Chapter 13 – Security

Table of Contents

References

(a) DoD Manual 5200.01, Vol 1-4, DoD Information Security Program

(b) SECNAVINST 5510.36B, Department of the Navy Information Security Program

(c) SECNAV M-5510.30, Department of the Navy Personnel Security Program

(d) SECNAVINST 5510.30B, DON Personnel Security Program (PSP)

(e) OPNAVINST 5530.14E (Chg 3), Navy Physical Security and Law Enforcement

(f) SECNAV 3070.2A, Operations Security

(g) NAVSEA M-5510.1, NAVSEA Security Program Manual

(h) Federal Acquisition Regulation (FAR)

(i) NAVSEA Standard Item 009-72, Physical Security at Private Contractor's Facility

(j) DoD 5220.22-M (Chg 2), National Industrial Security Program Operating Manual (NISPOM)

(k) OPNAVINST F3300.53C, Navy Antiterrorism (AT) Program

(l) DoD 5220.22-R, Industrial Security Regulation

(m) DoD Instruction 5220.22, National Industrial Security Program

(n) DoD Directive 5220.6, Defense Industrial Personnel Security Clearance Review Program

(o) DoD Instruction 8510.01 (Chg 1), Risk Management Framework (RMF) for DoD Information Technology (IT)

(p) DoD Instruction O-2000.16, DoD Antiterrorism (AT) Standards

(q) SECNAVINST 3300.2C, DoN Antiterrorism Program

Chapter 13 – Security

13.1 Introduction

Security is an “All Hands” responsibility and one that requires constant vigilance. This chapter provides basic security information important to all SUPSHIP personnel. It addresses the two major categories of SUPSHIP security responsibilities; first, the internal security of the command, including access control and classified material control; and second, SUPSHIP’s responsibility to oversee contractor compliance with contractual security requirements.

13.2 SUPSHIP Internal Security Responsibilities

13.2.1 SUPSHIP Personnel

Internal security programs and procedures are to be in place and are to be managed by a Security Officer that is appointed in writing by the Supervisor to protect documents from unauthorized disclosure to individuals within the organization or visitors. All personnel must possess the appropriate security clearance and have a “need to know” to gain access to specific classified documents or data. Department of Defense (DoD) and Department of Navy (DON) Antiterrorism/Force Protection (AT/FP) Program security requirements define policies and procedures that are to be in place for the protection of personnel and government property.

All SUPSHIP personnel are responsible for complying with internal security programs and security regulations and assisting in protection of classified information and data from unauthorized disclosure. Additionally, SUPSHIP personnel are to attend annual security briefings. Navy policies for safeguarding classified material and information are addressed in:

- DoDM 5200.01, Vol 1-4, DoD Information Security Program, reference (a)
- SECNAVINST 5510.36B, DON Information Security Program, reference (b)
- SECNAV M-5510.30, DON Personnel Security Program, reference (c)
- SECNAVINST 5510.30B, DON Personnel Security Program (PSP), reference (d)

In addition, the SUPSHIPs are responsible for implementing the directives concerning AT/FP Programs in their facilities (see paragraph 13.6).

The Administrative Contracting Officer (ACO) is assisted by the Security Officer and SUPSHIP project team in administering contractual terms and conditions for oversight of security programs and processes at the assigned industrial organization, or at commercial organizations that provide administrative or technical support through a contract with SUPSHIP. The oversight includes:

- Physical security for the industrial facility
- Industrial Security Program relative to plant security clearance and authorization for storage, processing, and handling classified documents
- Personnel access to naval vessels and facilities
- Contractually imposed AT/FP compliance

Personnel within SUPSHIPs who interface with contractors should be familiar with pertinent regulations and policies pertaining to contractors when contracts administered by the SUPSHIP involve access to classified information or require compliance with the AT/FP Program.

13.2.2 SUPSHIP Security Officer Responsibilities

The Security Officer is accountable to the Supervisor for all internal and external security matters for which the SUPSHIP is responsible. Responsibilities vary among SUPSHIPs based in part upon the added security requirements associated with safeguarding nuclear propulsion systems and associated secondary systems, equipment, and information. With the exception of the nuclear-related items, the following three primary functions and associated responsibilities are applicable to all SUPSHIPs.

