



---

# **NETWORK SECURITY OFFICER (NSO) GUIDEBOOK**



## **MODULE 08**

### **INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM GUIDELINES**

**THIS PAGE INTENTIONALLY LEFT BLANK**

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer  
Naval Command, Control and Ocean Surveillance Center  
In-Service Engineering East Coast Division  
Code 423  
4600 Marriott Drive  
North Charleston, SC 29406-6504

Commercial: 1-800-304-4636  
E-mail: [subscribe@infosec.nosc.mil](mailto:subscribe@infosec.nosc.mil)

Electronic versions of this document may be downloaded via anonymous ftp from [infosec.nosc.mil](http://infosec.nosc.mil) or the world wide web at <http://infosec.nosc.mil/infosec.html/>

Stocked: Additional copies of NAVSO P-5239-08 can be obtained from the Navy Aviation Supply Office (Code 03415), 5801 Tabor Avenue, Philadelphia, PA 18120-5099, through normal supply channels in accordance with NPFC PUB 2002D, NAVSUP P-437, or NAVSUP P-485, using AUTODIN, DAMES, or MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8235.

Local reproduction is authorized.

**THIS PAGE INTENTIONALLY LEFT BLANK**

## FOREWORD

The Navy Staff Office Publication 5239 (NAVSO P-5239) series, "Information Systems (IS) Security (INFOSEC) Program Guidelines," is issued by the Naval Information Systems Management Center. This series consists of modules providing procedural, technical, administrative, and supplemental guidance for all information systems, whether business or tactical. It applies to ISs used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data. Each module focuses on a distinct program element and describes a standard methodology for planning, implementing, and executing that element of the INFOSEC program within the Department of the Navy (DON). This module, The Network Security Officer (NSO) Guidebook, describes the NSO's roles and responsibilities within the DON INFOSEC program.

Terminology associated with information systems in general, and INFOSEC specifically, varies from Service to Service and from Command to Command. The Automated Data Processing System Security Officer (ADPSSO) from a decade ago is now called an Information System Security Officer (ISSO). With the connectivity of ISs to Local Area Networks (LAN) and Wide Area Networks (WAN), the NSO's role has emerged. Common DON terms for roles are discussed in section 2 of this guidebook.

Organizational differences make it difficult to precisely define discrete roles and responsibilities. Organizations may choose to implement the NSO responsibilities defined in this guidebook differently. The location and size of the activity or Command, as well as the complexity of the information systems and networks, may dictate how the NSO's role is implemented. In large Commands, the security responsibilities defined in this document may be divided among numerous security personnel. Conversely, smaller commands may have a single individual performing all of the functions identified.

This guidebook applies only to classified General Service (GENSER) and/or Sensitive But Unclassified (SBU) ISs. It does not apply to ISs processing Special Compartmented Information, Cryptographic, Cryptologic, Special Access Program, Single Integrated Operation Plan-Extremely Sensitive Information, or North Atlantic Treaty Organization information. Those systems are under the purview of their respective authorities.

During the preparation of this guidebook, several activities were contacted and interviewed for technical inputs. The following security personnel were extremely helpful in providing information and guidance: Commander-in-Chief, U.S. Atlantic Fleet (CINCLANTFLT); Space and Naval Warfare Systems Command (SPAWAR); Naval Sea Systems Command Automated Data System Activity (SEAADSA); Headquarters, U.S. Marine Corps (HQMC); Office of Naval Intelligence (ONI); Naval Security Group (NAVSECGRU); and Naval Command, Control and Ocean Surveillance Center, In-Service Engineering (NISE)-East.

**THIS PAGE INTENTIONALLY LEFT BLANK**

**TABLE OF CONTENTS**

**1.0 INTRODUCTION..... 1**  
 Purpose..... 1  
 Policy and Guidance ..... 1  
 Document Structure..... 1

**2.0 NETWORK SECURITY OFFICER ROLE ..... 3**  
 Defined Roles ..... 3  
 Qualifications and Prerequisites ..... 4  
 Relationships ..... 5

**3.0 NETWORK SECURITY OFFICER RESPONSIBILITIES ..... 8**

**3.1 Security Management ..... 8**

SECURITY POLICY AND PROCEDURES APPLICATION ..... 8  
 Responsibility ..... 8  
 Implementation..... 8  
     Policies and Procedures ..... 8  
     Key Document Development ..... 9  
     User Guidance ..... 9

