all garage doors lighted on the outside by at least a 40-watt light?</td>
<td></td>
</tr>
<tr>
<td>Are valuable items scribed with state and driver's license number?</td>
<td></td>
</tr>
<tr>
<td>Is a list of valuable items with description, serial numbers, date purchased, etc. maintained and kept in a secure location?</td>
<td></td>
</tr>
<tr>
<td>Are house keys and car keys kept on separate rings?</td>
<td></td>
</tr>
<tr>
<td>Are there plans that don't require a house key to be hidden under the doormat or in a similar location?</td>
<td></td>
</tr>
<tr>
<td>When resident is away, are there plans to make the home look lived in?</td>
<td></td>
</tr>
<tr>
<td>Are mail and newspapers stopped while away?</td>
<td></td>
</tr>
<tr>
<td>Are there light timers to turn one or more lights on and off at logical times?</td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Y</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Is a neighbor notified when occupants are gone?</td>
<td></td>
</tr>
<tr>
<td>Is a key left with a friend to check the home every so often?</td>
<td></td>
</tr>
<tr>
<td>Are NSF, police, or sheriff notified that residents will be gone?</td>
<td></td>
</tr>
<tr>
<td>Are valuables stored in a secure place such as a safe deposit box in a</td>
<td></td>
</tr>
<tr>
<td>bank while resident is gone?</td>
<td></td>
</tr>
<tr>
<td>Signature of Inspector</td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>Facility/Unit/Department</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Date</td>
<td>Inspector's Name</td>
</tr>
<tr>
<td>Are new unit personnel briefed on crime prevention and personal security procedures?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Are crime prevention briefings incorporated into regularly scheduled training?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Are procedures or SOPs established to ensure the safety and security of personnel?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Are unannounced checks made of installation areas?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Is sexual assault prevention training conducted and is the training documented and kept on file?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Does the command place emphasis on the prevention of sexual assault and other related crimes?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Are corrective action plans initiated when deficiencies are reported or noted?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Has the commander prohibited or limited the consumption of alcohol in the barracks?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Does the unit have an established visitor policy that prohibits visitors after a designated hour and is this policy enforced?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Are incidents of sexual assault reported immediately to the provost marshal and Sexual Assault Victim Intervention?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Is sexual assault prevention discussed in safety briefings at high-risk periods (pre- and post-deployment and before holiday weekends)?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Are personnel aware of sexual assault risk factors and basic preventive techniques?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Does the unit have the most-current list of off-limit areas in the community posted?</td>
<td>Y  N  N/A</td>
</tr>
<tr>
<td>Does NSF regularly patrol inside BHQ buildings?</td>
<td>Y</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature of Inspector</td>
<td></td>
</tr>
</tbody>
</table>
## Building Security Checklist

<table>
<thead>
<tr>
<th>Building Name/Number</th>
<th>Building location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Name of Inspector</td>
</tr>
<tr>
<td>Is area around building restricted?</td>
<td>Y</td>
</tr>
<tr>
<td>Is area fenced?</td>
<td>Y</td>
</tr>
<tr>
<td>Does fence have a personnel gate?</td>
<td>Y</td>
</tr>
<tr>
<td>Does fence have a vehicle gate?</td>
<td>Y</td>
</tr>
<tr>
<td>Are gates manned 24 hours or controlled by an electronic entry control system?</td>
<td>Y</td>
</tr>
<tr>
<td>Are fences and gates alarmed?</td>
<td>Y</td>
</tr>
<tr>
<td>Are fences and gates covered by CCTV?</td>
<td>Y</td>
</tr>
<tr>
<td>Are CCTV systems monitored 24 hours?</td>
<td>Y</td>
</tr>
<tr>
<td>Are gates capable of being locked?</td>
<td>Y</td>
</tr>
<tr>
<td>Is area marked with Restricted Area signage?</td>
<td>Y</td>
</tr>
<tr>
<td>Is area adjacent to fences clear of scrubs, trees, and other obstacles?</td>
<td>Y</td>
</tr>
<tr>
<td>Can vehicles drive next to fence and be used as a ladder?</td>
<td>Y</td>
</tr>
<tr>
<td>Is perimeter lighted?</td>
<td>Y</td>
</tr>
<tr>
<td>Question</td>
<td>Y</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Is outside of building perimeter lighted?</td>
<td>Y</td>
</tr>
<tr>
<td>Are lighting systems inspected on a regular basis?</td>
<td>Y</td>
</tr>
<tr>
<td>Are lighting systems adequate for CCTV systems?</td>
<td>Y</td>
</tr>
<tr>
<td>Are building entry control points manned?</td>
<td>Y</td>
</tr>
<tr>
<td>Are entrances monitored by CCTV?</td>
<td>Y</td>
</tr>
<tr>
<td>Are CCTV systems monitored 24 hours?</td>
<td>Y</td>
</tr>
<tr>
<td>Are entrance doors alarmed?</td>
<td>Y</td>
</tr>
<tr>
<td>Are all alarms monitored by installation dispatch center or NSF?</td>
<td>Y</td>
</tr>
<tr>
<td>Are alarm systems regularly tested?</td>
<td>Y</td>
</tr>
<tr>
<td>Is there backup power for alarm system?</td>
<td>Y</td>
</tr>
<tr>
<td>Are entrance doors keyed with dead-bolt locks?</td>
<td>Y</td>
</tr>
<tr>
<td>Are internal doors secured by dead-bolt locks?</td>
<td>Y</td>
</tr>
<tr>
<td>Are emergency exit doors alarmed?</td>
<td>Y</td>
</tr>
<tr>
<td>Question</td>
<td>Y</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Are keys controlled by a manager?</td>
<td></td>
</tr>
<tr>
<td>Are internal doors alarmed?</td>
<td></td>
</tr>
<tr>
<td>Are security systems in place?</td>
<td></td>
</tr>
<tr>
<td>Are employees instructed on operation of security systems and alarms?</td>
<td></td>
</tr>
<tr>
<td>Are external windows alarmed?</td>
<td></td>
</tr>
<tr>
<td>Do alarms deactivate if window or door is closed?</td>
<td></td>
</tr>
<tr>
<td>Is there a pass and ID system in place?</td>
<td></td>
</tr>
<tr>
<td>Do employees always wear visible ID badges?</td>
<td></td>
</tr>
<tr>
<td>Are visitors required to wear visible visitor ID badges?</td>
<td></td>
</tr>
<tr>
<td>Is a visitor log maintained?</td>
<td></td>
</tr>
<tr>
<td>Are offices cleaned during regular working hours?</td>
<td></td>
</tr>
<tr>
<td>Are cleaning persons escorted when in classified, restricted, or other sensitive areas?</td>
<td></td>
</tr>
<tr>
<td>Is an expected delivery list maintained?</td>
<td></td>
</tr>
<tr>
<td>Does building have security guards?</td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Y</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Is building regularly patrolled by NSF?</td>
<td></td>
</tr>
<tr>
<td>Does building have a dedicated parking area?</td>
<td></td>
</tr>
<tr>
<td>Is dedicated parking area inside the fence line?</td>
<td></td>
</tr>
<tr>
<td>Is parking area lighted during darkness?</td>
<td></td>
</tr>
<tr>
<td>If building is not located on an installation, is there an MOU/MOA with local authorities relating to responding to incidents?</td>
<td></td>
</tr>
</tbody>
</table>

Signature
## Personal Property Identification Records

### Credit Cards

<table>
<thead>
<tr>
<th>Name on Card</th>
<th>Company</th>
<th>Card Number</th>
<th>Expiration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Household and Personal Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Brand Name</th>
<th>Model Number</th>
<th>Serial Number</th>
<th>Value ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Television</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Television</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DVD Player</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CD Player</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radio</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MP3 Player</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microwave Oven</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lap Top Computer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desk Top Computer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Printer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Watch</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Watch</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Camera</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camcorder</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boom Box</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video Game System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Power Tools, Lawn &amp; Garden Equipment</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawn Mower</td>
<td></td>
</tr>
<tr>
<td>Garden Tractor</td>
<td></td>
</tr>
<tr>
<td>Trimmer</td>
<td></td>
</tr>
<tr>
<td>Skill Saw</td>
<td></td>
</tr>
<tr>
<td>Drill</td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>Make</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# APPENDIX D

**SEX OFFENDER POLICY ACKNOWLEDGEMENT & DISCLOSURE FORM**  
*(FH/BH/PPV)*

## SEX OFFENDER POLICY ACKNOWLEDGEMENT & DISCLOSURE

### PRIVACY ACT STATEMENT


**Principal Purposes:** To determine an individual's eligibility for Navy housing, including privatized housing.

**Routine Uses:** Used by region and installation housing office personnel to determine eligibility for Navy housing and by private partners who operate privatized Navy housing for management and operational purposes.

**Disclosure:** Voluntary; however, failure to provide the requested information may impact eligibility for Navy housing, including privatized housing.

### POLICY STATEMENT

In accordance with OPNAVINST 1752.3, to the maximum extent permitted by law or otherwise waived by Commander, Navy Installations Command or the Chief of Naval Personnel (CNP), sex offenders are to be identified and prohibited from accessing Navy facilities and occupying Navy-owned, leased, or PPV housing.

**Sex Offender Definition:** Any person convicted of a criminal offense requiring registration per the National Guidelines for Sex Offender Registration and Notification Act (SORNA) (42 U.S.C. § 16911-16912).

