Chapter 13 – Security

Table of Contents

13.1 Introduction 13-3

13.2 NAVSEA Security Program Guidance and Direction 13-3

13.3 SUPSHIP Security Responsibilities 13-4
13.3.1 Internal Security Responsibilities 13-4
13.3.2 External Security Responsibilities 13-4

13.4 SUPSHIP Security Organization 13-5
13.4.1 SUPSHIP Commanding Officer 13-5
13.4.2 Activity Security Manager (ASM) 13-5
13.4.3 Security Contracting Official (SCO) 13-6
13.4.4 Information System Security Manager (ISSM) 13-6
13.4.5 Top Secret Control Officer (TSCO) 13-6
13.4.6 Special Security Officer (SSO) 13-6
13.4.7 Antiterrorism (AT) Officer 13-7
13.4.7.1 ATO Responsibilities 13-7

13.5 Contract Security Requirements 13-8
13.5.1 Federal Acquisition Regulation (FAR) 13-8
13.5.2 National Industrial Security Program Operating Manual (NISPOM) 13-8
13.5.3 NAVSEA Contract Clauses Used in New Construction Contracts 13-9
13.5.4 NAVSEA Standard Item 009-72 13-9
13.5.4.1 Annual Review of NAVSEA Standard Item 009-72 13-10

13.6 Activities Overseeing Contract Security Requirements 13-10
13.6.1 Defense Counterintelligence and Security Agency (DCSA) Responsibilities 13-10
13.6.2 Government Contracting Activity (GCA) Responsibilities 13-11
13.6.3 SUPSHIP Responsibilities 13-12

Appendix 13-A: Acronyms 13-14

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

References

(a) NAVSEA M-5510.1, Naval Sea Systems Command Security Program Manual (July 2022)

(b) NAVSEAINST 3070.2, Naval Sea Systems Command Operations Security

(c) NAVSEA M-5510.2, NAVSEA Access and Movement Control Manual (November 2018)

(d) NAVSEAINST 5510.1D, Naval Sea Systems Command Security Program

(e) NAVSEAINST 5510.2D, Naval Sea Systems Command Access and Movement Control

(f) NAVSEAINST 5510.21A, Naval Sea Systems Command Insider Threat Program

(g) NAVSEAINST 5510.24, Naval Sea Systems Command Antiterrorism Policy

(h) NAVSEAINST 5527.1, Naval Sea Systems Command Security Accountability

(i) NAVSEAINST 5510.22, Naval Sea Systems Command Classified Information Systems Removable Media

(j) NAVSEAINST 5239.2B, Cybersecurity Program

(k) NAVSEAINST 2200.01A, Portable Electronics Devices Policy

(l) 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM)

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

(n) DoDM-5105.21, Volume 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities

(o) OPNAVINST F3300.53D, Navy Antiterrorism Program

(p) DoDI O-2000.16, Vol 1, DoD Antiterrorism (AT) Program Implementation – DoD Antiterrorism Standards (7 May 2021)

(q) DoDI O-2000.16, Vol 2, DoD Antiterrorism Program Implementation: DoD Force Protection Condition (FPCON) System (8 May 2017)

(r) SECNAVINST 3300.2C, DoN Antiterrorism Program

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

(t) DoDI 5220.31, National Industrial Security Program

(u) DoDM-5220.32, Volume 1, National Industrial Security Program: Industrial Security Procedures for Government Activities

(v) DoDM 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

Chapter 13 – Security

13.1 Introduction

Security is an all-hands responsibility, so it is important that all SUPSHIP personnel have a basic understanding of the command's security program and understand and are aware of potential security risks and threats. To that end, NAVSEA imposes annual security training requirements for all personnel. This training includes:

- Antiterrorism
- Operations Security
- NAVSEA Annual Security Refresher
- Counterintelligence and Insider Threat Awareness
- Foreign Disclosure
- Controlled Unclassified Information (CUI)

This chapter identifies the principal NAVSEA security directives providing direction and guidance for security programs common to all NAVSEA activities. While those programs also apply to SUPSHIPs, they are not addressed in this chapter, which instead focuses on the security programs directly associated with the SUPSHIP mission of administering assigned DoD contracts as well as any contracts for which SUPSHIP is the Procuring Contracting Officer (PCO) or the Government Contracting Activity (GCA).