COORDINATION WITH SECURITY PERSONNEL ..... 10  
 Responsibility ..... 10  
 Implementation..... 10  
     Coordination Tools ..... 10  
     Coordination With the NSM or ISSM ..... 11  
     Coordination With Other NSOs and ISSOs..... 11

COORDINATION WITH THE NETWORK ADMINISTRATOR(S) ..... 11  
 Responsibility ..... 11  
 Implementation..... 11  
     Formal Coordination ..... 11  
     Daily or Routine Coordination ..... 12

POC FOR USERS ..... 12  
 Responsibility ..... 12  
 Implementation..... 13

**3.2 Administrative Functions ..... 14**

ACCOUNTS ADMINISTRATION ..... 14  
 Responsibility ..... 14  
 Implementation..... 14  
     Account Establishment ..... 14  
     Account Termination..... 14

NETWORK ASSET ADMINISTRATION..... 15  
 Responsibility ..... 15  
 Implementation..... 15  
     Security-specific Coordination ..... 15  
     Administrative Coordination ..... 15

**TABLE OF CONTENTS**

Purging, Declassifying, and Downgrading Procedures .....	16
MALICIOUS SOFTWARE CONTROL AND REPORTING .....	16
Responsibility .....	17
Implementation.....	17
Malicious Software Control.....	17
User Guidance .....	17
SECURITY “WATCHDOG” .....	18
Responsibility .....	18
Implementation.....	18
COMPUTER SECURITY TOOLBOX.....	19
Responsibility .....	19
Implementation.....	19
<b>3.3 Training and Awareness .....</b>	<b>21</b>
IS/NETWORK USER SECURITY TRAINING .....	21
Responsibility .....	21
Implementation.....	21
Course Development and Conduct.....	21
Course Curriculum .....	21
Course Attendance .....	23
SECURITY AWARENESS .....	23
Responsibility .....	23
Implementation.....	23
<b>3.4 Physical and Logical Security .....</b>	<b>24</b>
Physical Security .....	24
Logical Security .....	24
PHYSICAL SECURITY .....	25
Responsibility .....	25
Implementation.....	25
Facility Physical Access .....	25
Environmental Hazards Protection.....	25
LOGICAL SECURITY .....	25
Responsibility .....	26
Implementation.....	26
User Identification and Authentication.....	26
Data Control and Protection .....	26
Password Management.....	26
Data Access .....	27
Interconnections and Controls.....	27
<b>3.5 Auditing .....</b>	<b>29</b>
Responsibility .....	29
Implementation.....	29
Monitoring Network Activity .....	29
Vulnerability Checkers .....	30
Intrusion Detection .....	31

## TABLE OF CONTENTS

Password Protection .....	31
Audit Trail Review .....	31
<b>3.6 Incident and Violations Reporting .....</b>	<b>33</b>
Responsibility .....	33
Implementation.....	34
Functions in Support of Reporting Mechanism.....	34
Incident Analysis.....	34
<b>3.7 Risk Management .....</b>	<b>35</b>
RISK MANAGEMENT PROGRAM.....	35
Responsibility.....	35
Implementation.....	35
REVIEW OF RISK ASSESSMENT.....	37
Responsibility.....	37
Implementation.....	37
SECURITY TEST AND EVALUATION.....	38
Responsibility.....	38
Implementation.....	38
<b>3.8 Accreditation .....</b>	<b>40</b>
Responsibility.....	40
Implementation.....	40
<b>3.9 Security Configuration Management .....</b>	<b>41</b>
Responsibility.....	41
Implementation.....	41
Change Review.....	41
Change Management.....	41
Change Testing.....	42
<b>3.10 Contingency Planning .....</b>	<b>43</b>
Responsibility.....	43
Implementation.....	43
<b>3.11 Security Documentation .....</b>	<b>44</b>
System Security Plan.....	44
Security Operating Procedures.....	45
Network Memorandum of Agreement .....	46
Authorized User List .....	46
Training and Awareness Documentation .....	46
IS Incident Report .....	46
Risk Assessment.....	47
ST&E Documentation .....	47
Plan and Procedures .....	47
Checklist.....	47
Report .....	47
Contingency Plan .....	47