13.2.2.1 Security Officer/Director Responsibilities

Security Officer responsibilities include:

a. Security Department or Division Head

b. Personnel, Information, Industrial, Physical, and Operations Security (OPSEC) that includes administering all SUPSHIP internal and external security matters per:

(1) SECNAVINST 5510.36B, DON Information Security Program

(2) SECNAV M-5510.30, DON Personnel Security Program Regulation

(3) SECNAVINST 5510.30B, DON Personnel Security Program (PSP)

(4) OPNAVINST 5530.14E (Chg 3), Navy Physical Security and Law Enforcement, reference (e)

(5) NAVSEAINST 5510.1C**, NAVSEA Security Program Instruction, reference (f)

(6) SECNAV 3070.2A, Operations Security, reference (g)

(7) NAVSEA M-5510.1**, NAVSEA Security Program Manual, reference (h)

** Denotes hyperlink requiring CAC/NMCI access

(8) FAR Subpart 4.4, Safeguarding Classified Information Within Industry, reference (i)

(9) Other NAVSEA instructions concerning specific security programs

c. administering the command's security education, training and awareness (SETA) programs

d. commanding security inspections and security assist visits

e. applying risk management relative to assessments of security preparedness

f. managing compliance with treaties requirements for security matters

g. managing workplace violence policy and procedures

h. serving as Contracting Officer's Representative (COR) for contract security matters

i. ensuring contractor compliance with physical security requirements of NAVSEA Standard Item 009-72, Physical Security at Private Contractor's Facility, reference (j), when contractually invoked (check applicable fiscal year)

13.2.2.2 Security Manager Responsibilities

Security Manager responsibilities include:

a. managing Communications Security (COMSEC) and Key Management Infrastructure (KMI) systems

b. managing work export issues with the contracting officer and contractor

c. maintaining oversight of disclosure of documents and data to foreign entities

d. managing classified material

e. interfacing with Defense Security Service (DSS), NAVSEA Office of Security Programs, and NAVSEA Procuring Contracting Officer (PCO) as stated in DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), reference (k), when the use of classified Information is required for contract performance

f. working with the contractor's Facility Security Officer (FSO), including:

(1) verifying that the contractor has a current facility security clearance

(2) confirming that the contractor's facilities and personnel clearances meet the requirements for accessing and handling classified documents and information as specified in the Security Requirements Clause required by FAR Subpart 4.4

(3) verifying that work spaces where classified material will be accessible during work hours and storage facilities are in compliance with the requirements in NISPOM and other applicable DoD or DON instructions

(4) obtaining a listing of contractor personnel who have current security clearances and who have been authorized levels of access and eligibility

(5) verifying that access control is compliant with the level of security that is imposed

(6) providing the Facility Security Officer (FSO) a list of all non-contractor personnel who have proper clearance and who will work with the contractor on classified portions of the job order

(7) receiving, reviewing and approving or disapproving all contractor access lists for ships under construction or commissioned ships under conversion or repair, and for transmission of the access lists to the vessels and the applicable shipyard or activity access control or security offices

(8) reviewing and approving the contractor's Access Control Plans (ACPs) for Government vessels and sites at which vessels are under construction or conversion, and administering the contractor's compliance with access to naval vessels and worksites

g. managing personnel security, visitor control, badge management, etc.

h. reviewing information proposed for public release for security compliance

i. ensuring protection of research and technology documents from inappropriate disclosure

j. ensuring the protection of controlled unclassified information (CUI)

k. maintaining oversight of Navy Nuclear Propulsion Information (NNPI) control processes

l. supporting the command in addressing international agreements

m. providing assistance with international security issues

n. managing Operations Security (OPSEC) requirements

o. ensuring contractor compliance with NAVSEA Standard Item 009-72, when invoked by contract, including reviewing and approving the contractor's Plant Protection Plan (PPP)

p. periodically visiting the contractor's spaces with the FSO to validate continuing compliance with all security regulations

13.2.2.3 Antiterrorism (AT) Officer Responsibilities

The Anti-Terrorism Officer responsibilities include:

a. managing the command AT Program

b. establishing and chairing the Antiterrorism Working Group (ATWG)

c. establishing and chairing the Threat Working Group (TWG)

d. conducting Threat Assessments

e. conducting Vulnerability Assessments

f. conducting Risk Assessments as requested

g. maintaining liaison with Government and private agencies concerning local threats and coordinating AT plans and security matters

h. exercising elements of the AT plans

i. coordinating budgeting and funding for the AT Program

j. ensuring contractor compliance with OPNAVINST F3300.53C**, Navy Antiterrorism (AT) Program, reference (l), when contractually invoked

