



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVENUE, S.E.
WASHINGTON NAVY YARD, DC 20376-0001

In Reply to
NAVSEAINST 5510.2C
Ser 09P/287
7 Aug 12

NAVSEA INSTRUCTION 5510.2C

From: Commander, Naval Sea Systems Command

Subj: NAVSEA ACCESS AND MOVEMENT CONTROL

Ref: (a) OPNAVINST 5530.14E CH-1

Encl: (1) NAVSEA Access and Movement Control Manual

1. Purpose. To update policy and procedures for access and movement control per reference (a), at all elements of the Naval Sea Systems Command and its affiliated Program Executive Offices (PEOs).

2. Cancellation. NAVSEAINST 5500.3A, NAVSEAINST 5510.2B and NAVSEAINST 5530.3A.

3. Scope and Applicability. This instruction addresses the access and movement control for all elements of NAVSEA including headquarters, field activities, and affiliated PEOs.

4. Action. All military, government civilian, and contractor personnel assigned to NAVSEA headquarters, affiliated PEOs, and field activities (including but not limited to NAVSEA shipyards, SUPSHIPS, regional maintenance centers, and warfare center divisions) shall comply with reference (a), the provisions of this instruction and the latest version of enclosure (1). This instruction is effective immediately.


M. E. JABALEY
Vice Commander

Distribution:

Electronically via the NAVSEA Intranet Website located at
<https://navsea.portal.navy.mil>

This page left intentionally blank

NAVSEA ACCESS AND MOVEMENT CONTROL MANUAL

August 2012



Director of Security,
Naval Reactors (SEA 08B)

Published by:
Director, Office of Security Programs
and Continuity Planning (SEA 09P)

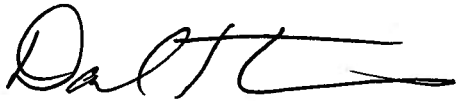
This page left intentionally blank

FOREWARD

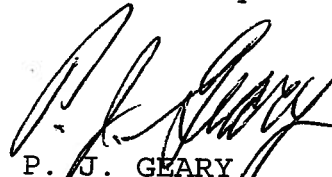
This NAVSEA manual combines three major instructions, and addresses Access and Movement Control at all elements of NAVSEA including headquarters, field activities and affiliated PEOs.

References (a) through (l) are listed in Appendix A. The definition of specific words, phrases and acronyms used in this manual are listed in Appendix B. Enclosure (1) is the Foreign National Access to Naval Vessels Clause. Enclosure (2) is the Foreign National Access to Naval Vessels (ACP Certification).

All personnel assigned to NAVSEA Headquarters, field activities and affiliated PEOs are responsible for implementing the provisions of this manual according to NAVSEAINST 5510.2C. It should be read in its entirety. While implementing the provisions of this manual, we must remember inadequate secrecy and access controls allow our potential adversaries to cause us harm but excessive secrecy inhibits our ability to conduct our own operations.



D. S. TROEGER,
Director of Security,
Naval Reactors (SEA 08B)



P. J. GEARY
Director, Office of
Security Programs and
Continuity Planning (SEA 09P)

This page left intentionally blank

7 Aug 12

TABLE OF CONTENTS

PARAGRAPH		PAGE
Chapter 1: NAVAL SHIPYARDS		
1-1	Scope	1-1
1-2	Standard Access Control Badges	1-1
1-3	Types of Badges	1-2
1-4	Colors Used on Standard Access Control Badges (Permanent or Temporary)	1-3
1-5	Category Identifiers	1-5
1-6	Authority to Remove Standard Access Control Badges from Shipyards	1-5
1-7	Controlled Areas	1-5
1-8	Events	1-18
1-9	Visitors.	1-20
1-10	Photography and Recording Devices	1-23
1-11	Disciplinary Action	1-25
Chapter 2: FIELD ACTIVITIES OTHER THAN NAVAL SHIPYARDS		
2-1	Scope	2-1
2-2	Standard Access Control	2-1
2-3	Visitors	2-1
2-4	Photography and Recording Devices	2-3
2-5	Disciplinary Action	2-6
Chapter 3: HEADQUARTERS		
3-1	Scope	3-1
3-2	Risk Mitigation	3-1
3-3	Standard Access Control	3-1
3-4	Unescorted Access	3-3
3-5	Visitors	3-3
3-6	Escorts	3-5
3-7	Building Support Personnel	3-6
3-8	Media Event Access	3-7
3-9	Special Event Access	3-8
3-10	Classified Events	3-8
3-11	Prohibited Items	3-8
3-12	Photography and Recording Devices	3-9
3-13	Disciplinary Action	3-11

Chapter 4: FOREIGN NATIONAL ACCESS TO NAVAL VESSELS

4-1	Scope	4-1
4-2	Standard Access Control	4-1
4-3	Application	4-2
4-4	Action	4-2
4-5	Disciplinary Action	4-5

Enclosure (1) Foreign National Access to Naval Vessels Clause

Enclosure (2) Foreign National Access to Naval Vessels (ACP
Certification)

Appendix A: References

Appendix B: Definitions

CHAPTER 1

NAVAL SHIPYARDS

1-1. Scope. This chapter updates requirements for physical security, access, and movement control for the naval shipyards. It defines specific types of areas within a shipyard, establishes the minimum physical security requirements for these areas (e.g. fences, posting of signs, etc.) as well as the requirements for sensitive work periods. It also defines the badge or identification systems required for access to these areas, and establishes procedures for special events. This manual is not directly applicable to remote shipyard sites (San Diego, Kings Bay, etc.) but should be used as guidance for shipyard controlled facilities at remote sites.

1-2. Standard Access Control Badges. Standard access control badges ensure uniformity of security identification. Badging for personnel visiting civilian or military service oriented functions outside the Controlled Industrial Area (CIA) is optional, based upon locally developed regulations.

a. Shipyard badges are the industry standard, 2 1/8 inches by 3 3/8 inch size. Badges must contain the NAVSEA logo at the top with the issuing shipyard name underneath. Permanent personnel badges must have a photograph with an authenticating signature along the left side.

b. The following statement must be placed on the back of the card:

U.S. GOVERNMENT PROPERTY
LOSS OF THIS CARD MUST BE REPORTED AT ONCE.

WARNING: ISSUED FOR OFFICIAL USE OF THE HOLDER
DESIGNATED HEREON. USE OR POSSESSION BY ANY OTHER
PERSON IS UNLAWFUL AND MUST MAKE THE OFFENDER LIABLE
TO PENALTY UNDER TITLE 18, U.S.C. 499, 506 AND 701.

IF FOUND, DROP IN ANY U.S. MAILBOX.
POSTMASTER - POSTAGE GUARANTEED.
RETURN TO: (Insert appropriate address for local
pass & ID offices)

c. Display badges in the performance of official duty only with the photograph facing out and above the waist. Pouches,

7 Aug 12

sleeves or other implements used to hold the badge must not obscure the face in any way nor alter the badge color. Personnel must maintain their badge in good order protecting it from loss, damage or misuse. No ornaments must be attached to the badge (e.g. 25 year service pin, command award pin, safety, or donor's pin, etc.). Shipyards may develop local policy for instances where the wearing of the badge externally is not appropriate such as "clean" environments in refueling areas.

d. Badges must be returned to the issuing agent for destruction when no longer valid. When badges are turned in they are to be cut into quarters, as a minimum, before disposal.

e. Lost or Misplaced Permanent/Temporary Access Control Badges must be reported immediately to security for removal from the Automated Entry Control System (AECS). A new badge with a new series number must then be issued. A method will be developed to ensure a lost badge can be immediately rendered unusable as soon as it's reported lost.

1-3. Types of Badges. The following types of standard access control badges are authorized for identification of individuals who have a need to access certain areas of the shipyard. Written procedures for each must be established locally.

a. Permanent Access Control Badges must be issued to employees requiring continued access to the shipyard. Photographs are required with the exception of military personnel. Civilian/Military personnel employed at second or part-time positions within the shipyard may be issued more than one badge at the shipyard's discretion.

(1) Badges must contain a permanently affixed photograph, expiration date (not to exceed three years from the date of issue), and badge number, plus the individual's name and signature.

(2) The photograph's background color must correspond to the color of the badge. The back of the badge must contain a magnetic strip for shipyard employees/tenant commands.

b. Military personnel are an exception and do not require a signature or photo on their identification badge. However, they must be required to have photo identification (i.e. Common Access Card (CAC)) in their possession.

7 Aug 12

c. Temporary Access Control Badges must be issued to individuals requiring temporary access to various areas within the shipyard. Photographs and signatures are not required but all such personnel must have other photo identification in their possession. Temporary access control badges must expire no more than 90 days from the day of issuance.

d. Shift badges must be issued to individuals who have forgotten their badge. At the shipyard's discretion, shift badges may also be used for personnel who have lost their badge and seek entry to the shipyard outside of normal Pass and Identification office hours. Shift badges may be issued by the CIA or facility entrance guard after verifying the person has been issued a valid badge. The shift badge must have the same color as permanent or temporary badges, must be a non-proximity badge, and must not include the name or signature of the individual nor any encoding or barcode. In lieu of a photograph, the field shall prominently read, "SHIFT BADGE, ONE SHIFT ONLY, DO NOT REMOVE FROM THE FACILITY". Shift badge numbers must consist of a random, sequential, or the employee's permanent badge number displayed on the last line of the badge. These badges must be accounted for locally.

1-4. Colors Used on Standard Access Control Badges

a. White Badges provide access to non-sensitive areas if desired by the shipyard, with specific procedures developed locally.

b. White "ESCORT REQUIRED" badges, marked in RED across the front of the badge, must be issued to:

(1) Foreign nationals approved by NAVSEA 08B and 09P (when no approved Security Island Program exists). Foreign nationals are defined in reference (e).

(2) Un-cleared contractors, and non-appropriated fund personnel who require one-time access to the CIA.

(3) Un-cleared visitors requiring access into the CIA.

c. Green Badges provide unescorted access to the CIA and Security Islands, excluding access to Nuclear Work Areas (NWAs) and Controlled Nuclear Information Area's (CNIAs), for the following personnel:

(1) Un-cleared permanent, temporary and military personnel where U.S. citizenship has been verified.

(2) Shipyard employees where access to classified information has been temporarily suspended pending security clearance action and whose continuing access to the CIA has been determined by the Shipyard Commander to be in the best interest of the shipyard.

(3) Foreign nationals serving as crew members aboard U.S. Navy ships berthed in the CIA, subject to the Uniform Code of Military Justice (UCMJ).