NAVSO P-5239-08

MARCH 1996

**TABLE OF CONTENTS**

Appendix A: Security Policy, Procedure, and Guidance  
Documentation.....A-1

## 1.0 INTRODUCTION

Technological progress and growth in information systems (IS) have increased information transfer, processing, and storage capabilities worldwide. These advances have also increased the risk of exploitation by accidental exposure and malicious threat agents. Information Systems Security (INFOSEC) is the discipline that provides an integrated and systematic approach to the security of all aspects of ISs. In implementing INFOSEC, the Navy has developed the Navy Staff Office Publication (NAVSO P-5239) series of documents to increase personnel understanding and awareness of INFOSEC requirements among IS sponsors, developers, and users, and to reduce risk in ISs to acceptable levels. NAVSO P-5239-01, Introduction to Information Systems Security, explains INFOSEC implementation. NAVSO P-5239-02, Terms, Abbreviations, and Acronyms, defines terms used within this document.

---

<b>Purpose</b>	This guidebook is a module within the NAVSO P-5239 series of documents that has been developed to assist in planning and operating ISs and to help system users maintain INFOSEC awareness. This guidebook provides guidance and direction to current, new, and prospective Network Security Officers (NSO) in implementing INFOSEC programs. Specifically, it describes NSO responsibilities and provides instruction for implementing them.
----------------	---

---

<b>Policy and Guidance</b>	Module NAVSO P-5239-08 was developed in accordance with Department of Defense (DOD) and Department of the Navy (DON) policy. Appendix A provides a bibliography of security policy, procedure, and guidance documentation.
----------------------------	--

---

<b>Document Structure</b>	Section 2.0 briefly describes the NSO's role, qualifications and prerequisites, and working relationships. Section 3 describes the NSO's responsibilities, organized in 11 task areas. The first task area, Security Management, can be considered an umbrella over the remaining 10 task areas. Specifically, the performance or conduct of the other 10 task areas is planned, coordinated, and facilitated under this overall management function. The 11 tasks areas are
---------------------------	--

- Security Management
  - Administrative Functions
  - Training and Awareness
- 
- Physical and Logical Security
-

- 
- Auditing
  - Incident and Violations Reporting
  - Risk Management
  - Accreditation
  - Security Configuration Management
  - Contingency Planning
  - Security Documentation.
-

## **2.0 NETWORK SECURITY OFFICER ROLE**

The NSO is formally appointed in writing by the program manager of a specific branch, division, or department, as appropriate, based on the structure and needs of the specific Command or activity. The Network Security Manager (NSM) or Information System Security Manager (ISSM) provides input to the program manager regarding the appointment decision. If requested, the NSM or ISSM may provide technical assistance in developing appointment memorandums or letters. The NSO appointment letter briefly summarizes the NSO's duties and responsibilities. Depending on the Command structure, more than one NSO may be appointed. Commands having complex network systems may need more NSOs to perform day-to-day activities and to respond to security problems and network user needs. For example,

- Multiple NSOs may be assigned to a single, large network system
- Site-specific NSOs may be assigned for geographically distributed nodes of a network system
- A single NSO may be assigned within a Command for multiple network systems.

The NSO is responsible for implementing and maintaining network security on behalf of the NSM or ISSM. The NSO reports to the Command's NSM and implements the overall INFOSEC program approved by the Designated Approving Authority (DAA). In Commands that do not have designated NSMs, the NSO(s) reports to the designated ISSM(s).

---

### **Defined Roles**

The NSO is responsible for the following:

- Ensuring that standard security procedures and measures that support the security of the entire network are developed and implemented, to include all network components such as fax machines and modem pools (see sections 3.1, 3.2, and 3.11)
  - Ensuring that network security procedures are being followed by all personnel having access to the network (see sections 3.1 through 3.10)
  - Reporting the security status of the network to the NSM or ISSM (see sections 3.1 through 3.10)
  - Ensuring that TEMPEST features on network hardware have not been altered (see section 3.2)
  - Ensuring that all networked computers display access warning banners (see sections 3.2 and 3.3)
  - Ensuring the accountability and protection of network assets (see sections 3.2 and 3.4)
  - Conducting user training and awareness activities as directed by the NSM or ISSM (see section 3.3)
-