13.3 Defense Security Service (DSS) Responsibilities

DoD 5220.22-M assigns security cognizance for Government Contracting Activity (GCA) contractors to DSS whose authority is exercised by the various DSS Field Offices. The geographical areas of responsibility of these DSS field offices are listed in the DoD 5220.22-R, Industrial Security Regulation (ISR), reference (m). The assignment of a DSS field office responsible for performing all the security functions is set forth in the DoD ISR. For the Navy, this is implemented by SECNAVINST 5510.36B and SECNAV M-5510.30. DSS is required to:

a. administer DoDI 5220.22, National Industrial Security Program (NISP), reference (n), as a separate program element on behalf of the GCAs

b. provide security education, training and awareness (SETA) to the industrial and GCA personnel

c. maintain a record of eligibility determinations for access to classified information for contractor personnel

** Denotes hyperlink requiring CAC/NMCI/OPNAV SharePoint Portal access

d. maintain a record of eligibility determinations that is accessible to all GCAs

e. maintain a system for communicating with NISP contractors and GCAs

f. certify and accredit the contractor's Information Systems (IS) for processing classified information and data

DoD 5220.22-M (NISPOM) applies to industry teams, including their development sites and ship construction sites. The NISPOM provides guidance to industry about security clearances, security training, classification and marking of documents, and appropriate storage. Section 8 of the NIPSOM specifically discusses IS security that includes guidance on how to properly certify and accredit IS, such as computers, media and networks. Following the NISPOM guidance, the contractors are inspected by, and must receive approval from DSS, to receive, store and create classified material. This includes certification and accreditation (C&A) of their IS to operate with classified information and data.

13.4 SUPSHIP External Security Considerations

SUPSHIP is a Government Contracting Activity (GCA) as defined in DoDI 5220.22. DoD sets policies, practices and procedures that are to be followed by GCAs for the effective protection of classified information provided to industry, including foreign classified information the U.S. Government is obligated to protect in the interest of national security. DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program, reference (o), establishes the standards and criteria for determining security eligibility for contractor personnel requiring access to classified information.

Government instructions, directives, manuals, etc. are not applicable to contractors unless they are contractually invoked. Modifications in the Government's AT/FP Program that increase requirements relative to shipbuilding contracts, or when active ships and submarines are under contract at a contractor's facility, must be contractually invoked in order to require contractor compliance with the added requirements, and for the SUPSHIPs to have the necessary authority to assure compliance.

As a DoD CAS Component, the Procuring Contracting Office (PCO) shall review all contracts before award to decide if releasing classified information is necessary for contract performance. If access to classified information is required for contract performance, the contract shall include the "Security Requirements" clause required by FAR Subpart 4.4, "Safeguarding Classified Information within Industry", and security classification guidance to the contractor shall be provided via a DD Form 254, Contract Security Classification Specification. When contractor access to classified information is required, the contract will require compliance with DoD 5220.22-M, National Industrial Security Program Operating Manual: (NISPOM). Additionally, a DoD Security Agreement, DD Form 441, shall be executed and the PCO should assure that the Contract Data Requirements List (CDRL) specifies that the contractor is to develop a Security Plan for the Navy. The Security Plan shall discuss measures that are, or will be, implemented by the contractor to protect

classified information at the shipyard construction sites, including buildings and the ship under construction. Special requirements exist that must be complied with for ships under construction prior to delivery. DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), reference (p), governs the certification, testing and accreditation of military Information Systems. SUPSHIP will utilize this instruction and the Security Plan to provide oversight of shipboard classified AIS processing.

For contracts requiring access to classified information, a contractor must have the appropriate facility clearance as authorized by DSS and as specified in the solicitation/Security Clause prior to contract award. The current facility clearance and storage capability may be verified by the cognizant DSS Office, the DSS Central Verification Activity (telephone 1-888-282-7682), or may be based on knowledge gained through current contractual dealings with the company, as would be the case with SUPSHIP.

The contractor's FSO is required to submit to the SUPSHIP Security Officer an Access Control Plan (ACP). The Security Officer is accountable for approving and oversight of the contractor's ACP for all non-US citizens. The ACP applies to contractor employees who may access naval vessels, including sites where naval vessels are being constructed. Any contractor who intends to hire non-citizens is required to obtain approval from SUPSHIP prior to employment if a government contract has been awarded or has the potential to be awarded to the contractor.