### NOTICE OF REQUIREMENT TO DISCLOSE

1. Military sponsors requesting assignment to Navy owned, leased or privatized housing are required to sign this acknowledgment and disclosure form.

2. Occupancy of Navy owned, leased or privatized housing will not be approved for otherwise eligible applicants if the applicant, any authorized dependents, or children residing in the home is a sex offender.

3. Anyone discovered to be a sex offender in the application process shall be denied access to Navy owned, leased or privatized housing.

4. Anyone found to be a sex offender after taking occupancy may lose the privilege of residing in Navy owned, leased or privatized housing, may be barred from the installation, and/or may be evicted. If eviction occurs, you may be responsible for all relocation expenses.

5. The Installation or Region Housing Program Director will immediately forward information regarding identified sex offenders to the Installation NCO and support SJA/OSC offices, to include a copy of the applicant's DD 2146 and this form. All information will be forwarded to CNIC within two working days.

6. Anyone found to have falsely certified the Acknowledgment shall be referred for personnel or eviction, as appropriate, and may be responsible for relocation expenses.

7. Denial of an application for assignment to Navy owned, leased or privatized housing under the applicable policy, may be appealed to the Region Commander via the military sponsor's chain of command.

### CERTIFICATION

I have read and understand the above policy. By my signature below, I certify that under a penalty of administrative action and/or prosecution for making a false official statement in violation of 18 U.S.C. § 1001 and for the Uniform Code of Military Justice, Article 107, that neither I nor any person living in my household is a registered convicted sex offender. I understand that if I am required to notify the Navy's Housing Office and the Installation Security Office immediately if circumstances change so that this certification is no longer true.

**Signature: John P. Sailor**  
**Date: 4 Feb 11**  
**Print Name: John P. Sailor**  
**Command: USS NeverSail**
<table>
<thead>
<tr>
<th>Security Personnel Equipment</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Concealable Tactical Response Carrier (CTRC) (DATA =LIII BPV)</td>
<td>Expandable Baton Case</td>
</tr>
<tr>
<td>Ballistic Insert, NIJLevel IV</td>
<td>9mm Holster, Beretta</td>
</tr>
<tr>
<td>Body Armor, Improved Outer Tactical Vest (IOTV) (DATA=LIVBPV)</td>
<td>Holster (9MM) Concealed Weapon (For MWD/INV)</td>
</tr>
<tr>
<td>Ballistic Insert, Esapi</td>
<td>9MM Ammo Pouch</td>
</tr>
<tr>
<td>Enhanced Side Torso Ballistic Plate Esbi</td>
<td>M16 Ammo Pouch</td>
</tr>
<tr>
<td>Helmet, Lightweight (LWH)</td>
<td>Belt keepers</td>
</tr>
<tr>
<td>Molle Pistol Mag Pouch Double</td>
<td>Radio Case</td>
</tr>
<tr>
<td>Molle M4/M16 Mag Pouch (Holds 3)</td>
<td>Handcuff Case</td>
</tr>
<tr>
<td>Molle Initial Attack Mot. XTS-5000 Radio Pouch</td>
<td>Key Holder</td>
</tr>
<tr>
<td>Molle Handcuff Pouch</td>
<td>Latex Glove Carrier</td>
</tr>
<tr>
<td>Handcuff</td>
<td>Shotgun Ammo Holder</td>
</tr>
<tr>
<td>Baton, Expandable</td>
<td>Tactical Vest (LH/RH)</td>
</tr>
<tr>
<td>Pepper Spray</td>
<td>Search Gloves</td>
</tr>
<tr>
<td>Pepper Spray Case</td>
<td>Kit Bag, Flyers</td>
</tr>
<tr>
<td>Flashlight</td>
<td>Harness</td>
</tr>
<tr>
<td>Flashlight Holder</td>
<td>Camelback Drinking System</td>
</tr>
<tr>
<td>Whistle</td>
<td>Mask, CPR</td>
</tr>
<tr>
<td>Duty Belt</td>
<td>Goggles (Sand, Wind, Dust)</td>
</tr>
</tbody>
</table>
### Training Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redman Training Xp Suit Instructor Set (SM/Med) - Head L</td>
<td>Remington 870 Training Gun</td>
</tr>
<tr>
<td>Redman Training Xp Suit Instructor Set (LG/XL) - Head L</td>
<td>Training Baton-21&quot;</td>
</tr>
<tr>
<td>Redman Student Suit (SM/Med) - Head M</td>
<td>Training Beretta, 9mm</td>
</tr>
<tr>
<td>Redman Student Suit (LG/XL) - Head M</td>
<td>Training Strike Bag</td>
</tr>
<tr>
<td>Training Knife</td>
<td></td>
</tr>
</tbody>
</table>

### Riot Control and Emergency Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disposable Cuffs</td>
<td>Riot Control Shields</td>
</tr>
<tr>
<td>Disposable Cuffs Cutter</td>
<td>Entry Two Shield Hs, 24 X 48</td>
</tr>
<tr>
<td>Leg Irons</td>
<td>Riot Protection Face Shield</td>
</tr>
<tr>
<td>Restraint Belts</td>
<td>Riot Baton 36 Inch</td>
</tr>
</tbody>
</table>

### Surveillance Detection Team Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Night Vision Monocular (AN/PVS 14)</td>
<td>Spotlight SD</td>
</tr>
<tr>
<td>Digital Camera</td>
<td>Binocular (7 X 50)</td>
</tr>
</tbody>
</table>

### Emergency Vehicle Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spotlight EV</td>
<td>Spike Strip</td>
</tr>
<tr>
<td>Stop Sign, Handheld</td>
<td>Traffic Vest</td>
</tr>
<tr>
<td>Flashlight Traffic Wand</td>
<td>Accident Template</td>
</tr>
<tr>
<td>Bolt Cutter, 24 Inch</td>
<td>Highway Warning Signals</td>
</tr>
<tr>
<td>First Aid Kit</td>
<td>Highway Warning Signals Hook On</td>
</tr>
<tr>
<td>Fire Extinguisher</td>
<td>Police Radar</td>
</tr>
<tr>
<td>Megaphone</td>
<td>Police Car Video Camera System</td>
</tr>
<tr>
<td>Blanket</td>
<td>Shotgun Mount</td>
</tr>
</tbody>
</table>

---

E-2 Enclosure (1)
### ECP Screening Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handheld Metal Detector</td>
<td>Low-Cost Vehicle Search Kit</td>
</tr>
<tr>
<td>Handheld Explosive Vapor Detector</td>
<td>Lighting Pack</td>
</tr>
<tr>
<td>Desktop Trace/Vapor Detector</td>
<td>Snakeeye Video Camera Pack</td>
</tr>
<tr>
<td>Walk-through Metal Detector</td>
<td>Snakeeye Support Pack</td>
</tr>
<tr>
<td>Portable Tent</td>
<td>Lumenyte Security Illuminated Mat System</td>
</tr>
<tr>
<td>Fiber Optics Pack</td>
<td>Inspection Mirror Set</td>
</tr>
<tr>
<td>8MM Fiberscope</td>
<td>Information Pack</td>
</tr>
<tr>
<td>4MM Nonconductive Semiflexible Fiberscope</td>
<td>Explosive Trace Detector</td>
</tr>
<tr>
<td>Inspection Mirror</td>
<td>Mirror, Inspection, Wheel MTD</td>
</tr>
</tbody>
</table>

### Mobile Vehicle Inspection Team Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expeditionary Vehicle Search Kit</td>
<td>Mirror, Inspection, Wheel MTD</td>
</tr>
<tr>
<td>Inspection Mirror</td>
<td></td>
</tr>
</tbody>
</table>