- 
- Performing network audits on NSM/ISSM-selected security events and reviewing network audit reports (see section 3.5)
  - Creating a network security incident reporting mechanism and reporting incidents to the NSM or ISSM when the network is compromised (see sections 3.6 and 3.11)
  - Initiating protective or corrective measures if a security problem is discovered (see section 3.6)
  - Performing risk management activities under the direction of the NSM or ISSM (see sections 3.7 and 3.11)
  - Participating in network penetration testing periodically (see section 3.7)
  - Ensuring that the network is accredited (see section 3.8)
  - Reviewing network configuration modifications to ensure that network security is not degraded (see section 3.9)
  - Ensuring that network security is included in all contingency plans, and that the contingency plans are tested periodically (see sections 3.10 and 3.11).
- 

**Qualifications and Prerequisites**

No specific formal college or other degree program is required for the NSO. However, extensive experience in INFOSEC, combined with a strong technical background in computer science, mathematics, engineering, or a related field, is extremely beneficial. This technical background must be balanced with effective communications and interpersonal skills because the NSO must associate with people at all levels of the organization. An NSO should meet the following criteria:

- Two years of experience in a computer-related field
- One year of working experience in INFOSEC
- Two years of network operating experience
- Education and training in computer science, mathematics, electrical engineering, and related fields
- Periodic attendance at appropriate-level INFOSEC training courses.

The NSO's security education and work experience should provide familiarity with all aspects of INFOSEC. Security training includes DOD and DON security courses, (e.g., Introduction to Computer Security or equivalent courses) and any available Command-specific training including computer-based training [CBT]. NSOs must also recognize that the network security profession changes

---

---

as rapidly as new technologies. NSOs must make efforts to keep up with emerging technologies and threats. NSOs can access information on new threats and network security techniques at a number of Internet security advisory homepages.

*Reference:* For more information on resources available to NSOs, see section 3.6, Incident and Violations Reporting.

---

## **Relationships**

In executing security responsibilities, the NSO interacts with personnel within and external to the site security organization. This section defines those interfaces and presents a uniform set of security roles and titles that are used throughout this guidebook and throughout the NAVSO P-5239 series.

---

### **Personnel/Activity**

### **INFOSEC Role**

DAA

The DAA is responsible for ensuring compliance with the DON INFOSEC Program for the activities and networks/ISs under the DAA's jurisdiction. The DAA grants interim and final approval to operate a network/IS in a specific security mode based on a review of the accreditation documentation and a confirmation that the residual risk is within acceptable limits.