Green Badges will be used instead of Yellow or Red Badges, regardless of clearance, if a person does not need access to a CNIA, NWA, Secure Room or classified information.

d. Yellow Badges provide unescorted access to the CIA, CNIA and Security Islands, excluding access to NWAs and access to Restricted Data, for the following personnel:

(1) Permanent, temporary and military personnel with an adjudicated government clearance that are not authorized access to Restricted Data (RD).

(2) Permanent, temporary and military personnel with an interim security clearance (temporary access).

e. Red Badges provide unescorted access to the CIA, CNIA, Security Islands, and NWAs, for the following personnel:

(1) Permanent, temporary and military personnel with an adjudicated government clearance that are authorized access to RD.

(2) Contractor personnel must not be issued Red Badges unless all requirements of the NISPOM are met, to specifically include a DD-254 or other document specifically authorizing access to RD.

(3) Janitorial and/or other tradesmen such as plumbers, electricians, etc., can be issued Red Badges provided they have the proper clearance. However their exposure to sensitive and classified material will be limited whenever possible.

f. Blue Badges provide access into the CIA (at shipyards with an approved Security Island Program). This badge must be

7 Aug 12

blue in color and issued to foreign nationals for identification purposes. Each badge must be properly annotated with the letters "FN" somewhere on the front of the badge and must be easily recognizable by shipyard personnel from a distance. The magnetic strip and bar code on standard access control badges issued to foreign nationals shall not be encoded and therefore must not be capable of operating an AECSSs.

1-5. Category Identifiers must be used to identify contractors and visitors. Each badge must be prominently stamped with the appropriate identifier and indicate when an escort is required. Authorized category identifiers are:

C = Contractors

V = Visitors (U.S. citizens only)

FN = Foreign National

1-6. Authority to Remove Standard Access Control Badges (SACBs) from Shipyards (except escort required badges and shift badges) is granted to shipyard employees, ship's personnel, and tenant activity personnel until the badge expiration date, issuance of a permanent badge, termination of employment, or shipyard re-badging. Civilian/military personnel of other DoD commands/components, and all other federal agencies, and contractors may be authorized by the shipyard to remove permanent and temporary badges from the issuing shipyard throughout officially authorized visit periods. SACBs must be confiscated from those personnel whose access to classified information has been suspended in accordance with reference (a).

1-7. Controlled Areas

a. Controlled Industrial Area (CIA)

(1) Physical Security Requirements. CIAs shall be designated a Level 2 "Restricted Area", with trained armed military personnel, certified/licensed civil service police or guards, or by approved AECS in accordance with reference (b) of this manual, with the following additional requirements:

(a) A lighted perimeter

(b) Centrally terminated Intrusion Detection Systems (IDS) on emergency exits from buildings that form part of the CIA perimeter or General Field Service Security Padlocks

7 Aug 12

FF-P-2827A or the High Security S&G 433C or 951 meeting MIL-DTL-43607, on points of entry/exit to the CIA.

(c) Waterfront areas must be protected by either of the following measures:

1. U.S. Fleet Forces Command Operational Order 3300-11; or

2. Harbor security boat patrols conducted per reference (b).

(d) Vehicular access entry and exit lanes require solid barriers, (e.g., keel blocks, concrete "jersey bounce" barriers to create curves or turns at entry points). A balance between safety and security must be achieved to permit rapid access for emergency vehicles. All access gates that undergo significant modification should be made to comply with UFC 4-022-01, Entry Control Facilities/Access Control Points.

(e) Changes affecting the CIA boundary must be forwarded, in writing, to NAVSEA 08B and 09P for information.

(f) CIA security fences must be 12 feet high without an outrigger. Outriggers for a 12 foot fence are not required. Most fences meet the previous standard of 8 feet. Changes to old fencing are not required by the new height requirement. However, all modifications or new fencing built after the date of issuance of this instruction must be 12 feet in height.

(g) Armed guards shall check for signs of attempted or successful unauthorized entry and for other activity which could degrade the security of the CIA. At a minimum, checks must be made every eight hours during normal working hours and every four hours after normal working hours.

(2) Access Controls. Access to a CIA must be controlled by each of the following:

(a) Fully trained and armed military personnel, civil service guards or police or an approved AECS.

(b) If AECS is not utilized, then guards must check badges by individually handling each badge (i.e. touching) to compare the photograph on the badge with the face of the bearer.

7 Aug 12

(3) Access Control Privileges. Access to a CIA must be limited to personnel who meet one of the following requirements (subject to the escort requirements specified in this manual):

(a) U.S. civil servant and contractor personnel who have official business within the CIA.

(b) Ships personnel and foreign nationals subject to the UCMJ assigned to U.S. Navy Ships berthed in the CIA.

(c) U.S. citizen contractor personnel.

(d) Official visitors (i.e., local, state or federal officials), who have been approved by NAVSEA 08B and 09P).

NOTE: State or federal regulatory visits to Non-Sensitive Areas (NSAs) within the CIA may be locally approved with a Generic Security Plan pre-approved by NAVSEA 08B and 09P.

(e) Foreign Nationals accessing the shipyard CIA (when no approved Security Island Program exists) other than ships force of ships berthed in the CIA, must be approved by NAVSEA 08B and 09P.

(f) Personnel who have a final government or interim security clearance with a need-to-know.

(g) Military personnel who are approved by the Shipyard Commander including U.S. Navy personnel who are Foreign Nationals and assigned to the shipyard, tenant and co-located commands.

(h) Persons with a high potential for employment or recruiting purposes, provided there is no access to classified, controlled unclassified, information (CUI), NNPI, CNIAs, or Security Islands.

(i) Access by agents of Naval Criminal Investigative Service (NCIS), must be authorized if visit procedures and requirements of this manual and reference (b) of this manual are met. Official NCIS credentials may not be used in lieu of the standard access control badge for access into the CIA for non-emergency purposes.

(j) Access to NNPI by reservists for active duty training shall be handled in accordance with reference (c) of this manual.

(k) Government vehicles including government leased or rented equipment may be brought into the CIA provided they are marked with license plates (such as GSA plates) or other identifiers and are being used to conduct official business. Official vehicles (including non-government vehicles for government employees on official government business) may be authorized access into the CIA by the Shipyard Director of Security.

(l) Contractor/commercial vehicular access to the CIA must be minimized and all vehicles must comply with the following requirements:

1. All contractor/commercial vehicles must be visually inspected prior to any entry into a CIA.
2. Vehicles must visibly display a CIA vehicle entry pass.
3. Vehicles must clearly display an authorized company sign or logo.
4. Vehicles must only be allowed in the CIA for transportation of contractors' tools, parts, and materials to and from the work site with the exception of MILCON scope projects. In this case, contractors may transport employees to and from work sites if a specific security plan has been developed and approved by the Shipyard Director of Security.

(m) Parking of privately-owned vehicles, including vanpools and private buses, within the CIA is prohibited. The Shipyard Director of Security may approve an exception to this policy for handicapped personnel.

(n) Emergency response personnel and vehicles must be provided unimpeded access to the emergency area. Emergency procedures must address at least the following:

1. Human safety must be the primary concern.
2. Ambulance, fire and other emergency vehicles must have unimpeded access during an emergency.
3. To whom emergencies must be reported (e.g., local 911, shipyard/regional emergency dispatch center, Director of Security).

7 Aug 12

4. Escort requirements must not impede emergency access.

5. Debriefing of emergency personnel when there was access to classified information at an appropriate time after resolving the emergency.

6. Coordination of emergency response operations (e.g., notifications, review local/regional emergency response operations, en-route procedures).

(o) Shipyard Commanders are authorized to invite relatives, dependents, or a limited number of personal guests for unclassified visits into the CIA. Members of ships forces berthed in the CIA may request visits by their relatives, dependents, or a limited number of personal guests (normally not to exceed 3 guests each).

1. Shipyard Commanders, and Commanding Officers of ships berthed within the CIA are to ensure this policy on visitation is not abused and does not interfere with mission requirements of the shipyard. Further, Shipyard Commanders may reduce the number of guests authorized as necessary.

2. Requests for entry of relatives, dependents or guests may be approved by the Shipyard Commander for periods between:

a. 0800-2200 Monday - Thursday; and

b. 0800-1630 on Friday, Saturday, Sunday, and approved federal holidays.

3. Access to CNIAs, NWAs, and Security Islands, are not authorized without SEA 08B and SEA 09P approval. Shipyard Director of Security must establish local procedures which must include a review of sensitive work, proposed routes to be used, safety related problems and escort requirements for these visitors for the period of time they must be in the CIA.

4. Parents must keep their young children within their immediate proximity with positive parental supervision at all times.

5. Considering the above, a Shipyard Commander may only authorize a Change of Command or other ceremony within the CIA during the above time periods provided it does not

7 Aug 12

interfere with shipyard work and does not include such things as media, civilian bands, schools, general public and city, county or state officials in an official capacity. No other times or days for such events must be authorized.

6. Vendors and contractors must not be brought into the CIA under relative, dependent, or CO's personal guest procedures.

(4) Official Visits

(a) Official visits must be coordinated with the Director of Security and approved by the Shipyard Commander. Coordination must include procedures for Routine and Non-Routine visits.

(b) Public Affairs activities related to CIAs shall be coordinated with the Shipyard Public Affairs Officer (PAO), Director of Security and the Naval Nuclear Propulsion Information Control Officer (NNPICO).

b. Nuclear Work Area (NWA)

(1) Physical Security Requirements. NWAs must be designated in writing by the Shipyard Director of Security and a current listing must be maintained by the security office. All NWAs must be validated by the NNPICO annually. Additionally, SEA 08B and SEA 09P must conduct compliance audits of NWAs during biennial physical security inspections. An NWA must be constructed and protected as noted below:

(a) An NWA must have a clearly defined perimeter. An NWA must be enclosed on all sides (i.e., walls, ceilings and floor) with the equivalent of a chain link fence or other barrier which will prohibit unauthorized entry. The perimeter may be a fence, the exterior walls of a building or structure, or the internal walls surrounding a space within a building or structure. Visual access to NNPI from outside a NWA must be denied.

(b) NWAs can be secured, when not manned, by using an AECS in conjunction with IDS.

(c) If an AECS is not used to secure the NWA, the access doors must be secured with a combination lock meeting the requirements of Federal Specification FF-L-2740, FF-L-2890 or MIL-FF-P-110_F or a key-operated padlock meeting the

7 Aug 12

requirements of MIL-P-43607 or a deadbolt lock meeting the requirements of UL-437. Keys must be controlled and under constant accountability.