13.2 NAVSEA Security Program Guidance and Direction

NAVSEA M-5510.1**, Naval Sea Systems Command Security Program Manual, reference (a), serves as the principal guidance and direction for NAVSEA headquarters and field activity security programs. Topics addressed in this comprehensive manual include:

- Security Management
- Personnel Security and Insider Threat
- Information Security Program
- Industrial Security
- Communications Security
- Operations Security (OPSEC) (supplemented by reference (b) below)
- Physical Security (PHYSEC), Antiterrorism and Force Protection (AT/FP)
- Research and Technology Protection
- Foreign Travel Program
- Security Education, Training, and Awareness (SETA) Program
- Key and Lock Control Program
- Anti-Terrorism Program
- Lost and Found Procedures
- Access Movement Control
- Foreign Disclosure Policy and Foreign Visit Programs

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

- Security Oversight

The following NAVSEA directives provide additional guidance and direction:

- NAVSEAINST 3070.2, Naval Sea Systems Command Operations Security, reference (b)
- NAVSEA M-5510.2**, NAVSEA Access and Movement Control Manual, reference (c). Note that chapter 2 of this instruction specifically addresses physical security and access control requirements for SUPSHIPs
- NAVSEAINST 5510.1D**, Naval Sea Systems Command Security Program, reference (d)
- NAVSEAINST 5510.2D**, Naval Sea Systems Command Access and Movement Control, reference (e)
- NAVSEAINST 5510.21A**, Naval Sea Systems Command Insider Threat Program, reference (f)
- NAVSEAINST 5510.24**, Naval Sea Systems Command Antiterrorism Policy (g)
- NAVSEAINST 5527.1, Naval Sea Systems Command Security Accountability, reference (h)
- NAVSEAINST 5510.22**, Naval Sea Systems Command Classified Information Systems Removable Media, reference (i)
- NAVSEAINST 5239.2B**, Cybersecurity Program (j)
- NAVSEAINST 2200.01A**, Portable Electronics Devices Policy, reference (k)
- NAVSEAINST 5450.36C, Missions, Functions and Tasks of the Supervisors of Shipbuilding, Conversion and Repair

13.3 SUPSHIP Security Responsibilities

13.3.1 Internal Security Responsibilities

Internal security responsibilities include managing applicable security programs within the command as directed by higher authority. NAVSEA M-5510.1** is the principal directive for establishing these command responsibilities and is augmented by the other NAVSEA directives listed in section 13.2. SUPSHIPs must also comply with applicable requirements of DoD, SECNAV, and OPNAV security directives.

13.3.2 External Security Responsibilities

External security responsibilities are related to the SUPSHIP mission of administering assigned DoD contracts awarded to the U.S. shipbuilding and ship repair industry. As the Contract Administration Office (CAO), SUPSHIPs provide onsite oversight of contractor adherence to contractual obligations, including contractually invoked industrial security requirements when delegated by the PCO. SUPSHIPs do not, however, have primary responsibility for oversight of contractor industrial security. As addressed in section 13.6.1, that responsibility falls on the Defense Counterintelligence Security Agency who administers the National Industrial Security Program (NISP) and contractor compliance with its requirements.

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

13.4 SUPSHIP Security Organization

13.4.1 SUPSHIP Commanding Officer

As commanding officers of NAVSEA field activities, NAVSEA M-5510.1** assigns the following security responsibilities to SUPSHIP commanding officers:

(a) Develop, establish, and implement effective command security programs consistent with higher-level authority.

(b) Mandate compliance at the command, detachments, and field offices.

(c) Designate, in writing, an Activity Security Manager (ASM) to direct the management of the command's security programs. The ASM must have sufficient authority and staff to effectively manage the programs for the command. The designation letter must be provided to SEA 00P via SEA 00P3 and updated whenever a new ASM is designated.