### Crime Scene/Investigation Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence Tags</td>
<td>Photo Identifier Cards</td>
</tr>
<tr>
<td>Evidence Bags</td>
<td>Trace Metal Detector Kit</td>
</tr>
<tr>
<td>Measuring Tape</td>
<td>Magnifiers</td>
</tr>
<tr>
<td>Evidence Tape</td>
<td>Petri Dishes</td>
</tr>
<tr>
<td>Evidence Letters A-Z</td>
<td>Eye Dropper</td>
</tr>
<tr>
<td>Evidence Numbers 1-15</td>
<td>Compass</td>
</tr>
<tr>
<td>Latent Print Kit</td>
<td>Respirator</td>
</tr>
<tr>
<td>Magnetic Print Kit</td>
<td>Safety Glasses</td>
</tr>
<tr>
<td>Police Barricade/ Crime Scene Tape</td>
<td>Tarpaulin</td>
</tr>
<tr>
<td>Casting Material</td>
<td>Water Bucket</td>
</tr>
<tr>
<td>Swabs</td>
<td>Dust Pan</td>
</tr>
<tr>
<td>Tweezers</td>
<td>First Aid Kit CSI</td>
</tr>
<tr>
<td>Hemostats</td>
<td>Tool Kit, Survival, Offroad</td>
</tr>
<tr>
<td>Scalpel Disposable</td>
<td>Broom</td>
</tr>
<tr>
<td>Scribes</td>
<td>Rake</td>
</tr>
<tr>
<td>Markers</td>
<td>Theft Detection Kit</td>
</tr>
<tr>
<td>Evidence Jar</td>
<td>Video Camera</td>
</tr>
<tr>
<td>Arson Evidence Cans</td>
<td>Video Camera Charger DC</td>
</tr>
<tr>
<td>Metal Detector</td>
<td>Video Camera Infrared Nightshot</td>
</tr>
<tr>
<td>Vacuums (Wet/Dry)</td>
<td>Hand-Held Tape Recorder</td>
</tr>
<tr>
<td>Scale Rulers and Templates</td>
<td>Basic Crime Scene Sketch Kits SK-B</td>
</tr>
<tr>
<td>Item Description</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Combination Comb</td>
<td>Nylon Harness With Quick Release Buckles</td>
</tr>
<tr>
<td>Dog Comb</td>
<td>Nylon Harness With 300 Lbs Test Tracking Line</td>
</tr>
<tr>
<td>Slicker Brush</td>
<td>Protective Coat Underlined Burlap Size 42-44</td>
</tr>
<tr>
<td>Grooming Brush</td>
<td>Protective Vest With Right Sleeve 30&quot; Long</td>
</tr>
<tr>
<td>Ray Allen Grip-It™ Long Line - 15'</td>
<td>Jute Cuff Tan In Color</td>
</tr>
<tr>
<td>Standard Muzzle - Military Style</td>
<td>Leather Ball Pouch</td>
</tr>
<tr>
<td>First Aid Kit WPack</td>
<td>33&quot; Long Tan In Color</td>
</tr>
<tr>
<td>Advanced Sleeve - Complete - Ambidextrous</td>
<td>23&quot; Long Tan In Color</td>
</tr>
<tr>
<td>Intermediate Sleeve - 23C - Ambidextrous</td>
<td>Leather Outside, Wool Interlining</td>
</tr>
<tr>
<td>Jute Trial Sleeve</td>
<td>Nylon Interlining Jute Outside Tan Outside</td>
</tr>
<tr>
<td>K-9 Resting Pad, Molded Polyethylene Pallet</td>
<td>24&quot; Long Juste Outside Tan In Color</td>
</tr>
<tr>
<td>Vari-Kennel By Doskocil - 500</td>
<td>Nylon Inside And Outside Brown And Tan In Color</td>
</tr>
<tr>
<td>Plastic Kennel X-Large 40&quot;X27&quot;X30&quot;</td>
<td>28&quot; Long Leather Outer Sleeve</td>
</tr>
<tr>
<td>Plastic Kennel Giant Size 48&quot;X32&quot;X35&quot;</td>
<td>Leather Forearm Gauntlet</td>
</tr>
<tr>
<td>Level II Ballistic Vest Patrol-Swat Series</td>
<td>Advanced Sleeve - Replacement Lower</td>
</tr>
<tr>
<td>Ray Allen K-9 Cool Vest - Large</td>
<td>Dbl Layer Jute Cuff W/Handle</td>
</tr>
<tr>
<td>Ray Allen K-9 Cool Vest - XL</td>
<td>Latigo Leather Laced Gauntlet</td>
</tr>
<tr>
<td>K-9 Cool Vest Unipaks - Med</td>
<td>Ray Allen Hand Protector - Left</td>
</tr>
<tr>
<td>K-9 Cool Vest Unipaks - Large</td>
<td>Ray Allen Hand Protector - Right</td>
</tr>
<tr>
<td>K-9 Cool Vest Unipaks - XL</td>
<td>Solid Rubber Ball - 2 1/2&quot;</td>
</tr>
<tr>
<td>Dog Cooling Vest Model #CZK9 Small</td>
<td>Solid Rubber Ball - 3&quot;</td>
</tr>
<tr>
<td>Dog Cooling Vest Model #CZK9 X-Large</td>
<td>Dog Ball - 6&quot;</td>
</tr>
<tr>
<td>Chillydog K-9 Cool Vest Model RCCD15XX-A</td>
<td>Medium Kong (2 1/4&quot; X 3 1/2&quot;)</td>
</tr>
<tr>
<td>Wool Blend Utility Blanket</td>
<td>Large Kong (2 3/4&quot; X 4&quot;)</td>
</tr>
<tr>
<td>Shedding Blade</td>
<td>King Kong (4&quot; X 6&quot;)</td>
</tr>
<tr>
<td>Large Animal Nail Clipper</td>
<td>Rake &amp; Shovel Poop Scoop</td>
</tr>
<tr>
<td>Stainless Steel Toenail Clipper</td>
<td>Metro Air Force Kennel Fan</td>
</tr>
<tr>
<td>Muttluks Dog Boot Medium Set Of 4</td>
<td>Navy Scent Kit For Training Explosive Detector Dogs</td>
</tr>
<tr>
<td>Muttluks Dog Boot Large Set Of 4</td>
<td>Navy Scent Kit For Training Explosive Detector Dogs</td>
</tr>
<tr>
<td>Harbor Patrol Boat Equipment</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Search Light</td>
<td>Life Vests</td>
</tr>
<tr>
<td>Flashlight HBP</td>
<td>Small Watercraft Inspection Guide</td>
</tr>
<tr>
<td>Binocular HP</td>
<td>Hydrophone</td>
</tr>
<tr>
<td>Night Vision Goggles (AN/PVS 15B)</td>
<td>Standard Anti-Exposure Coverall</td>
</tr>
<tr>
<td>Night Vision Monocular (AN/PVS 14)</td>
<td>Megaphone</td>
</tr>
<tr>
<td>Digital Camera HBP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Miscellaneous Security Equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alcohol Breath Analyzer</td>
</tr>
<tr>
<td>Narcotics Field Test Kits</td>
</tr>
<tr>
<td>Portable Surveillance System</td>
</tr>
<tr>
<td>Sandbangs w/ Tie Strings</td>
</tr>
<tr>
<td>Fingerpint Systems</td>
</tr>
</tbody>
</table>
## APPENDIX F
### CYCLE OF TRAINING

<table>
<thead>
<tr>
<th>January</th>
<th>Required Training for NSF:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use of Force/Deadly Force (Quarterly)</td>
</tr>
<tr>
<td></td>
<td>Crowd Control</td>
</tr>
<tr>
<td></td>
<td>Non-Lethal Weapons (OC Spray)</td>
</tr>
<tr>
<td></td>
<td>Baton</td>
</tr>
<tr>
<td></td>
<td>Physical Control Techniques</td>
</tr>
<tr>
<td></td>
<td>Traffic Control Techniques</td>
</tr>
<tr>
<td></td>
<td>AT Level 1 Brief</td>
</tr>
<tr>
<td></td>
<td>Weapons Qualifications</td>
</tr>
<tr>
<td></td>
<td>Physical Fitness</td>
</tr>
</tbody>
</table>

**Guard Mount Training:**

- Building Checks
- Communication Security
- CPR / First Aid
- Crime Scene Preservation
- FPCONS
- Jurisdiction
- Operational Security
- Pre-Planned Response Training
- Handcuffing Techniques
- Personnel Searching Techniques
- Statement Taking and Field Interview Card Info
- Uniform Wear and Regulations
- Use of Force Ladder of Force
- Vehicle Stops / Searches
- Weapons Handling / Conditions Codes
- Safety and ORM
- Complete security documents and correspondence
- Conduct area searches
- Conduct baggage and package inspections and searches
- Conduct building searches
- Respond to domestic violence incidents
- Respond to HAZMAT incidents

**NSOXP Drills:**

- NSO-06-AT- Alarm Response
- NSO-03-ATEntry Control Penetration (ECP)
- NSO-09-AT Active Shooter
- NSO-01-AT Surveillance
<table>
<thead>
<tr>
<th>February</th>
<th><strong>Required Training for NSF:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CPR</td>
</tr>
<tr>
<td></td>
<td>First Aid / First Responder</td>
</tr>
<tr>
<td></td>
<td>Drugs of Abuse Identification</td>
</tr>
<tr>
<td></td>
<td>Illegal Drug Identification</td>
</tr>
<tr>
<td></td>
<td>Tactical Communication</td>
</tr>
<tr>
<td></td>
<td>UCMJ</td>
</tr>
<tr>
<td></td>
<td>AT Level 1 Brief</td>
</tr>
<tr>
<td></td>
<td><strong>Guard Mount Training:</strong></td>
</tr>
<tr>
<td></td>
<td>Building Checks</td>
</tr>
<tr>
<td></td>
<td>Communication Security</td>
</tr>
<tr>
<td></td>
<td>CPR / First Aid</td>
</tr>
<tr>
<td></td>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td></td>
<td>FPCONS</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>Operational Security</td>
</tr>
<tr>
<td></td>
<td>Pre-Planned Response Training</td>
</tr>
<tr>
<td></td>
<td>Handcuffing Techniques</td>
</tr>
<tr>
<td></td>
<td>Personnel Searching Techniques</td>
</tr>
<tr>
<td></td>
<td>Statement Taking and Field Interview Card Info</td>
</tr>
<tr>
<td></td>
<td>Uniform Wear and Regulations</td>
</tr>
<tr>
<td></td>
<td>Use of Force Ladder of Force</td>
</tr>
<tr>
<td></td>
<td>Vehicle Stops / Searches</td>
</tr>
<tr>
<td></td>
<td>Weapons Handling / Conditions Codes</td>
</tr>
<tr>
<td></td>
<td>Detain civilian and military personnel</td>
</tr>
<tr>
<td></td>
<td>Fingerprint civilian and military personnel</td>
</tr>
<tr>
<td></td>
<td>Identify security perimeters</td>
</tr>
<tr>
<td></td>
<td>Identify security threats</td>
</tr>
<tr>
<td></td>
<td>Perform unarmed self defense techniques</td>
</tr>
<tr>
<td></td>
<td>Respond to crimes against persons</td>
</tr>
<tr>
<td></td>
<td>Respond to property crimes</td>
</tr>
<tr>
<td></td>
<td>Review AA&amp;E programs and instructions</td>
</tr>
</tbody>
</table>

|          | **NSOXP Drills:** |
|          | NSO-05-AT Vehicle Borne Improvised Explosive Device (VBIED) |
|          | NSO-01-AT Surveillance |
|          | NSO-7-AT Suspicious Package |
|          | NSO-14-AT Stand Off Attack |
**March**