(d) When secured, NWA's must be checked by an armed sentry at least twice per eight-hour shift without AECS or once per eight-hour shift with AECS if equipped with a centrally terminated IDS.

(e) A NWA sign must be posted at the entry point(s). Each sign must measure 12 inches high and 24 inches long with ¼ inch black letters and border on a white background that read: NUCLEAR WORK AREA (next line) RED SECURITY BADGE REQUIRED. Smaller signs may be used as needed in confined spaces such as ships or submarine hatches. The wording must be the same.

(f) All propulsion plant spaces of nuclear powered warships are NWA's and must be included in the active Shipyard NWA/CNIA listing. Propulsion plants of nuclear powered warships need not have barriers at all potential entrances.

(g) During availabilities, the Shipyard Director of Security may authorize Yellow-badged personnel access to specific propulsion plant spaces if there is a shortage of Red-badged (final cleared) workers. A security plan must be developed to ensure the necessary compensatory measures are in place to provide adequate security including:

1. Training of all Yellow and Red-badged shipyard personnel and Ship's Force assigned to the project;

2. The areas must be sanitized and safeguards must be put in place to prevent inadvertent disclosure of classified Naval Nuclear Propulsion Information (NNPI);

3. Senior project personnel must conduct tours of these spaces during each shift to verify NWA/CNIA controls are in place;

4. Shipyard Security Office personnel must conduct periodic surveillances to ensure all of the compensatory measures are in place;

5. Prior to allowing Yellow-badged personnel into these spaces, senior personnel involved with the project must tour the spaces and verify physical controls are satisfactory.

7 Aug 12

(2) Access Control. Only persons who possess a red shipyard badge must be permitted unescorted access to a NWA. Access by a person with a yellow badge is authorized if they are escorted by a person with a Red badge who is familiar with the area and the space is sanitized to avoid the disclosure of classified NNPI. Access to NWA's must be controlled by:

(a) Use of an AECS, (system may include use of the Personal Identification Number (PIN)); or

(b) Use of a manual access control system controlled by guards, watchmen, receptionist or other appropriately trained and cleared personnel (who have been issued a Red badge).

NOTE: Except as authorized by section 1-7 b.(1)(g) access to the propulsion plant spaces of a nuclear powered warship is only authorized for individuals with a Red badge (final government clearance) unless otherwise approved by SEA 08B and 09P.

(3) Access Control Privileges

(a) Access must be limited to those persons badged in accordance with paragraph 1-4 of this chapter and who meet one of the following requirements:

1. Personnel who have final security clearances based on formal investigations, who have been issued red standard access control badges and whose official duties require such access.

2. Personnel who have been issued a Yellow badge if they are escorted by a person knowledgeable of the NWA with a Red Badge, and the space is sanitized to avoid the disclosure of Restricted Data (RD). The escort of persons with Yellow badges may be authorized on a case by case basis by the shipyard's Director of Security who must ensure safeguards are put in place to prohibit inadvertent disclosure of RD.

3. Access to an NWA for White "escort required" badged or Green badged personnel for the performance of actions of an immediate nature (e.g., air conditioning repair, etc.) is authorized, provided: the employees are U.S. citizens, classified NNPI can be sanitized or access to classified and reactor plant information prevented, and the White or Green badged personnel are under continuous escort by a Red-badged

7 Aug 12

person knowledgeable of the NWA. Otherwise, White or Green badged personnel are not authorized access to NWAs.

(b) Medical personnel may be granted access to sanitized nuclear aircraft carrier and nuclear submarine reactor compartments for the purpose of an orientation tour provided:

1. No tours must be conducted in FPCON CHARLIE or higher.

2. All visitors shall be informed before entering the shipyard that photography is not permitted.

3. Medical responders must be continuously escorted by Red-badged Radiological Control Office (RADCON) employees familiar with the areas inside the reactor compartments and reactor auxiliary rooms.

4. All personnel acting as escorts must be trained to know escorted personnel cannot be given access to classified material or NNPI and must only be authorized to the area using the most direct route to the open reactor compartment.

5. Concurrence must be received from the ship, project and shipyard security officers in advance of such tours.

6. No more than 5 medical responder personnel may be escorted at a time.

7. The medical personnel must be U.S. citizens.

8. Tour routes must be properly sanitized prior to the start of the visit by shrouding, covering or removing equipment and materials considered sensitive to protect against any visual or physical access.

c. Controlled Nuclear Information Area (CNIA)

(1) Physical Security Requirements

(a) CNIA's must be designated in writing by the Shipyard Director of Security and a current listing must be maintained by the security office. All CNIA's must be validated by the NNPICO annually. Additionally, NAVSEA 08B and 09P must

7 Aug 12

conduct compliance audits of CNIAs during biennial physical security inspections with the following requirements:

1. A CNIA must be a clearly defined perimeter, constructed of permanent construction materials; (e.g., fencing, plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials) offering resistance to, and evidence of unauthorized entry into the area.

2. Visual access to NNPI from outside a CNIA must be denied. This can be accomplished by placing opaque material, blinds, or similar applications over windows and other openings.

3. IDS are not required on a CNIA.

4. An AECS can be used to secure the CNIA when it is not manned. The use of locks in conjunction with AECS is not required.

5. If AECS is not used to secure the CNIA, the access doors must be secured with a combination lock meeting the requirements of Federal Specification FF-L-2740, FF-L-2890 or MIL-FF-P-110_F or a key-operated padlock meeting the requirements of MIL-P-43607 or a deadbolt lock meeting the requirements of UL-437. Keys must be controlled and under constant accountability.

6. CNIAs must be checked by an armed sentry at least once every twenty-four hours unless protected by centrally terminated IDS in which case the area must be checked on a random basis as part of other patrols.

7. CNIA signs must be posted at the entrances. Signs must measure 12 inches high and 24 inches long with black letters on a white background that read: CONTROLLED NUCLEAR INFORMATION AREA (next line) RED OR YELLOW SHIPYARD BADGE REQUIRED. Smaller signs may be used as needed in confined spaces such as ship or submarine hatches. The wording must be the same.

(b) Temporary Establishment of CNIAs. Occasionally, shipyards may be required to perform work on unclassified reactor plant equipment in shop areas not designated a permanent CNIA. A temporary CNIA may be established during the period of time the equipment is being worked on. The temporary CNIA must

7 Aug 12

be disestablished upon completion of the work. The following procedures apply:

1. A tape or line must be fastened around the immediate area where the work is to be performed. A sign must identify the area as a temporary CNIA.

2. An individual, such as the equipment operator, must be assigned responsibility for controlling access to the roped off area and any unclassified reactor plant components or software.

3. If the software (e.g., diagrams, plans, drawings, etc.) is not present, the responsible individual is not required to be in the immediate area at all times during normal working hours (e.g., lunch, tool draw, etc.). However, the equipment (i.e., hardware) must be stowed in a permanent CNIA during other time periods (i.e., weekends); when it is not practical to assign an individual to control access.

4. Establishment of temporary CNIAs does not require the shipyard NNPICO or Shipyard Director of Security approval. However, each shipyard production group must have procedures in place for the establishment and control of temporary CNIAs.

(2) Access Control. Only persons who possess a Red or Yellow shipyard badge must be permitted unescorted entry into a CNIA. Access by a person with a Green badge is authorized if they are escorted by a person with a Red or Yellow badge who is familiar with the area and the space is sanitized to prevent the disclosure of NNPI. Access to CNIAs must be controlled by:

(a) Use of an AECS, (system may include use of a PIN); or

(b) Use of a manual access control system controlled by guards, watchmen, receptionist or other appropriately trained and cleared personnel (who have been issued a Red or Yellow badge).

(3) Access Control Privileges

(a) Unescorted access to the CNIA must be limited to those individuals who have a need-to-know and have either Red or Yellow badges.

7 Aug 12

(b) Access for purposes of an immediate nature is authorized for White "escort required" badged or Green badged personnel provided:

1. They are U.S. citizens, under continuous escort by a Red or Yellow-badged person knowledgeable of the CNIA; and

2. All classified information and unclassified Reactor Plant Information can be sanitized or access can be prevented.

d. Security Islands (SI) - An area where access to unclassified NNPI and/or sensitive unclassified technical information by unauthorized personnel is precluded. A Security Island can be, but is not limited to, a building, office, fenced area, dry dock, pier, or trailer. A Security Island will have a clearly defined perimeter, signs and controlled access.

(1) Physical Security Requirements

(a) Security Islands must be designated in writing by the Shipyard Director of Security and a current listing must be maintained by the security office. Security Islands must be validated by the NNPICO annually. Additionally, SEA 08B and 09P must conduct compliance audits of security Islands during biennial physical security inspections.

(b) Security Islands must have a clearly defined perimeter. This perimeter may be a fence, the exterior walls of a building or structure (e.g., dry-dock or ship), or the internal walls surrounding a space within a building or structure.

(c) Access to classified information from outside a Security Island must not be allowed. Short term casual observance of controlled unclassified information or Unclassified Naval Nuclear Propulsion Information (U-NNPI) from outside a Security Island is allowed. All other access to controlled unclassified information must not be allowed.

(d) Each Security Island entry point must be posted with a 2 foot x 1 foot sign as follows: "SECURITY ISLAND - ACCESS ONLY BY AUTHORIZED PERSONNEL". Roll-up or over-sized door entrances must be posted with more than one sign. Signs can be posted adjacent to the door opening.

7 Aug 12

(e) Security Island entry points must be monitored or controlled. When manned, access control devices such as key locks, cipher locks or AECS card readers can be used to control access to Security Islands. If access control devices are not utilized, there must be adequate monitoring of the entry points.

(f) Security Islands must be locked when not manned.

(2) Access Control. Only persons who possess a Red or Yellow shipyard badge must be permitted unescorted entry into an UNOCCUPIED Security Island. Access by a person with a Green badge into an UNOCCUPIED Security Island is authorized if they are escorted by a person with a Red or Yellow badge who is familiar with the area and the space is sanitized to prevent the disclosure of classified and controlled unclassified information. Access to Security Islands must be controlled by:

(a) Use of an AECS, (system may include use of a Personal Identification Number (PIN)); or

(b) Use of a manual access control system controlled by guards, watchmen, receptionist or other appropriately trained and cleared personnel (who have been issued a Red badge).