(d) Establish and maintain security oversight for detachments and field offices, to include self-inspections, security inspections, program reviews, and assist visits to evaluate and assess industrial security program effectiveness.

(e) Ensure command personnel who play a role in the command's security programs receive training commensurate with their roles and responsibilities and support the command's SETA program.

13.4.2 Activity Security Manager (ASM)

The ASM serves as the commanding officer's principal adviser responsible for management of the command's security programs. The SUPSHIP ASM, also known as the Security Manager or Security Officer, heads the SUPSHIP security division.

NAVSEA M-5510.1** assigns the following security responsibilities to the ASM:

(a) Comply with the requirements of higher-level directives.

(b) Manage the command's security program, including the information security program (ISP), personnel security (PERSEC), physical security (PHYSEC), antiterrorism/force protection (AT/FP), and industrial security (INDUSEC) program (for contracts procured by the SUPSHIP).

(c) Provide guidance and oversight on security matters to detachments and field offices.

(d) Brief the incoming commanding officer within 30 days of reporting on board on the status of security programs.

(e) Ensure that personnel performing security duties are kept abreast of changes in policies and procedures and are assisted in problem solving.

(f) Nominate candidates for SCO designation, who upon meeting training prerequisites and designation, will serve as SCO for the command.

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

(g) Support NAVSEA HQ-led security inspections, assist visits, and program reviews.

13.4.3 Security Contracting Official (SCO)

Per NAVSEA M-5510.1, SEA 00P designates the SCO for each NAVSEA subordinate command performing PCO functions. Typically, the SUPSHIP ASM is also assigned as the SCO. Duties include:

- Reviewing security requirements for contracts solicited by SUPSHIPs and ensuring the inclusion of a DD Form 254, DD Form 441, and appropriate contract security clauses and Contract Data Requirements Lists (CDRL)
- Ensuring classified contracts are awarded only to contractors cleared by DCSA
- Acting as the commanding officer's representative for SUPSHIP industrial security matters

13.4.4 Information System Security Manager (ISSM)

The ISSM is the SUPSHIP point of contact for all command Information Assurance (IA) matters and is responsible for implementing and maintaining the command's IA program. SUPSHIPs ISSMs are assigned to the Activity Chief Information Officer (ACIO)/Information Resources department (C800) rather than the security division. Per NAVSEA M-5510.1, ISSMs are assigned the following industrial security responsibilities:

- Review and approve or deny contractor requests for deviation from Part 117.18, Information Systems Security, of 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM), reference (l).
- Review and approve or deny contract requests for deviation from requirements for protecting CUI in nonfederal systems and organizations.

Additionally, the ISSM is responsible for overseeing contractor compliance with DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

SOM chapter 16, Cybersecurity Management, provides additional information regarding SUPSHIP ISSM responsibilities.

13.4.5 Top Secret Control Officer (TSCO)

When required, a TSCO is assigned for all commands that handle top secret information with duties as prescribed by SECNAVINST 5510.36B, Department of the Navy Information Security Program, reference (m).

13.4.6 Special Security Officer (SSO)

An SSO is assigned to SUPSHIPs that are DON accredited and authorized to receive, process, and store Sensitive Compartmented Information (SCI). The SSO has direct access to the commanding officer and serves as the command's primary point of contact for all SCI matters. The SSO is responsible for managing and administering the command's SCI security program, including the

operation and security controls of the Sensitive Compartmented Information Facility (SCIF). Program responsibilities are detailed in DoDM-5105.21, Volume 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities, reference (n).

13.4.7 Antiterrorism (AT) Officer

Per OPNAVINST F3300.53D**, Navy Antiterrorism Program, reference (o), SUPSHIPs are required to establish an AT program tailored to the local mission, conditions and terrorist threat. SUPSHIP commanding officers must designate an Antiterrorism Officer (ATO), in writing, to implement and manage the command's AT/FP program. Additionally, SUPSHIP, as the CAO, is charged with ensuring that contractually invoked AT/FP contractual requirements are in place and maintained by the contractor.