<table>
<thead>
<tr>
<th>Required Training for NSF:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apprehension and Arrest</td>
</tr>
<tr>
<td>Jurisdiction and Authority</td>
</tr>
<tr>
<td>Proper Watch Standing Procedures</td>
</tr>
<tr>
<td>Random Vehicle Inspection Search</td>
</tr>
<tr>
<td>Search and Seizure</td>
</tr>
<tr>
<td>Self –Incrimination / Admission</td>
</tr>
<tr>
<td>AT Level 1 Brief</td>
</tr>
</tbody>
</table>

**Guard Mount Training:**

<table>
<thead>
<tr>
<th>Building Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Security</td>
</tr>
<tr>
<td>CPR / First Aid</td>
</tr>
<tr>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td>FPCONS</td>
</tr>
<tr>
<td>Jurisdiction</td>
</tr>
<tr>
<td>Operational Security</td>
</tr>
<tr>
<td>Pre-Planned Response Training</td>
</tr>
<tr>
<td>Handcuffing Techniques</td>
</tr>
<tr>
<td>Personnel Searching Techniques</td>
</tr>
<tr>
<td>Statement Taking and Field Interview Card Info</td>
</tr>
<tr>
<td>Uniform Wear and Regulations</td>
</tr>
<tr>
<td>Use of Force Ladder of Force</td>
</tr>
<tr>
<td>Vehicle Stops / Searches</td>
</tr>
<tr>
<td>Weapons Handling / Conditions Codes</td>
</tr>
<tr>
<td>Perform non-verbal communications techniques</td>
</tr>
<tr>
<td>Review security policies, instructions and procedures</td>
</tr>
<tr>
<td>Detect DWI/DUI</td>
</tr>
<tr>
<td>Secure crime and accident scenes</td>
</tr>
<tr>
<td>Forms and reports/report writing</td>
</tr>
<tr>
<td>Changes in Standard Operating Procedures, Post Orders, etc.</td>
</tr>
<tr>
<td>Rules of Engagement</td>
</tr>
<tr>
<td>Search &amp; Seizure</td>
</tr>
<tr>
<td>Jurisdiction &amp; Authority</td>
</tr>
<tr>
<td>Conduct baggage and package inspections and searches</td>
</tr>
<tr>
<td>Conduct building searches</td>
</tr>
<tr>
<td>Respond to domestic violence incidents</td>
</tr>
</tbody>
</table>

**NSOXP Drills:**

<p>| NSO-04-AT Pedestrian Carried Improvised Explosive Device (PCIED) |
| NSO-13-AT Swimmer Attack |
| NSO-8-AT Bomb Threat (Written / Verbal) |</p>
<table>
<thead>
<tr>
<th>April</th>
<th>Required Training for NSF:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Deadly Force / Use of Force (Quarterly)</td>
</tr>
<tr>
<td></td>
<td>Antiterrorism Brief</td>
</tr>
<tr>
<td></td>
<td>Captains Mast / Court Martial</td>
</tr>
<tr>
<td></td>
<td>SOP Review</td>
</tr>
<tr>
<td></td>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td></td>
<td>Standard of Conduct</td>
</tr>
<tr>
<td></td>
<td><strong>Guard Mount Training:</strong></td>
</tr>
<tr>
<td></td>
<td>Building Checks</td>
</tr>
<tr>
<td></td>
<td>Communication Security</td>
</tr>
<tr>
<td></td>
<td>CPR / First Aid</td>
</tr>
<tr>
<td></td>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td></td>
<td>FPCONS</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>Operational Security</td>
</tr>
<tr>
<td></td>
<td>Pre-Planned Response Training</td>
</tr>
<tr>
<td></td>
<td>Handcuffing Techniques</td>
</tr>
<tr>
<td></td>
<td>Personnel Searching Techniques</td>
</tr>
<tr>
<td></td>
<td>Statement Taking and Field Interview Card Info</td>
</tr>
<tr>
<td></td>
<td>Uniform Wear and Regulations</td>
</tr>
<tr>
<td></td>
<td>Use of Force Ladder of Force</td>
</tr>
<tr>
<td></td>
<td>Vehicle Stops / Searches</td>
</tr>
<tr>
<td></td>
<td>Weapons Handling / Conditions Codes</td>
</tr>
<tr>
<td></td>
<td>Rules of evidence</td>
</tr>
<tr>
<td></td>
<td>Collect and/or seize evidence</td>
</tr>
<tr>
<td></td>
<td>Detain civilian and military personnel</td>
</tr>
<tr>
<td></td>
<td>Fingerprint civilian and military personnel</td>
</tr>
<tr>
<td></td>
<td>Identify security perimeters</td>
</tr>
<tr>
<td></td>
<td>Respond to crimes against persons</td>
</tr>
<tr>
<td></td>
<td>Respond to property crimes</td>
</tr>
<tr>
<td></td>
<td>Review AA&amp;E programs and instructions</td>
</tr>
<tr>
<td></td>
<td>Posse Comitatus Act/Military Authority</td>
</tr>
<tr>
<td></td>
<td>Issue Citation</td>
</tr>
<tr>
<td></td>
<td>Bomb Threats/Procedures</td>
</tr>
<tr>
<td></td>
<td><strong>NSOXP Drills:</strong></td>
</tr>
<tr>
<td></td>
<td>NSO-10-AT Small Boat Probe</td>
</tr>
<tr>
<td></td>
<td>NSO-02-AT Protest</td>
</tr>
<tr>
<td></td>
<td>NSO-11-AT Small Boat Attack</td>
</tr>
<tr>
<td></td>
<td>NSO-09-AT Active Shooter</td>
</tr>
<tr>
<td>May</td>
<td>Required Training for NSF:</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------</td>
</tr>
<tr>
<td></td>
<td>Mobile Patrol Procedures, Vehicle</td>
</tr>
<tr>
<td></td>
<td>Non-Lethal Weapons Training (OC)</td>
</tr>
<tr>
<td></td>
<td>Baton</td>
</tr>
<tr>
<td></td>
<td>Physical Control Techniques</td>
</tr>
<tr>
<td></td>
<td>Range Safety Rules</td>
</tr>
<tr>
<td></td>
<td>Weapons Safety and Handling</td>
</tr>
<tr>
<td></td>
<td><strong>Guard Mount Training:</strong></td>
</tr>
<tr>
<td></td>
<td>Building Checks</td>
</tr>
<tr>
<td></td>
<td>Communication Security</td>
</tr>
<tr>
<td></td>
<td>CPR / First Aid</td>
</tr>
<tr>
<td></td>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td></td>
<td>FPCONS</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>Operational Security</td>
</tr>
<tr>
<td></td>
<td>Pre-Planned Response Training</td>
</tr>
<tr>
<td></td>
<td>Handcuffing Techniques</td>
</tr>
<tr>
<td></td>
<td>Personnel Searching Techniques</td>
</tr>
<tr>
<td></td>
<td>Statement Taking and Field Interview Card Info</td>
</tr>
<tr>
<td></td>
<td>Uniform Wear and Regulations</td>
</tr>
<tr>
<td></td>
<td>Use of Force Ladder of Force</td>
</tr>
<tr>
<td></td>
<td>Vehicle Stops / Searches</td>
</tr>
<tr>
<td></td>
<td>Weapons Handling / Conditions Codes</td>
</tr>
<tr>
<td></td>
<td><strong>NSOXP Drills:</strong></td>
</tr>
<tr>
<td></td>
<td>NSO-12-AT Floating Object-Improvised Explosive Device (IED)</td>
</tr>
<tr>
<td></td>
<td>NSO-14-AT Stand Off Attack</td>
</tr>
<tr>
<td></td>
<td>NSO-15-AT Light Air Craft Attack</td>
</tr>
<tr>
<td></td>
<td>NSO-01-AT Surveillance</td>
</tr>
<tr>
<td>June</td>
<td><strong>Required Training for NSF:</strong></td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td></td>
<td>Crowd Control</td>
</tr>
<tr>
<td></td>
<td>Traffic Control Techniques</td>
</tr>
<tr>
<td></td>
<td>CPR</td>
</tr>
<tr>
<td></td>
<td>First Aid / First Responder</td>
</tr>
<tr>
<td></td>
<td>Drug of Abuse Identification</td>
</tr>
<tr>
<td></td>
<td>Illegal Drug Identification</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>Guard Mount Training:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Building Checks</td>
</tr>
<tr>
<td></td>
<td>Communication Security</td>
</tr>
<tr>
<td></td>
<td>CPR / First Aid</td>
</tr>
<tr>
<td></td>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td></td>
<td>FPCONS</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>Operational Security</td>
</tr>
<tr>
<td></td>
<td>Pre-Planned Response Training</td>
</tr>
<tr>
<td></td>
<td>Handcuffing Techniques</td>
</tr>
<tr>
<td></td>
<td>Personnel Searching Techniques</td>
</tr>
<tr>
<td></td>
<td>Statement Taking and Field Interview Card Info</td>
</tr>
<tr>
<td></td>
<td>Uniform Wear and Regulations</td>
</tr>
<tr>
<td></td>
<td>Use of Force Ladder of Force</td>
</tr>
<tr>
<td></td>
<td>Vehicle Stops / Searches</td>
</tr>
<tr>
<td></td>
<td>Weapons Handling / Conditions Codes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>NSOXP Drills:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NSO-17-AT Armed / Barricaded / Hostage Situation</td>
</tr>
<tr>
<td></td>
<td>NS0-06-AT- Alarm Response</td>
</tr>
<tr>
<td></td>
<td>NSO-03-AT Entry Control Penetration (ECP)</td>
</tr>
<tr>
<td></td>
<td>NSO-16-AT Chemical Biological Radiological Nuclear (CBRN) Assault</td>
</tr>
<tr>
<td>July</td>
<td><strong>Required Training for NSF:</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Apprehension / Arrest</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction and Authority</td>
</tr>
<tr>
<td></td>
<td>Proper Watch Standing Procedures</td>
</tr>
<tr>
<td></td>
<td>Random Vehicle Inspection</td>
</tr>
<tr>
<td></td>
<td>UCMJ</td>
</tr>
<tr>
<td></td>
<td>AT Level 1 Brief</td>
</tr>
<tr>
<td></td>
<td>Deadly Force / Use of Force (Quarterly)</td>
</tr>
<tr>
<td></td>
<td><strong>Guard Mount Training:</strong></td>
</tr>
<tr>
<td></td>
<td>Building Checks</td>
</tr>
<tr>
<td></td>
<td>Communication Security</td>
</tr>
<tr>
<td></td>
<td>CPR / First Aid</td>
</tr>
<tr>
<td></td>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td></td>
<td>FPCONS</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>Operational Security</td>
</tr>
<tr>
<td></td>
<td>Pre-Planned Response Training</td>
</tr>
<tr>
<td></td>
<td>Handcuffing Techniques</td>
</tr>
<tr>
<td></td>
<td>Personnel Searching Techniques</td>
</tr>
<tr>
<td></td>
<td>Statement Taking and Field Interview Card Info</td>
</tr>
<tr>
<td></td>
<td>Uniform Wear and Regulations</td>
</tr>
<tr>
<td></td>
<td>Use of Force Ladder of Force</td>
</tr>
<tr>
<td></td>
<td>Vehicle Stops / Searches</td>
</tr>
<tr>
<td></td>
<td>Weapons Handling / Conditions Codes</td>
</tr>
<tr>
<td></td>
<td>Secure evidence and property</td>
</tr>
<tr>
<td></td>
<td>Obtain permissive search authorization</td>
</tr>
<tr>
<td></td>
<td>Obtain verbal and written statements</td>
</tr>
<tr>
<td></td>
<td>Request assistance from outside agencies and activities</td>
</tr>
</tbody>
</table>