(3) Access Control Privileges

(a) Unescorted access to a Security Island must be limited to those individuals who have been issued a Red or Yellow badge and have a need-to-know.

(b) Access for purposes of an immediate nature is authorized for White "escort required" or Green badged personnel provided they are:

1. U.S. citizens, under continuous escort by a Red or Yellow-badged person knowledgeable of the Security Island requirements; and

2. All classified information and controlled unclassified Reactor Plant Information can be sanitized to prevent disclosure.

e. Non-Sensitive Area (NSA) - Access control measures for NSAs shall be established by the Shipyard Commander.

7 Aug 12

f. Waterfront Areas (WFA). Physical Security Requirements:

(1) Signs must be visible and readable in all waterfront approach areas for the distance specified for all Restricted Waters for each shipyard.

(2) Waterfront signs must be illuminated from dusk to dawn with sufficient candlepower to ensure visibility and readability. Lighted signs must be posted on piers, adjacent land areas, and barges or any other ancillary craft blocking the view of land area signs.

(3) Existing signs meeting the requirements of reference (b) of this manual may be used. However, any new or replaced signs placed on the waterfront must state the following:

WARNING

U.S. GOVERNMENT PROPERTY

RESTRICTED AREA

KEEP OUT

(4) Lettering size shall be legible from a minimum distance of at least 100 feet during normal daylight and illuminated nighttime conditions.

(5) Signs must have white backgrounds with a 1/4 inch black border and letters. If the word "WARNING" is used it must be in red.

g. Consent to Search and Prohibitions. Entry into NAVSEA controlled spaces within the shipyard constitutes consent to search of person and property. All firearms, personal knives with blades greater than 2 1/2 inches long, mace, pepper spray, brass knuckles, and all illegal drugs are prohibited. Possession of alcohol is prohibited in all NAVSEA spaces, specifically including the CIA.

1-8. Events

a. General Restrictions. Based on the sensitive work and volume of NNPI, special events such as family days (authorized annually), change of commands, reenlistments, award ceremonies

7 Aug 12

and retirements will normally not be held within CIAs, CNIAs, NWA's and Security Islands.

b. Exceptions to this policy must be approved by SEA 08B and 09P, and may be requested in cases where the following conditions are met:

(1) The nature of the requested event shall have a direct positive benefit to the U.S. Navy.

(2) Appropriate security measures must be feasible to implement, and the event must be of sufficient benefit to justify the expense and impact of being conducted within a restricted area.

(3) Visit Requests/Security Plans must be submitted, via e-mail, five (5) business days prior to the date of the visit and approved by SEA 08B and 09P. The proposed visit requests must be in the following format:

(a) Requesting facility:

(b) Subject:

(c) Purpose for the visit:

(d) Justification for the visit:

(e) Dates of the visit:

(f) Proposed security plan including:

1. Approximate number of visitors, including identification of foreign nationals.

2. Areas of the shipyard which must be accessible to the participants. The security plan must identify specific buildings and structures and provide a sketch map and a brief description of the ongoing work in each building.

3. Routes of entrance/exit during the event, including transportation routes and parking.

4. A map or diagram of the accessible areas.

5. Any special security/safety measures that must be taken during the event (e.g. post, area controls, etc.).

6. Pre-inspection of and sanitization of sensitive information in accessible and adjacent areas during the event.

7. Post-event search of the accessible area(s) to ensure that no contraband materials have been left behind and all participants have exited the shipyard.

8. Planned surveillance during the event.

(g) Special Considerations (i.e. any other events of a sensitive nature taking place on the same day and time):

(h) Points of Contact (POC):

c. Escorts. Sufficient escorts must be provided to ensure control of the participants during the event. Buses or vans may be escorted with one escort per vehicle. If the event includes visits to U.S. Navy ships, the ship Commanding Officer shall accept responsibility for safety and security while on board.

d. Force Protection Conditions (FPCONs)

(1) If FPCON ALPHA has been declared, the Shipyard Commander must assess the local threat and determine if the event will proceed as scheduled.

(2) If FPCON BRAVO or higher is declared prior to or during the event, the event must be cancelled, postponed or terminated until the FPCON has been returned to less than BRAVO.

1-9. Visitors

a. General. Shipyard Commanders or Designated Officials must approve visit requests using the Joint Personnel Adjudication System (JPAS) as required by reference (a) of this manual. Visitors shall be issued a badge in accordance with references (a) and (b) of this manual. All visitors requiring access to classified material shall meet the requirements of reference (a) of this manual.

b. Foreign Nationals

(1) Foreign nationals are defined in reference (e) of this manual. Access to the CIA (when no approved Security Island Program exists) by foreign nationals must be approved by

7 Aug 12

NAVSEA 08B and 09P and meet all requirements of reference (e) of this manual. If visit coordination requests are made directly to the shipyards, the request must be immediately referred to NAVSEA 08B and 09P. Foreign nationals must be issued White, "escort required" badges and must be under continuous escort.

(2) Visits to CIAs, CNIAs, Security Islands or NWA's by foreign nationals, representatives of foreign governments, foreign commercial interest and foreign news media must be approved by NAVSEA 08B and 09P. U.S. citizen employees of foreign commercial interest that require entry into a shipyard/CIA for the performance of a valid contract may be authorized access by the Shipyard Commander or Shipyard Director of Security. However, prior to authorizing entry the authorizing official must ensure adequate security measures are affected, and as a minimum to ensure no access to classified information and NNPI. Additionally, the visitor must be under constant escort when in the CIA. In each instance where access is approved by the shipyard, written notification must be provided to NAVSEA 08B and 09P. All other representatives of foreign commercial interests must be approved by NAVSEA 08B and 09P.

(3) Access by foreign nationals to non-sensitive areas must be controlled by local procedures. Foreign national crew members of U.S. Navy ships are subject to the UCMJ, but are not granted security clearances. These crew members shall not be granted access to NNPI. They may have access to the CIA, upon approval of the Shipyard Commander, and must be issued green badges for this purpose. Foreign national crew members (i.e. Personnel Exchange Officers (PEP)), who are not subject to the UCMJ, shall not be allowed access to the CIA and must be disembarked prior to arrival at the CIA.

c. News Media. Access to the CIA by news media personnel is prohibited, except as specifically authorized by NAVSEA 08B and 09P. News media access to the non-industrial areas of the shipyard, such as the Officer's Club, Chief Petty Officer's Club, ball parks and recreation areas may be approved by Shipyard Commander provided such access does not permit photographic coverage which would reveal any part of the CIA. Additionally, such media presence may not be used for political purposes (which could indicate U.S. Navy endorsement of a politician or issues he/she supports) or for official coverage of shipyard mission issues. To insure headquarters knowledge of potential public affairs issues, the shipyard must notify NAVSEA

7 Aug 12

08B, 09P and 00D of all media access to the non-CIA for any issues relating to the shipyard mission.

d. Congressional Visits

(1) Request for visits with prior notice by Members of the United States Congress, their aides, and committee staff members to the CIA must be handled expeditiously. All visits require approval of both the Shipyard Director of Security and NAVSEA 08B and 09P. The following guidelines must be used in handling unannounced visits:

(a) U.S. Members of Congress. Inform NAVSEA 08B and 09P as soon as possible and provide access. Members of Congress do not require security clearance eligibility and will be issued Red SACB.

(b) U.S. Congressional Staff. Verification of security clearances is required before access is granted to classified material or classified areas. Access to the CIA may be granted without a clearance check if staff members are under continuous escort, no access to classified information is provided and staff members are accompanying the Congressman. Inform NAVSEA 08B and 09P as soon as possible of these visits.

(c) Visitors with U.S. Members of Congress. Other than news media or documentary film teams, visitors with U.S. Members of Congress shall be treated as official visitors, requiring verification of security clearance and NAVSEA 08B and 09P approval for the visit.

(d) News Media and/or Documentary Film Teams, Accompanying U.S. Members of Congress. If the purpose of the elected official's visit is to conduct campaign activity and have the visit recorded, the official should be cordially advised that Department of the Navy (DoN) public affairs policy prohibits the use of the facility for such activity. If it is the elected official's intention to interact with the facilities' employees or to use the facility as an on camera backdrop, the official must be advised that this type of activity must be performed outside the facility.

e. Visits by Local, Regional and State Government Officials. These officials may have access to non-sensitive areas of the shipyard upon approval of the Shipyard Commander. Access to the CIA must be approved by NAVSEA 08B and 09P. An exception to this policy is made for visits to the Puget Sound

7 Aug 12

Shipyard Commander's office which is located within the CIA. Such visits may be authorized by the Shipyard Commander.

1-10. Photography and Recording Devices

a. Any device or equipment capable of recording, transmitting or exporting photographic images or audible information of any kind is prohibited when classified information, U-NNPI or other CUI defined by reference (f), is exposed unless specifically authorized in writing as described below. Voice recording is prohibited in all NAVSEA spaces unless specifically authorized by the Shipyard Director of Security.

b. Lock boxes are recommended as one of the options to temporarily secure such devices when classified information, U-NNPI or other CUI are exposed.

c. This requirement does not apply to printers, copiers, fax machines, US government controlled Communications Security (COMSEC) material and portable electronic devices subject to the security policies enforced by the Navy's enterprise wide Information Technology contracts (e.g., NMCI issued laptop computers and Blackberries).

d. Officially authorized photographic images and audible recordings of naval nuclear-powered ships and related nuclear support facilities shall be classified and appropriately marked according to the information revealed therein. Photographs containing NNPI shall be marked in accordance with references (g) and (h) of this manual. All other photographs must be classified and marked according to content until approved for public release by NAVSEA 08B, 09P and 00D in accordance with reference (i) unless covered under subsection 1-10. g. below.

e. Unofficial photography is prohibited within the CIA of the shipyard. Unofficial photography of the CIA from the outer perimeter gate/fence of the CIA is also prohibited.

f. Unofficial photography is approved for occupants of shipyard housing areas, but, only in the immediate housing area.

g. All images of the CIA are considered at least CUI or FOUO and must be authorized by the Shipyard Director of Security. Official photographers must possess valid camera permits issued by the shipyard security office. Shipyard Security Office must review and release photographs to other DOD

7 Aug 12

activities and to contractors who have legitimate requirements and the need-to-know. Release of photographs to any other party, taken of or within the CIA, requires NAVSEA 08B and 09P approval.

h. Local release authority is granted for specific types of official images/recordings taken within the CIA. Examples include images/recordings of employees or U.S. Navy personnel participating in award ceremonies, local celebrations, partnerships with local governments, and photographs of non-sensitive subjects where no sensitive information is revealed in any part. Examples of areas within the CIA where local approval authority may be used are office spaces, outside of buildings, topside of vessels alongside piers or topside on vessels in dry-docks where no classified information or CUI is revealed in any part.

i. There is no local release authority for photography involving CNIAs, NWAs, or Security Islands. Local procedures must be written to include procedures for requesting approval to take photographs and the actions required to approve the photography for public release.

j. Prior to being released to the public, all photographs must be reviewed at a minimum, by the cognizant shop or code, Safety Officer, Shipyard Director of Security, NNPICO, Information Security Manager, and Public Affairs Officer. These reviews must be documented and maintained on file for a period of two years after public release.

k. Local reviews shall preclude public release of classified information, CUI, occupational safety and health issues, poor work practices, inappropriate signs (i.e. RADCON signs), potential security vulnerabilities and any other photographs considered politically sensitive or convey an adverse liability to the Navy, NAVSEA or the shipyard. Photographs of this nature must be submitted to NAVSEA 08B and 09P for review. Under no circumstances may telephone approval be given for photographs or associated printed material.

l. Photography of areas other than the CIA, including other posted restricted areas, must be reviewed and approved by the Shipyard Public Affairs Officer, the Shipyard Director of Security, the NNPICO, and when appropriate, safety and radiological control directors prior to public release. This restriction also applies to federal, state, and local agencies.