Because SUPSHIPs are located in commercial shipyards and are not under the auspices of a base commander, SUPSHIPs should develop local directives that delineate AT/FP roles, responsibilities, and the procedures to be followed and support to be provided by SUPSHIP, the shipbuilder, ship's force/PCUs, SUPSHIP visitors, and any supporting security forces.

In addition to OPNAVINST F3300.53D**, the following directives provide AT/FP program guidance:

- DoDI O-2000.16, Vol 1**, DoD Antiterrorism Program Implementation: DoD Antiterrorism Standards (7 May 2021), reference (p)
- DoDI O-2000.16, Vol 2**, DoD Antiterrorism Program Implementation: DoD Force Protection Condition (FPCON) System (8 May 2017), reference (q)
- SECNAVINST 3300.2C, DON Antiterrorism Program, reference (r)
- NAVSEAINST 5510.24**, Naval Sea Systems Command Antiterrorism, reference (g)

13.4.7.1 ATO Responsibilities

ATO responsibilities include the functions listed below. Note that contractor responsibilities associated with these functions are imposed only when contractually invoked and supported/funded by the program manager.

a. Managing the command AT Program.

b. Establishing and convening the Antiterrorism Working Group (ATWG).

c. Establishing and convening 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. Developing an AT Plan.

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

i. Randomly exercising elements of the AT plan.

j. Ensuring contractor compliance with contractually invoked AT requirements, such as OPNAVINST F3300.53** and NAVSEA Standard Item (SI) 009-72, Physical Security at a Private Contractor Facility, reference (s).

k. Complying with the requirements of NAVSEAINST 5510.24**, including conducting and documenting an annual review of the required list of AT requirements outlined in the current version of SI 009-72 (see 13.5.4). Note that imposing NAVSEAINST 5510.24** requirements on a contractor would require a contract change for any requirement that has not been contractually invoked.

13.5 Contract Security Requirements

13.5.1 Federal Acquisition Regulation (FAR)

The NAVSEA PCO, in coordination with the NAVSEA SCO and the GCA (typically the Program Executive Office (PEO) or Program Manager (PM)), reviews contract procurement requests to determine if a contract requires contractor access to classified information. If it does, FAR Subpart 4.4, Safeguarding Classified Information within Industry, requires the use of DD Form 254, Contract Security Classification Specification, to establish classified access requirements. For those contracts, FAR 4.404, Contract Clause, requires contracting officers to insert FAR clause 52.204-2 in solicitations and contracts. This clause requires the contractor to comply with the Security Agreement, DD Form 441, which includes requirements for the contractor to:

- Provide and maintain a system of security controls in accordance with the NISPOM.
- Determine that any subcontractors involved in access to classified information have been granted an appropriate Facility Clearance (FCL). FCL and storage capability may be verified in the National Central Access Information Security System (NCAISS) portal of the National Industrial Security System or may be based on knowledge gained through current contractual dealings with the company, as would often be the case with SUPSHIP.
- Grant USG personnel the right to conduct security reviews of the procedures, methods and facilities utilized by the contractor.

For classified contracts, FAR 42.302(a)(21) requires the CAO to administer applicable portions of the industrial security program as delegated by the PCO. This requirement applies specifically to safeguarding classified information released to contractors.

13.5.2 National Industrial Security Program Operating Manual (NISPOM)

The NISPOM implements policy, assigns responsibilities, establishes requirements, and provides standard procedures and requirements for the protection of classified information that is disclosed to or developed by contractors of the U.S. Government (USG). It is applicable to all USG executive branch departments as well as industrial, educational, commercial, and other non-USG entities granted access to classified information by the executive branch. The NISPOM provides industry with rules and guidance for contractor security requirements, including but not limited to:

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

- Security organization
- Cooperation with federal agencies and USG reviews
- Security programs, such as the Insider Threat Program
- Reporting requirements
- Security clearances
- Security training and briefings
- Classification, marking and safeguarding classified information
- Classified visits and meetings, including by foreign nationals
- Subcontracting
- Information security