**NOSXP Drills:**

- NSO-09-AT Active Shooter
- NSO-05-AT Vehicle Borne Improvised Explosive Device (VBIED)
- NSO-01-AT Surveillance
- NSO-7-AT Suspicious Package
<table>
<thead>
<tr>
<th>August</th>
<th><strong>Required Training for NSF:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Search and Seizure</td>
</tr>
<tr>
<td></td>
<td>Self-Incrimination / Admissions</td>
</tr>
<tr>
<td></td>
<td>Crowd Control</td>
</tr>
<tr>
<td></td>
<td>Non-Lethal Weapons Training (OC Spray)</td>
</tr>
<tr>
<td></td>
<td>Baton</td>
</tr>
<tr>
<td></td>
<td>AT Level 1 Training</td>
</tr>
<tr>
<td></td>
<td><strong>Guard Mount Training:</strong></td>
</tr>
<tr>
<td></td>
<td>Building Checks</td>
</tr>
<tr>
<td></td>
<td>Communication Security</td>
</tr>
<tr>
<td></td>
<td>CPR / First Aid</td>
</tr>
<tr>
<td></td>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td></td>
<td>FPCONS</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>Operational Security</td>
</tr>
<tr>
<td></td>
<td>Pre-Planned Response Training</td>
</tr>
<tr>
<td></td>
<td>Handcuffing Techniques</td>
</tr>
<tr>
<td></td>
<td>Personnel Searching Techniques</td>
</tr>
<tr>
<td></td>
<td>Statement Taking and Field Interview Card Info</td>
</tr>
<tr>
<td></td>
<td>Uniform Wear and Regulations</td>
</tr>
<tr>
<td></td>
<td>Use of Force Ladder of Force</td>
</tr>
<tr>
<td></td>
<td>Vehicle Stops / Searches</td>
</tr>
<tr>
<td></td>
<td>Weapons Handling / Conditions Codes</td>
</tr>
<tr>
<td></td>
<td><strong>NSOXP Drills:</strong></td>
</tr>
<tr>
<td></td>
<td>NSO-04-AT Pedestrian Carried Improvised Explosive Device (PCIED)</td>
</tr>
<tr>
<td></td>
<td>NSO-13-AT Swimmer Attack</td>
</tr>
<tr>
<td></td>
<td>NSO-8-AT Bomb Threat (Written / Verbal)</td>
</tr>
<tr>
<td></td>
<td>NSO-10-AT Small Boat Probe</td>
</tr>
<tr>
<td>September</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td><strong>Required Training for NSF:</strong></td>
<td></td>
</tr>
<tr>
<td>Physical Control Techniques</td>
<td></td>
</tr>
<tr>
<td>Traffic Control Techniques</td>
<td></td>
</tr>
<tr>
<td>CPR</td>
<td></td>
</tr>
<tr>
<td>First Aid</td>
<td></td>
</tr>
<tr>
<td>Drug Abuse Identification</td>
<td></td>
</tr>
<tr>
<td><strong>Guard Mount Training:</strong></td>
<td></td>
</tr>
<tr>
<td>Building Checks</td>
<td></td>
</tr>
<tr>
<td>Communication Security</td>
<td></td>
</tr>
<tr>
<td>CPR / First Aid</td>
<td></td>
</tr>
<tr>
<td>Crime Scene Preservation</td>
<td></td>
</tr>
<tr>
<td>FPCONS</td>
<td></td>
</tr>
<tr>
<td>Jurisdiction</td>
<td></td>
</tr>
<tr>
<td>Operational Security</td>
<td></td>
</tr>
<tr>
<td>Pre-Planned Response Training</td>
<td></td>
</tr>
<tr>
<td>Handcuffing Techniques</td>
<td></td>
</tr>
<tr>
<td>Personnel Searching Techniques</td>
<td></td>
</tr>
<tr>
<td>Statement Taking and Field Interview Card Info</td>
<td></td>
</tr>
<tr>
<td>Uniform Wear and Regulations</td>
<td></td>
</tr>
<tr>
<td>Use of Force Ladder of Force</td>
<td></td>
</tr>
<tr>
<td>Vehicle Stops / Searches</td>
<td></td>
</tr>
<tr>
<td>Weapons Handling / Conditions Codes</td>
<td></td>
</tr>
<tr>
<td><strong>NSOXP Drills:</strong></td>
<td></td>
</tr>
<tr>
<td>NSO-12-AT Floating Object-Improvised Explosive Device (IED)</td>
<td></td>
</tr>
<tr>
<td>NSO-14-AT Stand Off Attack</td>
<td></td>
</tr>
<tr>
<td>NSO-15-AT Light Air Craft Attack</td>
<td></td>
</tr>
<tr>
<td>NSO-01-AT Surveillance</td>
<td></td>
</tr>
<tr>
<td>October</td>
<td>Required Training for NSF:</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td>Crowd Control</td>
</tr>
<tr>
<td></td>
<td>Non-Lethal Weapons Training (OC Spray)</td>
</tr>
<tr>
<td></td>
<td>Baton</td>
</tr>
<tr>
<td></td>
<td>Physical Control Techniques</td>
</tr>
<tr>
<td></td>
<td>Deadly Force / Use of Force</td>
</tr>
<tr>
<td></td>
<td>Guard Mount Training:</td>
</tr>
<tr>
<td></td>
<td>Building Checks</td>
</tr>
<tr>
<td></td>
<td>Communication Security</td>
</tr>
<tr>
<td></td>
<td>CPR / First Aid</td>
</tr>
<tr>
<td></td>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td></td>
<td>FPCONS</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>Operational Security</td>
</tr>
<tr>
<td></td>
<td>Pre-Planned Response Training</td>
</tr>
<tr>
<td></td>
<td>Handcuffing Techniques</td>
</tr>
<tr>
<td></td>
<td>Personnel Searching Techniques</td>
</tr>
<tr>
<td></td>
<td>Statement Taking and Field Interview Card Info</td>
</tr>
<tr>
<td></td>
<td>Uniform Wear and Regulations</td>
</tr>
<tr>
<td></td>
<td>Use of Force Ladder of Force</td>
</tr>
<tr>
<td></td>
<td>Vehicle Stops / Searches</td>
</tr>
<tr>
<td></td>
<td>Weapons Handling / Conditions Codes</td>
</tr>
<tr>
<td></td>
<td>NSOXP Drills:</td>
</tr>
<tr>
<td></td>
<td>NSO-09-AT Active Shooter</td>
</tr>
<tr>
<td></td>
<td>NSO-05-AT Vehicle Borne Improvised Explosive Device (VBIED)</td>
</tr>
<tr>
<td></td>
<td>NSO-01-AT Surveillance</td>
</tr>
<tr>
<td></td>
<td>NSO-7-AT Suspicious Package</td>
</tr>
<tr>
<td>November</td>
<td><strong>Required Training for NSF:</strong></td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>CPR</td>
<td>First Aid / First Responder</td>
</tr>
<tr>
<td>Illegal Drug Identification</td>
<td>Tactical Communication</td>
</tr>
<tr>
<td>UCMJ</td>
<td></td>
</tr>
</tbody>
</table>