7 Aug 12

If there is a question about the sensitivity of the photographs, they must be forwarded to NAVSEA 08B and 09P for review.

m. Members of ship's force who are assigned to living quarters on-board ships inside the CIA may transit directly between non-CIA areas and the living barge / ship while carrying personal camera cell phones, laptops (including those with web cameras), and similar Personal Electronic Devices (PEDS) with cameras. This is not authorized for sailors who have other housing or for the Duty Section on board the ship/barge. The applicable ship is responsible for maintaining accountability using the following controls:

(1) Assume responsibility for the security process and train the sailors on these control requirements.

(2) Register, track and label (or issue passes) for all relevant devices.

(3) Ensure the devices are powered off and carried so they are not openly visible during transit between the non-CIA areas and the living barge/ship. The devices may not be taken anywhere else in the CIA such as lunch rooms, snack bars, smoking gazebos, etc.

(4) Ensure sailors sign a "page 13" entry acknowledging all restrictions and potential consequences including administrative and disciplinary actions if they violate these restrictions.

(5) Submit an updated list of personnel authorized to carry these devices (including the type of device) every two weeks to the Shipyard Director of Security.

1-11. Disciplinary Action

a. Failure to comply with the requirements of this chapter are subject to the following disciplinary actions in accordance with reference (j).

(1) First offense: reprimand to removal;

(2) Second offense: 5-day suspension to removal;

(3) Third offense: 10-day suspension to removal.

7 Aug 12

b. Supervisors are responsible for initiating appropriate administrative and disciplinary action.

7 Aug 12

CHAPTER 2

FIELD ACTIVITIES OTHER THAN NAVAL SHIPYARDS

2-1. Scope. This chapter updates requirements for physical security, access, and movement control for all NAVSEA Field Activities other than Naval Shipyards. NAVSEA Field Activities operating in an area under the jurisdiction of NAVSEA 08 shall follow the guidance in Chapter 1 of this manual where applicable.

2-2. Standard Access Control. Commanding Officers (COs) and Officers In Charge (OICs) shall consider local threats, vulnerabilities, and their mission then ensure appropriate security measures are in place to meet the access control requirements (including visitors) of references (a), (b) and (j) of this manual.

2-3. Visitors

a. Commanding Officers, OICs or Designated Officials must approve visit requests to their activities using the Joint Personnel Adjudication System (JPAS) as required by reference (a) of this manual. Visitors shall be issued a badge in accordance with references (a) and (b) of this manual. All visitors requiring access to classified material shall meet the requirements of reference (a) of this manual. Categories of visitors include but are not limited to:

- (1) Dependents
- (2) Civil service retirees
- (3) Representatives of local and state government agencies, business officials, or civic organizations
- (4) School teachers and students
- (5) Reservists (Access to NNPI for active duty training shall be handled in accordance with reference (c) of this manual)
- (6) Official military or civilian visitors
- (7) U.S. citizens who are authorized contractor personnel

7 Aug 12

(8) U.S. Navy crew members, including foreign nationals of new construction ships within a private shipyard complex

(9) U.S. citizens for employment purposes.

(10) News media.

b. Commanding Officers of SUPSHIP commands co-located at contractor facilities, may approve visits to ships at the contractor facility when requested by either the Commanding Officer or Prospective Commanding Officer (PCO) of the ship by following the requirements of this manual. Continuous escort is required for these visitors.

c. Foreign Nationals (FN)

(1) Foreign Nationals (FN) are defined in reference (e) of this manual.

(2) All FN visitors requesting access to a NAVSEA facility they are not assigned by the Navy International Program Office (Navy IPO):

(a) May be authorized access only during normal business hours;

(b) Must be issued "escort required" badges; and

(c) Must be under continuous escort.

(3) Commanding officers may approve visits by FN if the visit involves access only to information approved for public release.

(4) All other visits by FN must be requested as a Foreign Visit Request (FVR) in the Foreign Visit System (FVS).

(5) Commanding officers may approve access by U.S. citizen employees of foreign commercial interests for the performance of a valid contract by following the requirements of this manual. Prior to authorizing access, the commanding officer must ensure adequate security measures are fully developed and implemented to prevent access to classified information or any type of Controlled Unclassified Information (CUI) defined in reference (f) of this manual.

7 Aug 12

(6) Access by FN to non-sensitive areas must be controlled by local procedures. FN crew members of U.S. Navy ships are normally subject to the UCMJ, but are not granted security clearances. These crew members shall not be granted access to CUI unless approved by the commanding officer.

(7) FN personnel, such as Foreign Liaison Officers (FLO), Personnel Exchange Program Officers (PEPO), Engineer and Scientist Exchange Program (ESEP) and Cooperative Program Personnel (CPP), who have been accredited/assigned by the Navy IPO and are resident at a NAVSEA field activity must be issued a NAVSEA FN picture badge with a brown background.

(8) FN who have a NAVSEA brown background picture badge must be granted unescorted access during normal business hours to all common areas, including access routes to their assigned work area(s), restrooms, ATMs, cafeterias, vending machines, copier rooms, auditoriums, training rooms, corridors, and light courts. If these FN require access to other areas, including program offices outside their assigned area(s), the cognizant Contact Officer must acquire the approval of the office to be visited.

(9) FN are not authorized to serve as escorts at anytime.

2-4. Photography and Recording Devices

a. Any device or equipment capable of recording, transmitting or exporting photographic images or audible information of any kind is prohibited when classified information, U-NNPI or other CUI defined in reference (f) is exposed unless specifically authorized in writing as described below. Voice recording is prohibited in all NAVSEA spaces unless specifically authorized by the Commanding Officer.

(1) Lock boxes are recommended as one of the options to temporarily secure such devices when classified information, U-NNPI or CUI is exposed.

(2) This requirement does not apply to printers, copiers, fax machines, US government controlled Communications Security (COMSEC) material and electronic equipment required in support of official surface - subsurface testing environments.

(3) This requirement does not apply to portable electronic devices subject to the security policies enforced by

7 Aug 12

the Navy's enterprise wide Information Technology contracts (e.g., NMCI issued laptop computers and Blackberries).

b. Photographic images and audible recordings shall be appropriately classified and marked according to the information revealed therein and must be approved for public release in accordance with reference (i) of this manual. Photographic images and recordings containing NNPI shall be marked in accordance with references (g) and (h) of this manual.

c. Local release authority is granted for specific types of photographic images and audible recordings. Examples include images/recordings of employees or U.S. Navy personnel participating in award ceremonies, local celebrations, partnerships with local governments, and photographs of non-sensitive subjects where no sensitive information is revealed in any way. Examples of areas where local approval authority may be used are sanitized office spaces, outside of buildings, topside of vessels alongside piers or topside on vessels in dry-docks where no classified information or CUI is revealed in any way.

d. Commanding Officers, Supervisors of Shipbuilding, Conversion and Repair (SUPSHIPS), and Officers in Charge (OIC) may authorize official photography or audible recordings within their respective commands by issuing a written command permit approved by the local command Security Director/Officer/Manager.

(1) Each command must establish a permit approval process or procedure.

(2) While granting permit approval, Command Security Directors/Officers/Managers must:

(a) Ensure each permit applicant acknowledges in writing their responsibility to prevent any accidental imaging/recording/exporting of classified information or CUI and each image/recording is subject to the standard clearance process for public release in accordance with reference (i);

(b) Ensure each permit applicant acknowledge in writing all restrictions and potential consequences including administrative and disciplinary actions if they violate these restrictions; and

7 Aug 12

(c) Keep written records of each applicant's acknowledgements above for two years after the approved permit is no longer valid.

(3) The local security office may issue permits to NAVSEA personnel who will function as official command photographers for renewable two-year periods.

(4) The local security office may issue permits to NAVSEA personnel for specific internal events such as awards, reenlistments, retirements and promotions etc.

(5) Prior to uncontrolled or public release, all images/recordings must be endorsed at a minimum, by the local cognizant shop or office code, Operations Security (OPSEC) Officer, Safety Officer, Security Director/Officer/Manager, Information Assurance Manager, and Public Affairs Officer.

(6) Local reviews shall preclude public release of classified information, CUI, occupational safety and health issues, poor work practices, inappropriate signs (i.e. RADCON signs), potential security vulnerabilities and any other images/recordings considered politically sensitive or convey an adverse liability to the Navy, NAVSEA or the command. Images/recordings of this nature must be submitted to NAVSEA 09P for review. Under no circumstances may telephone approval be given for images or associated printed material.

(7) Members of ship's force who are assigned to living quarters on-board ships/barges docked at NAVSEA facilities may transit directly to and from the living barge/ship while carrying personal camera cell phones, laptops (including those with web cameras), and similar Personal Electronic Devices (PEDS) with cameras. This is not authorized for sailors who have other housing. The applicable ship is responsible for maintaining accountability using the following controls:

(a) Assume responsibility for the security process and train the sailors on these control requirements.

(b) Register, track and label (or issue passes) for all relevant devices.

(c) Ensure the devices are powered off and carried so they are not openly visible during transit between other areas and the living barge/ship. The devices may not be taken anywhere else on NAVSEA facilities.