13.5.3 NAVSEA Contract Clauses Used in New Construction Contracts

In addition to FAR clause 52.204-2, NAVSEA prescribes the use of the following contract clauses for all shipbuilding, craft construction, and repair/overhaul contracts:

- C-211-H001 Access to Vessels**
- C-211-H005 Plant Protection**
    - Implements NAVSEA Standard Item 009-72, Physical Security at a Private Contractor Facility
- C-222-H001 Access to Vessels by non-U.S. Citizens**
- C-227-H003 Protection of Naval Nuclear Propulsion Information**
- C-227-H004 Transmission Abroad of Equipment or Technical Data Relating to the Nuclear Propulsion of Naval Ships**

Note that this section addresses only those requirements that are routinely invoked in NAVSEA shipbuilding, craft construction, and repair/overhaul contracts. The PCO may include additional security requirements at the request of the PEO, PM, or as directed by higher authority, which may require oversight by SUPSHIP per FAR 42.302(a)(21) if delegated by the PCO.

13.5.4 NAVSEA Standard Item 009-72

NAVSEA Standard Item (SI) 009-72, Physical Security of U.S. Naval Vessels and Crew at Private Contractors Facilities, is required to be invoked by NAVSEA contract clause C-211-H005** in all shipbuilding, craft construction, and repair/overhaul contracts (note that older contracts may not include this requirement). Because SI 009-72 is subject to annual updates, it is important to identify the version of SI 009-72 invoked for individual contracts. A contract change will be required if an updated version of 009-72 is intended to be applied to a contract with a prior version invoked.

SI 009-72 requires the contractor to have a written security plan for the protection of personnel, U.S. Naval vessels, work in progress, and the material and equipment to be installed. The security plan must address:

- Force Protection measures and the ability of the contractor to meet requirements for Conditions Normal, Alpha, Bravo, Charlie, and Delta
- Security conferences with SUPSHIP, Ship's Force, and federal, state, and local authorities

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

- Establishment and enforcement of land and water areas adjacent to U.S. Naval vessels as restricted areas
- Roles and responsibilities for application of deadly force in the protection of U.S. Navy assets and crews
- Physical security controls, including perimeter barriers, perimeter opening controls, access and circulation control, waterfront surveillance, armed security force, protective lighting, signs and posting of boundaries, and procedures for mass notification
- Random Antiterrorism Measures (RAM)

Per SI 009-72 and the NAVSEA Plant Protection clause (C-211-H005**), the shipbuilder must provide a copy of their security plan to SUPSHIP for review and approval. The ASM works with the contractor Facility Security Officer (FSO), the SUPSHIP ACO, and the program office to ensure compliance with the shipbuilder's security plan and the requirements of SI 009-72. Government personnel must comply with the contractor's security policies when they are in the contractor's facility. If the Government requests additional security arrangements beyond those required by the contract, a contract change must be authorized with an appropriate adjustment in the contract price.

13.5.4.1 Annual Review of NAVSEA Standard Item 009-72

Per NAVSEAINST 5510.24, SUPSHIPs are required to conduct and document an annual review of AT requirements outlined in the most current NAVSEA Standard Item 009-72. SEA 04Z will solicit and collect comments and recommended changes to 009-72, and any other recommended changes to NAVSEA standard items, to support timely submission to the Standard Specifications for Repairs and Alteration Committee (SSRAC). The SSRAC meets annually to review and modify NAVSEA standard items to ensure they reflect current requirements and provide the intended benefit to RMCs and SUPSHIPs in the oversight of their respective contracts. NAVSEAINST 5510.24 does not impose any requirements on the shipbuilder unless contractually invoked.