**Guard Mount Training:**
- Building Checks
- Communication Security
- CPR / First Aid
- Crime Scene Preservation
- FPCONS
- Jurisdiction
- Operational Security
- Pre-Planned Response Training
- Handcuffing Techniques
- Personnel Searching Techniques
- Statement Taking and Field Interview Card Info
- Uniform Wear and Regulations
- Use of Force Ladder of Force
- Vehicle Stops / Searches
- Weapons Handling / Conditions Codes

**NSOXP Drills:**
- NSO-02-AT Protest
- NSO-11-AT Small Boat Attack
- NSO-04-AT Pedestrian Carried Improvised Explosive Device (PCIED)
- NSO-13-AT Swimmer Attack
<table>
<thead>
<tr>
<th>December</th>
<th>Required Training for NSF:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Apprehension and Arrest</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction and Authority</td>
</tr>
<tr>
<td></td>
<td>Proper Watch Standing Procedures</td>
</tr>
<tr>
<td></td>
<td>Random Vehicle Inspection</td>
</tr>
<tr>
<td></td>
<td>Search and Seizure</td>
</tr>
<tr>
<td></td>
<td>Self-Incrimination</td>
</tr>
<tr>
<td>Guard Mount Training:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Building Checks</td>
</tr>
<tr>
<td></td>
<td>Communication Security</td>
</tr>
<tr>
<td></td>
<td>CPR / First Aid</td>
</tr>
<tr>
<td></td>
<td>Crime Scene Preservation</td>
</tr>
<tr>
<td></td>
<td>FPCONS</td>
</tr>
<tr>
<td></td>
<td>Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>Operational Security</td>
</tr>
<tr>
<td></td>
<td>Pre-Planned Response Training</td>
</tr>
<tr>
<td></td>
<td>Handcuffing Techniques</td>
</tr>
<tr>
<td></td>
<td>Personnel Searching Techniques</td>
</tr>
<tr>
<td></td>
<td>Statement Taking and Field Interview Card Info</td>
</tr>
<tr>
<td></td>
<td>Uniform Wear and Regulations</td>
</tr>
<tr>
<td></td>
<td>Use of Force Ladder of Force</td>
</tr>
<tr>
<td></td>
<td>Vehicle Stops / Searches</td>
</tr>
<tr>
<td></td>
<td>Weapons Handling / Conditions Codes</td>
</tr>
<tr>
<td>NSOXP Drills:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NSO-09-AT Active Shooter</td>
</tr>
<tr>
<td></td>
<td>NS0-06-AT- Alarm Response</td>
</tr>
<tr>
<td></td>
<td>NSO-03-AT Entry Control Penetration (ECP)</td>
</tr>
<tr>
<td></td>
<td>NSO-05-AT Vehicle Borne Improvised Explosive Device (VBIED)</td>
</tr>
<tr>
<td>Weapons Training</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Weapons Qualifications will be conducted (IAW) OPNAV 3591.F</td>
</tr>
<tr>
<td></td>
<td>M-9 Service Pistol</td>
</tr>
<tr>
<td></td>
<td>12 GA Shotgun</td>
</tr>
<tr>
<td></td>
<td>M-16 Service Rifle</td>
</tr>
</tbody>
</table>
APPENDIX G
CRIME STATISTICS EXAMPLE

Report Should Include the Following

Date of Report
Methodology
Summary and Analysis
Quadrennial Comparisons
Persons Crimes
Sexual Misconduct
DUIs
Drug Related Offenses
Property/Economic Crimes
Time and Location

Methodology Example

Military Subjects Only
Persons Crimes
- Violent Crimes: Assaults/Aggravated Assaults, Robbery, Kidnapping
- Drunk and Disorderly
- Underage Drinking
Sexual Misconduct (includes all attempts)
- Rape
- Aggravated Sexual Assaults
- Forced Sodomy
- Sexual Contact: Wrongful, Aggravated, Abusive
- Child Specific Crimes: Pornography, Indecent Acts/Liberties, Carnal Knowledge
Property/Economic Crimes
- Larceny/Shoplifting
- Damage to Property: Private and Government
- Entrance Crimes: Unlawful Entry, Trespassing, B/E, Burglary

Summary and Analysis Example

Depict increase or decrease in all category of crime as stated in Methodology
- No robbery and kidnapping incidents occurred in Dec 08 and (1) robbery and no kidnapping incidents occurred in Dec 09.
- Drunk and Disorderly incidents reduced (17%) from Dec 08 thru Dec 09.
- Slight decrease of 7% in personnel apprehended for Underage Drinking offenses
- Age break out of offenders is 19 YOA = 6, 20 YOA = 6 and 2 over 21 who provided the alcohol
- A 80% decrease in personnel apprehended for acts of sexual misconduct
- Rapes and attempts decreased from 6 in Dec 08 to 0 in Dec 09
- Sexual Contact offenses decreased from 6 in Dec 08 to 0 in Dec 09
- Aggravated Sexual Assaults saw no change with two incidents reported each month
- DUI incidents increased 133% from Dec 08 to Dec 09
- 6 of the 7 DUI incidents were detected after a traffic accident
- 4 of the incidents occurred off post and resulted in an arrest by local police
- Drug Incidents increased dramatically (111%) from 9 incidents in Dec 08 to 19 in Dec 09.
- In Dec 09, 17 of the 19 offenders were from an incident involving “Salvia”
- Property and Economic crimes saw an 86% increase from 21 in Dec 08 to 39 in Dec 09.

**Quadrennial Comparison Example**

**(FY 2010 numbers will build during the year)**
Bar Graph Example

(Rolling Two-Year Comparison)
Pie Chart Example—Time and Location

Time of Offenses

- 113 (47%)
- 57 (24%)
- 17 (7%)
- 12 (5%)
- 6 (2%)
- 3 (1%)
- 33 (14%)

Location

- 145 (60%)
- 97 (40%)

Legend:
- Off post
- On post
1. Purpose. To establish and prescribe procedures for Navy Commercial Access Control System (NCACS) access control to Commander, Navy Installations Command (CNIC) bases in the Continental United States (CONUS), Hawaii and Guam via Entry Control Points (ECPs) equipped with a Vendor/Contractor Identity Management and Installation Access Control System.

2. Background.
   a. General. NCACS (the System) is an enterprise identity management and perimeter installation access control solution. NCACS is designed to manage commercial vendors, contractors, sub-contractors, suppliers and service providers (vendors/contractors) not authorized to receive a Department of Defense (DoD) Common Access Card (CAC), regardless of how they access the installation, e.g. on foot, personally owned vehicle, delivery vehicle, semi-truck, or any other method. System participants will be enrolled, vetted, credentialed, and their access privileges to CNIC installations will be regularly and electronically updated, verified and documented upon each ingress at all perimeter ECPs.

   b. Objective and Goals. Implementation of NCACS is intended to:

      (1) Enhance installation safety and security by using a common system across the CNIC enterprise to enroll, authenticate, credential, authorize and manage access privileges of vendors/contractors coming aboard CNIC installations.

      (2) Enhance efficiency and effectiveness at Pass and Identification Offices (Visitor Control Center) through improved business processes and a significant reduction in the issuance of contractor/business passes and other locally produced credentials.

      (3) Enhance efficiency and effectiveness at all perimeter ECPs; specifically through the improved management of
vendors/contractors, their vehicles and throughput of all vehicles coming aboard CNIC installations.

c. Voluntary. Participation in NCACS is not mandatory. This SOP does not eliminate other traditional methods of permitting access to Navy Installations.

(1) Local Passes. Vendor/contractor employees not participating in NCACS may apply for local passes subject to federal, DOD, DON and CNIC policy and procedures for minimum screening, and local installation access rules and procedures. See Paragraph 4 of this SOP for specific procedures.

(2) CAC. Some contractors providing long-term services and requiring access to Navy Information Technology systems may be eligible for a Common Access Card (CAC). Eligibility for CACs is significantly limited by law and regulation. See Paragraph 5 of this SOP for specific procedures.

(3) Other Federal Credentials. Validated credentials issued by the Department of Transportation Workers Identification Credential (TWIC).

(4) PVI-I. Personal Identification Verification Interoperability (PVI-I) credentials are not generally accepted as access “flash pass” documents. Until such time as a PVI-I is determined to meet vetting standards, be amenable to electronic verification, meet all legal and regulatory standards, and is officially accepted and approved by DOD, DON, and CNIC, the credential will be limited to an identification document (See Enclosure 2).

d. Sponsors. CNIC uses a methodology that involves Navy Activities that “sponsor” contractors and vendors for issuance of either a NCACS credential or a CAC.