13.5 Physical Security within Contractor Facilities

Primary guidance for private shipyard security, when invoked by contract, is contained in NAVSEA Standard Item (SI) 009-72, Physical Security of U.S. Naval Vessels and Crew at Private Contractors Facilities. A shipbuilding contract performance period typically covers several years. Because SI 009-72 is subject to an annual update, increased requirements in the SI beyond those specified in the existing contract must be contractually invoked if the new requirements are to be implemented.

The contractor is required to have a Plant Protection Plan (PPP), compliant with the NAVSEA Standard Item 009-72, when contractually invoked. The SUPSHIP Security Officer reviews and approves the PPP. The SUPSHIP Security Officer, contractor's FSO, Contracting Officer and Program Office personnel participate in security planning and oversight in assuring compliance during the contract's performance period. The contractor must establish and maintain a personnel identification system, control visitor access to the facility, and control the receipt and removal of property from the facility. Government personnel must comply with the contractor's security regulations when they are in the contractor's facility. If the Government wants physical security arrangements other than those required by the original contract, the change in requirements must be authorized by a contract modification with an adjustment in contract price. Additional security requirements could include such items as additional security in ship's force parking areas or the patrol of water approaches to the contractor's facility.

The PCO shall include in the solicitation any requirements for providing protection for U.S. Government employees and property. Typically, the contractor will augment its security force to monitor and assure the well-being of government personnel.

13.6 Antiterrorism/Force Protection (AT/FP)

SUPSHIP is required to implement the AT/FP within the command. Additionally, SUPSHIP, as ACO, is charged with ensuring that all AT/FP requirements invoked in the contract are in place and maintained by the contractor for the duration of the performance period. The following are some of the more important documents concerning the AT/FP Program:

- DoDI O-2000.16, DoD Antiterrorism (AT) Standards, reference (q)
- SECNAVINST 3300.2C, DON Antiterrorism Program, reference (r)
- NAVSEA Standard Item 009-72

OPNAVINST F3300.53C**, Navy Antiterrorism (AT) Program, provides guidelines on how to set up an AT/FP program, including training and appointing Antiterrorism Officers (ATO) and Force Protection Officers (FPO). The other documents outline the requirements for protecting Navy personnel and property in contractor facilities. The AT/FP mandates are focused on establishing positive plans and deterrents to preclude unauthorized entry with the intent to cause damage to personnel or equipment from ashore or from the water.

The contractor typically will not implement emerging new requirements made to government directives that are not already contained in the contract unless a change is made to the contract and they are compensated for the change. For example, if OPNAVINST F3300.53C** was invoked in a contract being administered by SUPSHIP and the instruction was subsequently revised to include new requirements, the contractor could not be held responsible for implementing the new requirements unless a contract change was issued that imposed the new requirements. An appropriate contract price adjustment would also be necessary to accommodate the difference in cost between the original and new requirements.

** Denotes hyperlink requiring CAC/NMCI/OPNAV SharePoint Portal access

Appendix 13-A: Acronyms

ACO	Administrative Contracting Officer
ACP	Access Control Plan
AIS	Automated Information System
AT	Anti-Terrorism
AT/FP	Anti-Terrorism/Force Protection
ATO	Anti-Terrorism Officer
ATWG	Anti-Terrorism Working Group
C&A	Certification and Accreditation
CAS	Contract Administration Service
CDRL	Contract Data Requirements List
COMSEC	Communications Security
COR	Contracting Officer's Representative
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoD-R	Department of Defense Regulation
DoN	Department of the Navy
DSS	Defense Security Service
FAR	Federal Acquisition Regulations
FPO	Force Protection Officer
FSO	Facility Security Officer
GCA	Government Contracting Activity

IS	Information System
ISP	Information Security Program
KMI	Key Management Infrastructure
NAVSEA	Naval Sea Systems Command
NAVSEAINST	Naval Sea Systems Command Instruction
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NNPI	Navy Nuclear Propulsion Information
OPNAVINST	Chief of Naval Operations Instruction
OPSEC	Operations Security
PCO	Procuring Contracting Officer
PPP	Plant Protection Plan
SECDEF	Secretary of Defense
SECNAVINST	Secretary of Navy Instruction
SECNAV-M	Secretary of the Navy Manual
SUPSHIP	Supervisor of Shipbuilding, Conversion and Repair, USN
TWG	Threat Working Group