7 Aug 12

(d) Ensure sailors sign a "page 13" entry acknowledging all restrictions and potential consequences including administrative and disciplinary actions if they violate these restrictions.

2-5. Disciplinary Action

a. Failure to comply with the requirements of this chapter are subject to the following disciplinary actions in accordance with reference (j).

- (1) First offense: reprimand to removal;
- (2) Second offense: 5-day suspension to removal;
- (3) Third offense: 10-day suspension to removal.

b. Supervisors are responsible for initiating appropriate administrative and disciplinary action.

7 Aug 12

CHAPTER 3

HEADQUARTERS

3-1. Scope. This chapter updates requirements for physical security, access and movement control at NAVSEA buildings located at the Washington Navy Yard (NAVSEA HQ).

3-2. Risk Mitigation. The open architecture of NAVSEA HQ combined with the prevalent access to classified information and the current threat environment create a significant vulnerability to inadvertent and unauthorized disclosure of classified and Controlled Unclassified Information (CUI) defined in reference (f) of this manual. To mitigate this risk, NAVSEA HQ is designated as a Level II Restricted Area in accordance with reference (b) of this manual. Because of the potential to adversely affect national security, no person shall be given unescorted access to NAVSEA HQ without a favorable personnel security determination in accordance with references (a) and (j) of this manual.

3-3. Standard Access Control

a. All persons entering NAVSEA HQ spaces:

(1) Shall comply with the directions and orders of the on-site uniformed security force and the terms of this manual;

(2) Shall adhere to the access control requirements of references (a), (b) and (j) of this manual;

(3) Shall comply with the prohibited items guidance in section 3-11 of this manual;

(4) May be granted unescorted access during normal working hours if they are listed in the Joint Personnel Adjudication System (JPAS) with current security clearance eligibility;

(5) May be granted access only with an escort if they do not have current security clearance eligibility or cannot be located in JPAS; and

(6) Are subject to search.

7 Aug 12

b. NAVSEA HQ and Common Access Card (CAC) Badges:

(1) Are issued to facilitate access into NAVSEA HQ spaces.

(2) Can be encoded to allow unlimited unescorted access following the requirements of Section 3-4 below.

(3) Must be displayed above the waist with the photograph clearly displayed at all times while within NAVSEA spaces.

(4) Should not be worn in a visible manner when outside NAVSEA HQ to preclude unauthorized duplication and potential targeting of employees.

(5) Are the property of the federal government and must be returned to the Office of Security Programs and Continuity Planning, Security Operations Division (SEA09P1) when they are no longer needed, expired, or in the event access privileges are revoked.

c. NAVSEA Field Activity/Virtual SYSCOM Badges: Government and active military badges from NAVSEA field activities and those of the virtual SYSCOMs (e.g., SPAWAR, NAVAIR, NAVSUP, etc.), will be accepted for unescorted access to NAVSEA spaces other than properly designated Restricted Areas during normal business hours.

d. Lost or Missing Badges:

(1) Must be reported to the NAVSEA Visitor Control Center (VCC) and/or SEA 09P1 immediately and

(2) Can be replaced at the VCC after the affected employee fills out NAVSEA Form 5510/16.

e. The Visitor Control Center (VCC):

(1) Is located in the main lobby of building 197;

(2) Is operated during the hours of 0630-1630 Monday through Friday, (excluding federal holidays); and

(3) Issues NAVSEA picture badges by appointment from 0900-1100, Monday through Friday.

7 Aug 12

3-4. Unescorted Access

a. NAVSEA (including field activity and affiliated Program Executive Office) employees, other government personnel and contractors requesting unescorted access to NAVSEA HQ, must:

(1) Be a U.S. citizen, with a favorable personnel security determination as required by references (a) and (j) of this manual; and

(2) Be endorsed by the cognizant sponsoring/requesting NAVSEA organization and approved by the Office of Security Programs and Continuity Planning (SEA 09P).

b. The Process for Unescorted Access:

(1) Prior to unescorted access approval, the sponsoring/requesting NAVSEA Administrative Officer (AO) must enter the personal information into Total Workforce Management Services (TWMS); then

(2) The sponsoring/requesting NAVSEA organization or the Contracting Officer's Representative (COR) must complete NAVSEA Form 5510/9 (NAVSEA WNY Badge Request Form), and acquire the signature of the NAVSEA authorizing official/ NAVSEA COR and/or cognizant AO; then

(3) The person seeking unescorted access must take the completed 5510/9 form to the VCC to complete the process for their picture badge.

3-5. Visitors

a. Visit requests must be submitted using the Joint Personnel Adjudication System (JPAS) as required by reference (a). Visitors shall be issued a badge in accordance with references (a) and (b) of this manual. All visitors requiring access to classified material shall meet the requirements of reference (a) of this manual. Categories of visitors include but are not limited to:

(1) Dependents

(2) Civil service retirees

(3) Representatives of local and state government agencies, business officials, or civic organizations

(4) School teachers and students

(5) Reservists (Access to NNPI for active duty training shall be handled in accordance with reference (c) of this manual.)

(6) Official military or civilian visitors

(7) U.S. citizens who are authorized contractor personnel

(8) U.S. Navy crew members, including foreign nationals of new construction ships within a private shipyard complex

(9) U.S. citizens for employment purposes

(10) News media

b. Foreign Nationals (FN)

(1) FN are defined in reference (e) of this manual.

(2) All FN visitors not assigned to NAVSEA HQ by the Navy IPO:

(a) May be authorized access only during normal business hours;

(b) Must be issued "escort required" badges; and

(c) Must be under continuous escort.

(3) Senior officials at the 06 or GS-15 level may approve visits by FN if the visit involves access only to information approved for public disclosure.

(4) All other visits by FN must be requested as a Foreign Visit Request (FVR) in the Foreign Visit System (FVS).

(5) Senior officials at the 06 or GS-15 level may approve access by U.S. citizen employees of foreign commercial interests for the performance of a valid contract by following the requirements of this manual. Prior to authorizing access, the senior official must ensure adequate security measures are fully developed and implemented to prevent access to classified information or any type of Controlled Unclassified Information (CUI) defined in reference (f) of this manual.

7 Aug 12

(6) Access by FN to non-sensitive areas may be approved by senior officials at the O6 or GS-15 level. FN crew members of U.S. Navy ships are normally subject to the UCMJ, but are not granted security clearances. These crew members shall not be granted access to CUI unless approved by the commanding officer.

(7) FN, such as Foreign Liaison Officers (FLO), Personnel Exchange Program Officers (PEPO), Engineer and Scientist Exchange Program (ESEP) and Cooperative Program Personnel (CPP), who have been accredited by the Navy International Program Office (Navy IPO) must be issued a NAVSEA FN picture badge with a brown background. The Office of Security Programs and Continuity Planning, Tech Protection and International Security Division (SEA 09P5) is responsible for issuing the necessary paperwork for a NAVSEA FN badge.

(8) FN who have a NAVSEA brown background picture badge must be granted unescorted access during normal business hours to all common areas, including access routes to their assigned work area(s), restrooms, ATMs, cafeterias, vending machines, copier rooms, auditoriums, training rooms, corridors, and light courts. If these FN require access to other areas, including program offices outside their assigned area(s), the cognizant Contact Officer must acquire the approval of the office to be visited and SEA 09P5.

(9) FN are not authorized to serve as escorts at anytime.

c. Washington Navy Yard (WNY) Tenants. Other WNY government tenant employees are authorized access to the Building 197 cafeteria and ATM (0630-1430) Monday through Friday, (except federal holidays) by obtaining a standard cafeteria badge from the uniformed guard at the main entrance to building 197.

3-6. Escorts

a. Only NAVSEA HQ on-site resident employees, contractors and other U.S. government personnel, are authorized to serve as escorts.

b. Escorts are responsible for their assigned visitors throughout the duration of the visit and may escort a maximum of six people at any given time.

7 Aug 12

c. All escorts must ensure classified information and CUI are protected from inadvertent disclosure from audible or written communication at all times. This includes ensuring co-workers turn-over, cover or store all classified and CUI while the visitor is present. Pre-coordination with co-workers is recommended.

d. When escorting into Restricted Areas (RA), escorts must announce, "un-cleared persons are entering the RA", to ensure all personnel working in the RA are aware of this fact.

e. Escorts must meet their visitors at the Visitor Control Center at the main entrance of building 197 and ensure they surrender their visitors badge and depart at the same location.

3-7. Building Support Personnel (BSP)

a. BSP:

(1) Are defined as contractor maintenance, janitorial and cafeteria personnel assigned to work at NAVSEA HQ;

(2) Must be U.S. citizens or be in possession of a valid Green Card issued by the U.S. State Department;

(3) Must comply with the guidance of reference (k) before being authorized unescorted access to the cafeteria or common areas inside NAVSEA HQ; and

(4) Must be issued a standard yellow badge when meeting the criteria above and unescorted access is desired. Yellow badges must be visible above the waist.

b. Cafeteria personnel are authorized unescorted access to the cafeteria and the immediate surrounding area from 0500-1600 on normal weekdays (excluding federal holidays).

c. Janitorial personnel are authorized unescorted access to common areas from 0530-1600 on normal weekdays (excluding federal holidays). Common areas include ingress and egress areas of the buildings assigned, restrooms, ATM machine, cafeteria, vending machines, copier rooms, auditorium, training rooms, corridors, elevators, stairways and light courts. When they need access to departmental areas, they shall be under continuous escort or observation.

7 Aug 12

d. Maintenance personnel are authorized unescorted access the common areas and departmental areas as described above in section 3-7 c. from 0630-1600 on normal weekdays (excluding federal holidays).

e. Non-emergency BSP access for anytime other than 0500-1600 on normal weekdays requires SEA 09P1 written approval and must be requested in writing two business days in advance. The request must include:

- (1) The date(s), time and type of work;
- (2) The building and room of the work;
- (3) The name of the company performing the work;
- (4) A list of the individuals performing the work including their full name, social security number, date and place of birth, and citizenship; and
- (5) The names and office codes of those who will serve as their escorts until the BSP exit the building.

f. Emergency after-hour BSP access must be coordinated through the NAVSEA Facilities Management office and the NAVSEA Duty Officer who in turn must notify SEA 09P1 and direct the building uniformed guard force to escort the incoming BSP during the emergency.