(1) NCACS Sponsoring Activities. A Navy Activity that desires to sponsor a vendor company for enrollment in NCACS must be designated and approved as a Sponsoring Activity (SA) by the Approved Facility Contact (AFC)—normally the Force Protection/Physical Security Specialist or the Navy Visitor Control Center Supervisor. See Paragraph 3 of this SOP for specific procedures.

(2) NCACS Single Source Coordinator. For vendors or companies having no specific relationship with a particular Navy Activity, yet having a legitimate requirement for access (such
as taxi, shuttle, and limousine services), the AFC may designate a Navy Activity that will serve as a Single Source Coordinator (SSC). A typical SSC might be Navy Exchange or Fleet and Family Support Center. See Paragraph 3 of this SOP for specific procedures.

(3) CAC Trusted Agents. A Navy Activity that desires to sponsor a contractor employee seeking the issuance of a CAC must accomplish the application through an active duty military or civil service employee Trusted Agent (TA). TAs are approved and designated by the Trusted Agent Security Manager (TASM) under the applicable procedures of the Contractor Verification System (CVS). See Paragraph 5 of this SOP for specific procedures.

(4) Privilege of Sponsorship. Contractor and vendor sponsorship by SAs, SSCs, and TAs is a privilege, not a right, and the Navy reserves the discretion to remove sponsorship at any time when in the best interests of the Government.

e. System Company. CNIC will accomplish the NCACS System effort utilizing contractor support (“System Company”).

3. NCACS Procedures

a. Enrollment. The installation and tenant organization SAs will provide the AFC a list of approved vendor/contractor companies and (for each company) the name of their designated System Company Administrator (SCA). Once the vendor/contractor company is approved, they may then enroll with the NCACS System.

b. Registration. Once enrolled, those companies may direct their employees to register into NCACS. For those vendor/contractor companies not included on the original approved vendor/contractor company list, the following applies:

(1) Vendor/contractor companies must obtain sponsorship from an installation/tenant organization SA.

(2) The SA then provides the names, addresses, and associated identification information relating to vendor/contractor companies to the AFC.

(3) The AFC then approves (or disapproves) the vendor/contractor company for addition to the approved vendor/contractor company list.
c. Employee Registration and Credentialing.

(1) The vendor/contractor company must provide the NCACS System with an approved employee list. The data required either before or during registration in NCACS may include but is not limited to:

   (a) Name  
   (b) Social Security Number  
   (c) Company/Employer Information  
   (d) Company Address  
   (e) Company Phone Number(s)  
   (f) Contract Number(s)  
   (g) Contract Date(s) of Performance  
   (h) Company-issued Employee Identification  
   (i) Number  
   (j) Individual digital photo  
   (k) Date of birth  
   (l) Fingerprints  
   (m) Declaration of U.S. Citizen  
   (n) Declaration of non U.S. Citizen  
   (o) Employee Home Address  
   (p) Employee/Personal Phone Numbers

(2) When the vendor/contractor employee(s) registers into NCACS, the System Company conducts a background screening on each vendor/contractor employee by validating an individual’s identity and biometrically authenticating their enrollment into the system.

   (a) Identity. To validate identity, the vendor/contractor employee must present one document from List A or if unavailable, two documents from list B. The lists of acceptable documents may be found in Form I-9, OMB No. 1115-0136, and Employee Eligibility Verification. These documents must be reviewed and deemed authentic to the satisfaction of the Government agent.

   (b) Biometrics. To biometrically authenticate enrollment into the system, the credential will be scanned and
the fingerprint biometric captured utilizing the handheld device provided with the system.

(3) Once the vendor/contractor employee’s identity has been validated and enrollment into the system biometrically authenticated, the credential is issued. Based upon current protocols:

(a) A NCACS credential with a green stripe, will be issued to those non-CAC eligible vendors/contractors who are United States Citizens AND who are documented/eligible for employment in the United States. Prior to issuance of the NCACS credential, these persons will present (to the Government employee issuing the NCACS credential), a valid US Passport or Birth Certificate so documenting their United States Citizenship.

(b) A NCACS credential with a blue stripe, will be issued to those non-CAC eligible vendors/contractors who are not United States Citizens, BUT who are eligible for employment in the United States. Prior to issuance of the NCACS credential, these persons will present (to the Government employee issuing the NCACS credential) documents as required from Enclosure 2 so documenting that they are eligible for employment in the United States.

(c) Non-CAC eligible vendors/contractors holding a NCACS credential with a blue stripe or green stripe are authorized unescorted perimeter access to US Navy Shore Installations covered by this policy.

(d) The credentials will be NIST-Special Publication 800-104 Aligned Topography and a FIPS PUB 201-1 Process Aligned.

d. Screening Failure. If a vendor/contractor employee fails the background screening, the employee and their company are advised in writing. Reasons for failure of the background screening and denial for participation in NCACS may include but are not be limited to:

(1) Identity verification failure
(2) Any felony conviction
(3) Registered sex offender
(4) On a terrorist watch list
(5) Any outstanding federal, state or local criminal warrant
e. Credential Issuance. Once an NCACS participant is registered, screened, validated, approved, and credentialed by the Navy, they are now eligible to access an installation.

(1) Cleared By System Company. If the vendor/contractor employee clears the background screening, the System Company creates and sends the NCACS credential to the Navy Visitor Control Center or other designated location for issuance. The System Company will inform the vendor/contractor employee of the location of the Navy Visitor Control Center where the credential will be issued.

(2) Navy Approval and Issuance. Subject to and in conformity with local SOPs, the AFC will review and approve (or deny) access to the installation and the issuance of the NCACS credential.

f. Validity. If the vendor/contractor employee passes the background screening process, the NCACS credential that is issued to the vendor/contractor employee is valid for one year. Throughout the year, the vendor/contractor employee must continue to meet background screening standards. Periodic background screenings are conducted to verify continued NCACS participation and installation access privileges. Background screening includes but is not limited to:

(1) When a vendor/contractor employee first registers to participate in NCACS.

(2) Periodic (every 92 days).

(3) When vendor/contractor registers for annual NCACS renewal.

(4) At any time, upon request by the Regional Commander, Region Security Officer (RSO), Installation Security Officer (ISO) or the Installation Commanding Officer (CO).

g. Revocation. NCACS access privileges will be immediately suspended/revoked if at any time a vendor/contractor employee becomes ineligible. Grounds for becoming ineligible and having access privileges suspended/revoked include but are not limited to:

(1) A vendor/contractor employee no longer works for the company through which he/she enrolled.

(2) A vendor/contractor employee does not pass the background screening (initial, periodic, on annual renewal).
(3) A vendor/contractor employee or company violates any NCACS rules, terms, or conditions.

(4) A vendor/contractor company requests that their employee be removed from NCACS.

(5) A vendor/contractor company is no longer eligible, ends their participation or no longer does business aboard the installation.

(6) At the direction of an ISO/RSO/CO.

h. Return of Credentials. Participating companies are required to immediately return revoked employee NCACS credentials to the System Company or the AFC, or immediately notify the System Company or the AFC in writing:

(1) That an employee has departed the company without having properly returned or surrendered the NCACS credentials;

(2) That there is a reasonable basis to conclude that an employee, or former employee, might pose a risk, compromise, or threat to the safety or security of the installation or anyone therein.

i. Appeals. Appealing initial disqualification, suspension or revocation of participation in NCACS.

(1) Any person being denied initial participation in NCACS or who has their NCACS privileges suspended or revoked for any reason, may appeal the denial/suspension/revocation.

(2) Vendor/contractor employees may initiate the appeal process when a background screen failure results in disqualification from participation in NCACS and the vendor/contractor employees does not agree with the reason for disqualification. The appeal process must be initiated within 30 days of receiving written notice of disqualification.

(3) Vendor/contractor employees may apply for a waiver when a background screening failure results in disqualification from participation in NCACS. The waiver process must be initiated within 60 days of receiving written notice of disqualification.

(4) All waiver requests will be initiated with the ISO. The CO will be the final determination authority.

(5) The ISO/CO shall consult with the Installation Legal Officer or Staff Judge Advocate when determining suitability.
j. Entry Control Point (ECP) Standards. On every ingress through a perimeter ECP, vendors/contractors participating in NCACS will present their credential. ECP personnel will scan the credential which will result in the verification of the credential, and grant of general access privileges and specific access profiles (time of day, day of week) for that installation. Further, ECP personnel may biometrically authenticate (using a fingerprint scan) the person presenting the credential to ensure that this is the same person who registered into NCACS. The following provides the procedures, roles, and responsibilities to successfully implement and execute the System:

(1) The participant presents their NCACS credentials at the perimeter ECP to the security sentry who will scan the credential utilizing the handheld device provided with the system.

(2) The handheld device will display a digital picture and the name of the NCACS participant; the company name with whom the participant is associated, check against the local (ECP) server to determine if the NCACS participant has current access privileges and meets the specific access profile (day of week and time of day).

(3) If the system responds in the affirmative, and if in the opinion of the sentry the data matches the individual requesting access, AND no other mitigating safety and security factors are present, access to the installation may be granted.

(4) Generally, NCACS participants will have access to all perimeter ECPs during all hours they are open, excluding vehicle size limitations and other physical ECP constraints. However, at credentialing the ISO/RSO or CO, can limit and/or assign specific ECP which can be used.