NSM

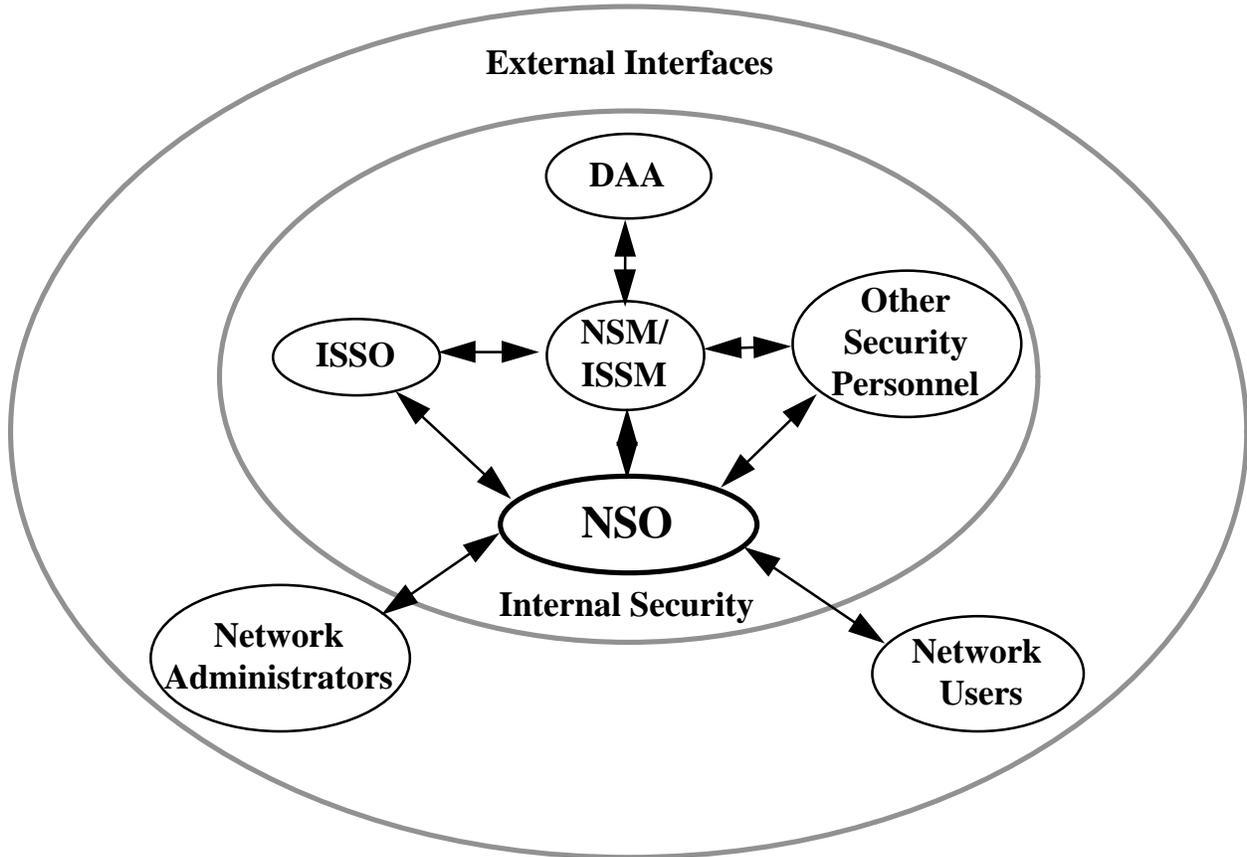
The NSM is responsible for the overall security operation of the network and is the focal point for policy, guidance, and assistance in security matters. The NSM ensures that the network complies with the requirements for interconnecting to external systems or networks. Depending on the size of the activity, geographical distribution, and complexity of the site, the NSM role may be performed by the ISSM. The NSO reports to the NSM or ISSM for INFOSEC matters and may report to another authority for collateral duties.

ISSM

The ISSM acts as the focal point for all security matters pertaining to the IS(s) under his or her purview. The ISSM is responsible for ensuring that the INFOSEC program requirements are met. The ISSM accomplishes this by performing, directing, coordinating, administering, and overseeing various activities and personnel. The NSO reports to the ISSM for INFOSEC matters when there is not an NSM designated.

ISSO	<p>The Information System Security Officer (ISSO) acts on behalf of the ISSM to implement the security policy of an IS(s) and acts as the immediate point of contact for all INFOSEC matters. In many cases, the roles and responsibilities of the ISSO and NSO overlap. Often, the NSO performs duties similar to those of an ISSO. Therefore, the NSO should work closely with the ISSO (or ISSOs) to ensure that security policies are applied and enforced uniformly. In Commands that do not have designated NSOs, the network-specific responsibilities are performed by the ISSO.</p>
Other Site Security Personnel	<p>Other security-related billets exist depending on the structure and size of the Command or Activity. A Site Security Manager, the principal advisor on information and personnel security in the Command, is responsible to the Commanding Officer for the management of the overall security program. Physical and Personnel Security Officers may also be designated. The NSO coordinates with other security personnel to ensure the consistent implementation of security policies and procedures.</p>
User	<p>In this document, the term “user” refers to all personnel (i.e., users, operators, and maintainers) who access the IS or network for authorized purposes. The NSO ensures that network users are aware of their security responsibilities and trained to understand and use network security features.</p>
Network Administrator	<p>The Network Administrator is responsible for the administration and operation of a network and works with the NSO to ensure the network operates in accordance with Command security policies and procedures. The Network Administrator may also be the NSO for his or her particular network.</p>

Figure 1 illustrates the relationship of the NSO with security and nonsecurity personnel.



**Figure 1**  
**NSO Relationships to Personnel**

### **3.0 NETWORK SECURITY OFFICER RESPONSIBILITIES**

The NSO is responsible for ensuring that users comply with the INFOSEC program requirements and procedures. The NSO accomplishes this by managing various activities and personnel. This section defines the NSO's responsibilities in each task area previously identified.