3-8. Media Event Access

a. All media events must involve only public domain information and must be conducted only in common areas.

b. Access for media events must be approved by the Office of Corporate Communications (SEA 00D), and SEA 09P1, and must be requested two business days in advance. The request must provide:

- (1) The date(s), time and subject of the event;
- (2) The building and room of the event;
- (3) The name of the media companies expected at the event;

7 Aug 12

(4) A list of the media personnel to be present for the event including their full name, social security number, date and place of birth, and citizenship;

(5) A list of camera equipment to be used; and

(6) The names and office codes of those who will follow the escort requirements of section 3-6 of this manual.

c. All photographic and recording devices used for media events must have a pass issued by SEA 00D in compliance with section 3-12 of this manual.

3-9. Special Event Access. Access for special events, including large conferences, retirements, promotion ceremonies, training events and symposiums must be approved by SEA 09P1. NAVSEA offices sponsoring special events or other group activities must provide SEA 09P1 with a list of the names of those from outside of NAVSEA who are expected to attend. The list must be submitted two business days prior to the scheduled event.

3-10. Classified Events. If the special event involves classified information, the sponsoring office must consult with the Office of Security Programs and Continuity Planning, Information and Industrial Security Division (SEA 09P3) and must appoint a NAVSEA government employee to serve as the security coordinator for the event.

3-11. Prohibited Items

a. Weapons or other dangerous materials.

b. Alcoholic Beverages.

c. Items described in section 3-12 below.

d. Other items, the possession of which is prohibited by Federal, state or municipal law, Department of Defense or Department of Navy instruction, directive and policies.

3-12. Photography and Recording Devices

a. Any device or equipment capable of recording, transmitting or exporting photographic images or audible information of any kind is prohibited when classified information, U-NNPI or other CUI defined in reference (f) is exposed unless specifically authorized as described below.

(1) Lock boxes are recommended as one of the options to temporarily secure such devices when classified information, U-NNPI or other CUI are exposed.

(2) This requirement does not apply to printers, copiers, fax machines, US government controlled Communications Security (COMSEC) material and portable electronic devices subject to the security policies enforced by the Navy's enterprise wide Information Technology contracts (e.g., NMCI issued laptop computers and Blackberries).

(3) Photographic images and audible recordings are authorized in the following areas when neither classified information nor CUI are present or revealed in any way:

(a) Anywhere outside of NAVSEA HQ buildings;

(b) In the following areas during NAVSEA approved ceremonies and special events:

1. The second floor atrium of building 197;

2. The cafeteria and the area immediately adjacent to the cafeteria on the first floor of building 197;

3. The area between the employee entrance and the elevators on the first floor of building 197;

(c) Additional areas approved in writing by SEA 09P1 on a case by case basis.

(4) Additional exemptions to this requirement must be approved in writing in advance by both SEA 09P1 and SEA 00I1 using reference (1).

b. Photographic images and audible recordings shall be appropriately classified and marked according to the information revealed therein and must be approved for public release in accordance with reference (i) of this manual. Photographic

7 Aug 12

images and recordings containing NNPI shall be marked in accordance with references (g) and (h) of this manual.

c. Anyone other than approved media personnel and official command photographers who wishes to take photographic images or audible recordings outside of the areas named above, must acquire a NAVSEA Photographic and Audible Recording Device Permit (reference (1)) approved by SEA 09P1. Areas where exposure to classified information or CUI is possible must be sanitized by the host office prior to allowing photographic images or audible recordings to be taken.

(1) While approving these permits, SEA 09P1 must ensure each permit applicant acknowledges the following in writing using reference (1):

(a) Their responsibility to prevent any imaging/recording/exporting of classified information or CUI;

(b) All images/recordings are subject to the standard clearance process for public release in accordance with reference (i); and

(c) All restrictions and potential consequences including administrative and disciplinary actions if these restrictions are violated.

(2) SEA 09P1 must keep written records of each applicant's acknowledgements above for two years after the approved permit is no longer valid.

d. Official command photographers and media personnel must acquire a Photographic and Audible Recording Device Permit (reference (1)) approved by SEA 00D.

(1) While approving these permits, SEA 00D must:

(a) Ensure official command photographers are NAVSEA government employees who acknowledge the following in writing using reference (1):

1. Understand their responsibilities to protect classified information and CUI in accordance with references (d) and (f) of this manual; and

7 Aug 12

2. Understand all restrictions and potential consequences including administrative and disciplinary actions if these restrictions are violated.

(b) Ensure media personnel understand the limitations of their authorization in accordance with section 3-8 of this manual.

(c) Keep written records of the permits for two years after the approved permit is no longer valid.

3-13. Disciplinary Action

a. Failure to comply with the requirements of this chapter are subject to the following disciplinary actions in accordance with reference (j).

(1) First offense: reprimand to removal;

(2) Second offense: 5-day suspension to removal;

(3) Third offense: 10-day suspension to removal.

b. Supervisors are responsible for initiating appropriate administrative and disciplinary action.

7 Aug 12

CHAPTER 4

**FOREIGN NATIONAL
ACCESS TO NAVAL VESSELS**

4-1. Scope. This chapter updates requirements for physical security, access and movement control of foreign nationals defined by reference (e) of this manual on all U.S. Navy vessels under design, construction, conversion, repair or overhaul. This includes all associated work for these vessels but does not include vessels under the jurisdiction of SEA 08. All such vessels or any component thereof under the jurisdiction of NAVSEA 08 shall follow the guidance in Chapter 1 of this manual where applicable.

4-2. Standard Access Control

a. Unless approved as described below, foreign nationals shall not be allowed on the following premises:

(1) Aboard U.S. Navy vessels under construction, conversion, repair, or overhaul; and

(2) At the design, construction, conversion, repair and overhaul sites and facilities, including but not necessarily limited to docks, ways, dry-docks and piers.

b. Foreign national access to the above must be approved in writing by the cognizant Commanding Officer (CO), Officer in Charge (OIC), Supervisor of Shipbuilding, Conversion and Repair (SUPSHIP) or their designated representative in consultation with the NAVSEA Office of Security Programs and Continuity Planning (SEA 09P) and with the endorsement of:

(1) The local Security Manager/Officer; and

(2) The cognizant Contract Administration Office (CAO).

c. Foreign nationals shall not be eligible for access to the above areas until:

(1) The officials named in Section 4-2. b. of this manual concur such access is in the best interest of the United States after consulting the most current Defense Counterintelligence Information System (DCIIS) webpage titled

7 Aug 12

"Worldwide Threat Levels, to U.S. Navy Vessels" @ <http://dciis.dia.smil.mil/threat/worldwide.html>; and

(2) The contractor desiring to employ the foreign national(s) develops an Access Control Plan (ACP) meeting the requirements of enclosure (1) approved by both the local Security Manager/Officer and CAO.

d. A contractor's compliance with an approved ACP must be monitored and verified on a periodic basis by the local Security Manager/Officer and CAO. Noncompliance serves to cancel the authorization previously granted, and the contractor would then be precluded from the continued use of foreign nationals on that contract until such time as compliance with an approved ACP is demonstrated. Continued use of foreign national contractor employees without an approved ACP or when a previous authorization has been cancelled, is considered a security violation.

e. When it is in the best interest of the United States, the previous authorization for access of foreign national contractor employees may be cancelled by the NAVSEA Director of Security Programs and Continuity Planning (SEA 09P) or the cognizant NAVSEA directorate or echelon III (i.e. SEA 04 or CNRMC).

4-3. Application

a. The requirements of this manual shall be invoked via the clause in enclosure (1) in all new Navy contracts, agreements, and job orders involving design, construction, conversion, repair and overhaul of Navy vessels and all work associated therewith under the cognizance of NAVSEA.

b. An ACP is valid only for the specific contract or agreement it is originally intended. An ACP which is approved for a Master Ship Repair Agreement (MSRA), an Agreement for Boat Repair (ABR) or a Basic Ordering Agreement (BOA) is valid and applicable to all job orders awarded under the respective agreement.

4-4. Action

a. The NAVSEA 02 Contracts Directorate shall include the clause in enclosure (1) of this manual invoking the requirements of this manual in all new NAVSEA headquarters solicitations for the design, construction, conversion, repair, or overhaul of

7 Aug 12

naval vessels as applicable. Enclosure (2) must also be included in all new applicable solicitation packages.

b. The NAVSEA Program Manager's Data Manager must list the ACP as a Contract Data Requirements List (CDRL) item.

c. The cognizant CO, OIC or SUPSHIP must enforce the regulations concerning access by foreign national contractor employees.

d. Contractors entering into a MSRA, ABR or BOA who intend to hire foreign nationals must submit an ACP meeting the requirements of enclosure (1) subject to approval by the local Security Manager/Officer and CAO.

e. Local Security Managers/Officers must:

(1) Establish and maintain guidelines indicating criteria for an acceptable ACP;

(2) Review, approve or disapprove all contractor access lists for work on board Navy vessels;

(3) Transmit the access lists to the vessels and the applicable shipyard or activity access control or security office;

(4) Endorse foreign national access as described in section 4-2 of this manual; and

(5) Approve ACPs along with the local CAO as described in section 4-2 of this manual.

f. The cognizant Contract Administration Office (CAO) must:

(1) Include enclosures (1) and (2) of this manual and list the ACP as a CDRL item in all locally issued ship work or job order contracts and solicitations when applicable;

(2) Endorse foreign national access as described in section 4-2 of this manual;

(3) Approve ACPs along with the local Security Manager/Officer as described in section 4-2 of this manual;

(4) Advise the contractor of the adequacy of its ACP;

7 Aug 12

(5) Develop a procedure to monitor and verify contractor compliance with its ACP;

(6) Maintain on file all data necessary to monitor and verify contractor compliance with the requirements of enclosure (1) including:

(a) A copy of each approved ACP and data reflecting the number, nationality and positions held by foreign national employees; and

(b) The following data on foreign nationals from countries referenced on the above DCIIS webpage:

1. Name;
2. Place of birth;
3. Citizenship (if different from place of birth;
4. Date of entry to U.S.;
5. Extenuating circumstances (if any) concerning immigration to the U.S;
6. The number of years employed by the contractor;
7. Their position; and
8. Any stated intent concerning U.S. citizenship.

(7) Report to NAVSEA 02 on the oversight of contractor performance to ensure the contractor's compliance with the provisions of its approved ACP.

g. Contractors. When foreign national contractor employees are desired for the accomplishment of ship work under a specific agreement or contract, contractors must:

(1) Develop an ACP and submit it to the cognizant local Security Manager/Officer and CAO for approval in accordance with enclosure (1) of this manual; and

7 Aug 12

(2) Submit enclosure (2) of this manual to the local CAO showing intent to use foreign national employees with an approved ACP or action to develop an ACP.