(5) Other than for Random Anti-Terrorism Measures (RAM) or in the case of an elevation of Force Protection Conditions (FPCON) no vehicle inspection is required.

(6) If the identity of the individual requesting entry is in question, or in the case of a RAM or elevated FPCON, a biometric (fingerprint) authentication will be made to confirm the individual is an NCACS participant.

(7) If the biometric check authenticates the individual and access privileges are current, AND no other mitigating
safety and security factors are present, access to the installation may be granted.

(8) RAMs and biometric validation of the NCACS participants and their vehicles may also be conducted as determined by the CO, RSO, or ISO.

(9) The NCACS participants may not act as escorts for other person(s).

(10) The NCACS participants are not authorized access to restricted areas unless they have their NCACS credential and are authorized access (and as locally required) for the restricted area. The NCACS participants may also be required to present a Commercial Bill of Lading (CBL) or Government Bill of Lading (GBL) when access to restricted areas is required.

(11) The NCACS participants are not required to obtain and/or display US Navy decals on vehicles they are operating onto an installation.

k. Interim Eligibility. Vendor/contractor employees who have registered to participate in NCACS, but who have not yet completed the background screening and have not received a credential, may be provided interim access approval until they are authorized participation in NCACS or denial to participate in the System.

(1) Interim access will not exceed a period of twenty-eight (28) calendar days.

(2) Interim access may be renewed, subject to the approval of the AFC and guidance of the local SOP.

l. Taxi, Limousine, and Shuttle Access. Access procedures and standards for taxis, limousines, and shuttle services, will be governed by:

(1) The NCACS System as described herein; or

(2) A locally issued pass (See Paragraph 4 below); or

(3) At the election of the CO, under the process and procedures of CNICINST 5530.1A. In the event that this process is made available to taxis, limousines, and shuttles, the CO must ensure compliance with all of the standards of those laws and regulations found at Enclosure 1 of this SOP. Until these
standards can be adhered to, passes will be limited in duration to one (1) day.

4. **Locally Issued Passes.** In the event that a vendor elects not to participate in NCACS, or the contractor is ineligible to receive a CAC, the individual employee may apply for a locally issued pass in order to access to the installation.

   a. **Local SOP.** Installations and Regions will establish individual SOPs to properly implement the guidance of Federal, DOD, Navy, and CNIC guidance. The SOPs will include detailed standards and procedures for the application, issuance, and the authentication of passes, including, at a minimum, the following:

      (1) **Processing.** Must be processed at the Navy Visitor Control Center, under local and higher directive procedures.

      (2) **Vetting.** Will undergo necessary personal identification and background checks including but not limited to:

         (a) National Criminal Investigation Check (NCIC) background check.

         (b) Will meet the requirements as set forth in OPNAVINST 1752.3; POLICY FOR SEX OFFENDER TRACKING, ASSIGNMENT AND ACCESS RESTRICTIONS WITHIN THE NAVY, dated, 27 MAY 2009.

         (c) Will be checked against the local no entry and debarment lists.

         (d) Will undergo other such additional checks as required by current, revised, or newly issued federal directives, DoD policy, DoN Policy, or CNIC Directives.

         (e) Will undergo any additional checks as otherwise required or deemed appropriate by the RSO, ISO, or the CO.

   b. **Time Limitation.** The CO has the authority to permit access to the Installation, together with the responsibility to ensure that permitted access comports with applicable law, regulation, and policy. Accordingly, the following guidance is provided:

      (1) The initial enterprise-wide time standard for the validity of a pass to access an installation will be not more than one (1) day.
(2) If an Installation identifies a need to issue passes that exceed the enterprise-wide time standard:

(a) The Installation SOP will identify the basis and rationale for the time period of passes issued. Factors such as security posture, resources for monitoring, high-risk assets, and related considerations must be considered and addressed.

(b) Passes will be issued for a period of time commensurate with the level of vetting accomplished by the Installation Visitor Control Center/Pass Office. In the event that only minimal vetting is possible, it is to be anticipated that only minimal periods of access will be permitted.

(3) Periods of validity may be curtailed or restricted in the future by Federal, DOD, Navy, and CNIC guidance.


a. In most cases, general vendors are not eligible for Common Access Cards (CAC). A CAC is not appropriate for vendor employees who provide temporary services; who are hired for short-term (less than six months) projects; who merely deliver goods or supplies to Navy installations; or who are employed to provide goods or services wholly ancillary to the core Navy missions (such as workers at an on-base concession store/snack bar). Only those individual contractors who have a legitimate basis for requesting a CAC, such as embedded (co-located) advisory and assistance contractors; contractors having long-term and routine access to multiple installations to support core Navy functions; contractors performing duties requiring access to Navy IT systems (e.g., NMCI); and contractors performing under Statements of Work (SOWs) and Performance Work Statements (PWSs) that properly and legitimately identify their personnel as qualified for a CAC will be considered eligible. For this purpose, entitlement to a CAC will require a need for both physical access to a Navy installation or facility and logical access to NMCI.

b. In the event that a TA determines that the issuance of a CAC to a specific contractor employee is appropriate, the TA must ensure that all Federal, DOD, DON, CNIC, and local rules, policies, and procedures are followed, and that proper vetting and background investigation(s) are accomplished. The TA is responsible for compliance with the following authorities:
6. Responsibilities.

   a. Enrollment and registration into NCACS is the sole responsibility of the vendor/contractor company.

   b. Navy Regions and installations will issue written guidance (Implementing Local SOPs) that articulate the specific provisions and requirements of this. This SOP may be supplemented by individual Regions and installations to the extent that it does not conflict or give authority beyond the guidelines established in the SOP, federal law and DOD/DON policy. All activity supplements must be approved by the parent Navy Region.

   c. COs have the authority over, and responsibility for, the safety and security of an installation. While discretion is vested in the authority of the CO, compliance with all legal requirements must be adhered to, and deviation from the guidance of this SOP must be subject to careful consideration.

   d. Installations will identify a Trusted Agent (TA) for the NCACS System. Responsibilities may include but are not limited to; providing an Approved Vendor/Contractor Company List (ACL), identifying NCACS Sponsor(s) and updates, coordinating command, installation and tenant sponsor briefings, coordinate guard/police training, develop Standard Operating Procedures (SOPs) for implementation of NCACS installation access.
e. Tenant Organizations will provide an ACL, identify NCACS Sponsor(s), and ensure updates to both.

f. The NCACS System Company is responsible to:

(1) Purchase and maintain ownership of System hardware and software (System equipment).

(2) Install equipment.

(3) Coordinate implementation of NCACS.

(4) Communicate with vendors/contractors participating in NCACS.

(5) Conduct a background screening(s) on the participating vendor/contractor employee(s).

(6) Manufacture a Federal/Navy-approved format credential if the vendor/contractor employee passes the background screening.

(7) Forward and submit all manufactured credentials to the Navy AFC for approval and issuance.

(8) Notify vendor/contractor employee that their NCACS credential has been forwarded to the Navy for issuance. Inform the vendor/contractor employee of the location of the Navy Visitor Control Center where the credential will be issued.

(9) Monitor access privileges which will be immediately suspended or revoked, if at any time a vendor/contractor employee becomes ineligible to continue participation in NCACS.

(10) Provide monthly reporting on the NCACS System to the installation.

(11) Provide life cycle maintenance and support for the NCACS System.
Enclosure 1

List of Applicable Authorities

• HSPD-12; Homeland Security Presidential Directive

• DTM-09-12; Directive Type Memorandum

• FIPS-201; Federal Information Processing

• P.L. 110-181 (FY 2008) Sec 1069; Public Law, Standards for Entry to Military Installations in the United States

• OPNAVINST 1752.3; Operations Naval Instruction, Policy for Sex Offender Tracking, Assignment and Access Restrictions within the Navy, dtd 27 May 2009

An additional authority is anticipated in the near future:

• OPNAVINST 5530.14X(Implementation of DTM-09-12); Navy Physical Security and Law Enforcement Program
### Lists of Acceptable Documents

All documents must be unexpired.

**LIST A**
Documents that Establish Both Identity and Employment Authorization

1. U.S. Passport or U.S. Passport Card
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa
4. Employment Authorization Document that contains a photograph (Form I-766)
5. In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, as long as the period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form
6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association between the United States and the FSM or RMI

**LIST B**
Documents that Establish Identity

1. Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address
2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address
3. School ID card with a photograph
4. Voter's registration card
5. U.S. Military card or draft record
6. Military dependent's ID card
7. U.S. Coast Guard Merchant Mariner Card
8. Native American tribal document
9. Driver's license issued by a Canadian government authority

For persons under age 18 who are unable to present a document listed above:

10. School record or report card
11. Clinic, doctor, or hospital record
12. Day-care or nursery school record

**LIST C**
Documents that Establish Employment Authorization

1. Social Security Account Number card other than one that specifies on the face that the issuance of the card does not authorize employment in the United States
2. Certification of Birth Abroad issued by the Department of State (Form FS-545)
3. Certification of Report of Birth issued by the Department of State (Form DS-1350)
4. Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal
5. Native American tribal document
6. U.S. Citizen ID Card (Form I-197)
7. Identification Card for Use of Resident Citizen in the United States (Form I-179)
8. Employment authorization document issued by the Department of Homeland Security

Illustrations of many of these documents appear in Part 8 of the Handbook for Employers (M-274)