13.6 Activities Overseeing Contract Security Requirements

This section describes the three Government activities most directly involved in security oversight of contractors involved in U.S. Navy ship construction: DCSA, the assigned GCA, and the SUPSHIP assigned as the CAO. While DCSA and the GCA may have personnel assigned responsibilities for each shipbuilder, SUPSHIPs are the only activities providing full-time, onsite presence. As a result, SUPSHIPs are uniquely positioned to observe day-to-day security operations and be aware of conditions and risks affecting the shipbuilder's security environment. SUPSHIPs should communicate any concerns they have regarding shipbuilder security programs with DCSA, the GCA, SEA 00P, and the PCO, as appropriate.

13.6.1 Defense Counterintelligence and Security Agency (DCSA) Responsibilities

Per the NISPOM, DCSA serves as the Cognizant Security Office (CSO) for DoD and administers the NISP on behalf of DoD GCAs. Local DCSA support to GCAs, SUPSHIPs, and cleared contractors is provided by field offices identified on the Industrial Security Directorate (ISD) Field Locations page of the DCSA website.

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

In accordance with the NISPOM, NAVSEA M-5510.1, DoD Instruction 5220.31, National Industrial Security Program, reference (t), and the DCSA website (https://www.dcsa.mil), DCSA responsibilities include:

a. Providing GCAs with assurance that contractors are eligible for access to classified information and have systems in place to properly safeguard classified information in their possession and to which they have access.

b. Working in professional partnerships with contractor facility management staff and FSOs and establishing and maintaining procedures and tools for timely communication with NISP contractors and GCAs.

c. Conducting recurring security reviews of NISP contractors and notifying the GCA when a contractor's security posture is rated as marginal or unsatisfactory. These ratings also dictate that DCSA conduct a Compliance Security Review.

d. Maintaining a complete program of certification, accreditation, and oversight of contractor information systems used to process and store classified information.

e. Proposing changes to NISPOM and DoDM-5220.32, Volume 1, National Industrial Security Program: Industrial Security Procedures for Government Activities, reference (u).

f. Budgeting, funding, and administering the NISP.

g. Providing security education and training for DoD, other federal agencies, and cleared contractors under NISP.

h. Deciding eligibility for access to classified information by cleared company personnel.

i. Maintaining a record of eligibility determinations for cleared company personnel requiring access to classified information.

j. Establishing and maintaining a system for timely and effective communication with NISP contractors and GCAs.

k. Consulting with Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) or DoD components when there is a question as to whether there is a legitimate U.S. Government requirement for contractors or contractor personnel to have access to classified information.

13.6.2 Government Contracting Activity (GCA) Responsibilities

The DD Form 254 identifies the GCA for each contract. In most cases the GCA will be the requirements or funding activity, such as the cognizant PEO for ship construction contracts. DoDM-5220.32 (Vol 1), sets policies, practices, and procedures to be followed by GCAs for the effective protection of classified information provided to industry, including foreign classified information the U.S. Government must protect in the interest of national security.

Per DoDM 5220.32 (Vol 1), GCA responsibilities include:

a. Determining security requirements for assigned contracts and ensuring incorporation of DD Form 254 in classified solicitations and contracts

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

b. Determining clearance status of prospective contractors

c. Providing pre-award access to classified information when required

d. Exercising approval authority for the public release of any unclassified information related to the classified contract or subcontract

e. Responding to contractor requests for interpretation of classification guidance

f. Providing written instructions to contractors if authorization to retain classified information will be extended beyond the automatic 2-year retention period

g. Providing downgrading or declassification instructions to the contractor

h. Requesting a DCSA review if circumstances indicate that classified information may be at risk

i. Notifying DCSA of any suspicious contacts or other incidents related to onsite contractors in accordance with DoDM 5220.32 (Vol 1), Section 8

j. Initiating an investigation of unauthorized disclosure of classified information to determine the cause and establish responsibility in accordance with DoDM 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information, reference (v).

k. Complying with requirements of DoDM 5220.32 (Vol 1), Section 11: Information Systems (IS) Security, for procurements requiring contractors to process classified information on an IS or to connect to a GCA network