4-5. Disciplinary Action

a. Failure to comply with the requirements of this chapter are subject to the following disciplinary actions in accordance with reference (j).

(1) First offense: reprimand to removal;

(2) Second offense: 5-day suspension to removal;

(3) Third offense: 10-day suspension to removal.

b. Supervisors are responsible for initiating appropriate administrative and disciplinary action.

7 Aug 12

FOREIGN NATIONAL ACCESS TO NAVAL VESSELS CLAUSE

1. No person known to be a foreign national defined by reference (e) of this manual shall be eligible for access to naval vessels, work sites and adjacent areas when said vessels are under construction, conversion, overhaul, or repair, except upon a finding by NAVSEA or his designated representative that such access should be permitted in the best interest of the United States. The contractor shall establish procedures to comply with the requirements of this clause and the NAVSEA M-5510.2 in effect on the date of this contract or agreement.

2. If the contractor desires to employ foreign nationals in the performance of work under this contract or agreement that requires access as specified in paragraph (a) to this clause, approval must be obtained prior to access for each contract or agreement where such access is desired. To request such approval, the contractor shall submit to the cognizant Contract Administration Office (CAO), an Access Control Plan (ACP) which shall contain as a minimum, the following information:

a. A badge or pass oriented identification, access, and movement control system for foreign national employees with the badge or pass to be worn or displayed on outer garments at all times while on the contractor's facilities and when performing work aboard ship.

(1) Badges must be of such design and appearance that permits easy recognition to facilitate quick and positive identification.

(2) Access authorization and limitations for the bearer must be clearly established and in accordance with applicable security regulations and instructions.

(3) A control system, which provides rigid accountability procedures for handling lost, damaged, forgotten, and no longer required badges, must be established.

(4) A badge or pass check must be performed at all points of entry to the contractor's facilities or by a site supervisor for work performed on vessels outside of the contractor's plant.

7 Aug 12

b. The contractor's plan for ascertaining citizenship and for screening employees for security risk.

c. Data reflecting the number, nationality, and positions held by foreign national employees, including procedures to update data as foreign national employee data changes, and pass to the cognizant CAO.

d. The contractor's plan for ensuring subcontractor compliance with the provisions of the contractor's ACP.

e. These conditions and controls are intended to serve as guidelines representing the minimum requirements of an acceptable ACP. They are not meant to restrict the contractor in any way from imposing additional controls necessary to tailor these requirements to a specific facility.

3. To request approval for foreign national employees, the contractor shall include in their ACP the following employee data: name, place of birth, citizenship (if different from place of birth), date of entry to U.S., extenuating circumstances (if any) concerning immigration to U.S., number of years employed by the contractor, position, and stated intent concerning U.S. citizenship. The local NAVSEA commanding officer will make individual determinations of desirability of access for the above group. Until written NAVSEA approval is received, the contractor must deny access to vessels for employees who are foreign nationals.

4. An ACP which has been approved for specific Master Ship Repair Agreement (MSRA) or Agreement for Boat Repair (ABR) or Basic Ordering Agreement (BOA), is valid and applicable to all job orders awarded under that agreement.

5. The contractor shall fully comply with approved ACPs. Noncompliance by the contractor or subcontractor serves to cancel any authorization previously granted, in which case the contractor shall be precluded from the continued use of foreign nationals on this contract or agreement until such time as compliance with an approved ACP is demonstrated and upon a determination by the CAO that the Government's interests are protected. Further, the Government reserves the right to cancel previously granted authority when such cancellation is determined to be in the Government's best interest. Use of foreign nationals, without an approved ACP or when a previous authorization has been cancelled, will be considered a violation of security regulations. Upon confirmation by the CAO of such

7 Aug 12

violation, this contract, agreement or any job order issued under this agreement may be terminated for default.

6. Prime contractors have full responsibility for the proper administration of the approved ACP for all work performed under this contract or agreement regardless of the location of the vessel and must ensure compliance by all subcontractors, technical representatives and other persons granted access to U.S. Navy vessels, adjacent areas, and work sites.

7. In the event the contractor does not intend to employ foreign nationals in the performance of work under this contract, but has foreign national employees, such employees must be precluded from access to the vessel and its work site and those shops where work on the vessel's equipment is being performed. The ACP must spell out how non-U.S. citizens are excluded from access to contract work areas.

8. The same restriction as in paragraph 7 above applies to other foreign nationals who have access to the contractor's facilities (e.g., for accomplishing facility improvements, from foreign crewed vessels within its facility, etc.).

Foreign National Access To Naval Vessels (ACP Certification)

1. The bidder or offeror, in the performance of any contract and/or job order resulting from this solicitation ___intends, _____ does not intend (check applicable line) to employ foreign nationals in the performance of work that requires access to naval vessels, work sites and adjacent areas when such vessels are under construction, conversion, overhaul or repair.

2. If the bidder or offeror, "intends" in paragraph 1 above, the bidder shall insert in the spaces provided below, the required information:

3. Whether or not the bidder or offeror intends to employ foreign nationals, the actual access of foreign nationals to naval vessels is subject to the requirements of the clause entitled "FOREIGN NATIONAL ACCESS TO NAVAL VESSELS".

ACCESS CONTROL PLAN (ACP)

Approved ACP No. _____

If no approved ACP, indicate below the actions taken or anticipated relative to ACP submission to applicable Contract Administration Office. (See NAVSEA M-5510.2)

7 Aug 12

APPENDIX A

REFERENCES

1. The following references will aid in interpreting this manual:

- (a) SECNAVINST 5510.30, Department of the Navy (DoN) Personnel Security Program (PSP) Instruction
- (b) OPNAVINST 5530.14, Navy Physical Security and Law Enforcement Program
- (c) OPNAVINST 5510.163, Control of Naval Reserve Personnel Involvement in Naval Nuclear Propulsion Matters
- (d) SECNAV M-5510.36, DoN Information Security Program
- (e) SECNAVINST 5510.34, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives
- (f) DODM 5200.01-V4 of 24 February 2012, DoD Information Security Program: Controlled Unclassified Information
- (g) OPNAVINST N9210.3, Safeguarding of Naval Nuclear Propulsion Information (NNPI)
- (h) CG-RN-1, Revision 3, of February 1996, Department of Energy (DOE) - Department of Defense (DOD) Classification Guide for the Naval Nuclear Propulsion Program
- (i) NAVSEAINST 5230.12, Release of Information to the Public
- (j) Department of the Navy Civilian Human Resources Manual Subchapter 752 of December 2003
- (k) CNO 5510 Ser N09N2/11U213200 of 22 Dec 11, Department of the Navy Implementation of Homeland Security Presidential Directive 12
- (l) NAVSEA Form 5512/8, NAVSEA Photographic or Audible Recording Device Permit

7 Aug 12

APPENDIX B

DEFINITIONS

1. The following terms and their definitions, listed in alphabetical order, will aid in interpreting this manual:

a. Automated Entry Control System (AECS) - A computer based system designed to manage and facilitate access control processing.

b. Armed Guard - An authorized person equipped with a firearm whose primary function is to protect property and who has qualified with the firearm by means of an approved weapons qualification course. The guard is considered armed when the firearm and ammunition are readily available for immediate use.

c. Contractors - For the purpose of this instruction, contractors, vendors and salespersons will be identified as contractors.

d. Controlled Industrial Area (CIA) - A CIA is a restricted area of a shipyard in which construction, conversion, repair or overhaul of U. S. Navy ships is conducted.

e. Controlled Nuclear Information Area (CNIA) - A CNIA is an area where unescorted access would provide access to significant amounts of unclassified naval nuclear propulsion information (U-NNPI). In a CNIA all unsecured classified National Security Information (NSI) will be under the direct control of an authorized individual who has either a yellow or red badge. All unsecured Restricted Data (RD) is under direct control of an authorized individual who has a red badge. If unescorted access to an area would provide access to classified Naval Nuclear Propulsion Plant Information, then the area must be identified as a Nuclear Work Area.

f. Force Protection Condition (FPCON) - A DoD-approved system standardizing DoD's identification of and recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. The system is the principal means for a commander to apply an operational decision on how to protect against terrorism and facilitates coordination among DoD Components and support for antiterrorism activities. Details are provided in DODI 2000.16 of 2 October 2006.

7 Aug 12

g. Non-Sensitive Area (NSA) - NSAs are those locations, buildings, and areas which are government property under the control of a Shipyard Commander, but do not involve either a CIA, CNIA, NWA, Security Island, or Other Sensitive Area (OSA). These areas include government, civilian, or military service oriented functions (e.g., Navy Exchange, Commissary, child care, banks, restaurants, etc.). When a shipyard is a tenant activity, this designation will only apply to those areas under shipyard control.

h. Nuclear Work Area (NWA) - Nuclear work areas are those areas which are of a nature that unescorted access to them would result in access to classified Naval Nuclear Propulsion Information (NNPI), (either National Security Information (NSI) or Restricted Data (RD)). The mere presence of classified NNPI in an area does not make the location a NWA. If the classified NNPI is under direct continuous control of authorized individuals, so that escorted access or other controls are utilized which will prevent access by unauthorized individuals to this classified information, the area need not be designated as a NWA. NNPI is defined in reference (g) and security classification guidance is provided in reference (h). For purposes of this definition, the engineering spaces of nuclear powered ships, within the shipyard, are considered NWAs.

i. Official Visit - Official visits are those visits authorized by the Commanding Officer that have a direct relationship to the basic mission and functions of a command.

j. Other Sensitive Area (OSA) - An OSA is an area or a building in the shipyard outside the CIA, where sensitive work is conducted, but which is not designated a NSA, CNIA, NWA or Security Island, where additional access controls are required. If the OSA contains sensitive functions which require restricted area designation, they will be separately designated and controlled in accordance with restricted area requirements of reference (b).

k. Restricted Area - Restricted areas are established in writing by the Commanding Officer. These areas are established in accordance with section 797 of title 50, U.S.C. There are three types of Restricted Areas: Level 3, Level 2, and Level 1. Definitions of these areas are contained in reference (b).

l. Sensitive Work Periods - Sensitive Work Periods are periods in which critical shipyard functions or events occur, requiring increased security measures. Such functions and

7 Aug 12

events include, but, are not limited to defueling, refueling, and special ocean engineering operations.

m. Watchman - A watchman is an unarmed person whose primary function is to control access.