13.6.3 SUPSHIP Responsibilities

Contract administration duties and responsibilities of the SUPSHIP Security Division include:

a. Interfacing as necessary with the DCSA, NAVSEA PCO, NAVSEA Office of Security Programs (SEA 00P), the assigned GCAs, and the shipbuilder to promote an effective and compliant security posture for SUPSHIP-cognizant activities associated with the contract.

b. Per FAR 42.302(a)(21), administering applicable industrial security program requirements when delegated by the PCO.

c. Collaborating with contractor FSOs to establish standard contractor badging and access control procedures for both contractor and Government personnel.

d. Arranging familiarization training to ensure Government personnel understand and comply with access control procedures and that crewmembers accept shipyard badges for designated access.

e. Providing the contractor with security clearance and access authorization for Government personnel accessing the shipyard.

f. Reviewing and approving the contractor's SI 009-72 security plan when contractually invoked by NAVSEA clause C-211-H005 Plant Protection**) or other clause.

g. Except as may be specified by a contract's DD-254, make appropriate notifications to SEA 00P3 and SEA 00P6 when made aware of security incidents involving classified information or CUI, When classified information has been subjected to electronic data spillage, ensure it is retained

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

and provided to the Original Classification Authority via SEA 00P6 for a damage assessment when warranted.

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

Appendix 13-A: Acronyms

ACO	Administrative Contracting Officer
ACP	Access Control Plan
ASM	Activity Security Manager
AT	Anti-Terrorism
ATO	Anti-Terrorism Officer
ATWG	Anti-Terrorism Working Group
C&A	Certification and Accreditation
CAO	Contract Administration Office
CAS	Contract Administration Service
CFR	Code of Federal Regulations
CDRL	Contract Data Requirements List
COMSEC	Communications Security
COR	Contracting Officer’s Representative
CSO	Cognizant Security Office
CUI	Controlled Unclassified Information
CVS	Central Verification System
DCSA	Defense Counterintelligence and Security Agency
DD	Defense Department
DoD	Department of Defense
DoDD	Department of Defense Directive

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

DoDI	Department of Defense Instruction
DoD-R	Department of Defense Regulation
DoN	Department of the Navy
FAR	Federal Acquisition Regulations
FCL	Facility Clearance
FP	Force Protection
FPCON	Force Protection Condition
FPO	Force Protection Officer
FSO	Facility Security Officer
GCA	Government Contracting Activity
IA	Information Assurance
INDUSEC	Industrial Security
IS	Information Systems
ISD	Industrial Security Directorate
ISSM	Information Systems Security Manager
ISP	Information Security Program
IT	Information Technology
KMI	Key Management Infrastructure
MOA	Memorandum of Agreement
NAVSEA	Naval Sea Systems Command
NAVSEAINST	Naval Sea Systems Command Instruction

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

NCAISS	NISP Central Access Information Security System
NISP	National Industrial Security Program
NISS	National Industrial Security System
NISPOM	National Industrial Security Program Operating Manual
NNPI	Navy Nuclear Propulsion Information
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	Chief of Naval Operations Instruction
OPSEC	Operations Security
PCO	Procuring Contracting Officer
PCU	Pre-Commissioning Unit
PEO	Program Executive Officer
PERSEC	Personnel Security
PHYSEC	Physical Security
PM	Program Manager
PPP	Plant Protection Plan
PSI	Personnel Security Investigations
RMC	Regional Maintenance Center
RMF	Risk Management Framework
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCO	Security Contracting Official

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access

SECDEF	Secretary of Defense
SECNAVINST	Secretary of Navy Instruction
SECNAV-M	Secretary of the Navy Manual
SETA	Security, Education, Training and Awareness
SI	Standard Item
SOM	SUPSHIP Operations Manual
SSO	Special Security Officer
SSRAC	Standard Specification for Repairs and Alterations Committee
SUPSHIP	Supervisor of Shipbuilding, Conversion and Repair, USN
TSCO	Top Secret Control Officer
TWG	Threat Working Group
USG	U.S. Government

** Denotes hyperlinks requiring CAC, NMCI, or other restricted access