#### **3.1 Security Management**

This section describes the responsibilities of the NSO within the overall task area of management, which is the umbrella covering the other 10 task areas. It focuses specifically on planning and coordinating tasks required for an effective network INFOSEC program. These planning and coordination tasks are broken into the following areas: security policy and procedures application, coordination with security personnel, coordination with Network Administrators, and point of contact (POC) for users.

### **SECURITY POLICY AND PROCEDURES APPLICATION**

<b>Responsibility</b>	The NSO maintains a thorough understanding of security policy and procedures applicable to the specific network. If required, the NSM, ISSM, or higher authority clarifies the application of INFOSEC policy and procedures. The NSO disseminates network INFOSEC policies and procedures to network users and ensures that users abide by these policies and procedures.
-----------------------	---

#### **Implementation**

<b>Policies and Procedures</b>	The NSO researches and analyzes current DOD, DON, and any Command-level directives, guidelines, regulations, and policies that address network security and that apply to his or her specific Command or Activity (e.g., that discuss DOD/DON roles, telecommunications issues, firewall implementation, and other Command-specific guidance for safeguarding information). This ensures that the NSO is aware of and abides by applicable security requirements. As guided by the NSM or ISSM, the NSO applies knowledge of DOD and DON policies by participating in the development of key network-specific documentation (discussed below). Additionally, the NSO reviews site- and/or system-specific technical documentation, such as the Trusted Facility Manuals
--------------------------------	---

(TFM) and the Security Features User's Guides (SFUG). The NSO

---

may be delegated to provide input to the update of the TFMs and SFUGs or other site- or system-specific security documentation.

---

**Key Document Development**

The NSO provides input to the ISSO(s) for the development of System Security Plans (SSP) for every DON IS under his or her cognizance. The NSO may also be tasked to assist the ISSO(s) in developing of site-specific Security Operating Procedures (SOP).

The NSO is responsible for developing appropriate network-related Memorandums of Agreement (MOA), also referred to as Memorandums of Understanding (MOU), and Memorandums of Record (MOR). A MOA establishes the security roles and requirements that must be enforced by each connecting network. For networks that connect to other networks that are under the purview of different DAAs, an MOA is developed with the other DAA. The MOA identifies the required confidentiality, integrity, and availability services and constraints under which the connected systems can operate, including data sensitivity, user authorization, and physical and system configuration. An MOR is used when connecting networks have the same DAA. The time required to coordinate with the necessary parties must be factored into the schedule for activating the network. The time required varies with activities and Commands.

---

**User Guidance**

The NSO provides guidance and oversight to network users in interpreting and implementing security policies and procedures through training and awareness activities and by providing one-on-one guidance and direction on an as-needed, as-required basis. The NSO also supervises network user work practices to ensure that policies and procedures are followed correctly.

*Reference:* Security policy, procedure, and guidance documentation is identified in Appendix A. For more information concerning the SFUG and TFM, see NCSC-TG-026 and 016 (of what is commonly referred to as the “rainbow series”), respectively. For more information concerning SSPs and SOPs, see section 3.11, Security Documentation. For more information concerning MOAs and MORs, see NCSC-TG-011, version 1, Trusted Network Interpretation Environment Guideline. For more

information concerning the NSO’s role regarding network users, see below (this section), POC for Users, and section 3.3, Training and Awareness.

---

## **COORDINATION WITH SECURITY PERSONNEL**

---

**Responsibility** The NSO coordinates with security personnel (including NSMs/ISSMs, ISSOs, other NSOs, and personnel in other security departments within the Command, such as personnel, physical, industrial, and operations) to ensure that security policies and procedures are uniformly implemented.

---

### **Implementation**

**Coordination Tools** The NSO participates in security status meetings to keep informed of all activities, problems, and issues relevant to network security in their network and in networks and systems to which their network interfaces. Additionally, they report network INFOSEC activities that impact other security functions. These meetings focus on such topics as:

- Implementation of new Command security policies and procedures
- Security violations
- New network connections and connection terminations
- Hostile or malicious software use
- Network accreditation status (including security test and evaluation [ST&E] and risk assessment results)
- New procedures required to access a particular system
- Configuration control
- Command reorganizations
- Needed and/or new security services.

The NSO will also formally coordinate activities among security departments through internal memorandums or their electronic equivalent.

---

**Coordination With  
the NSM or ISSM**

The NSO interacts regularly with the NSM or ISSM to:

- Report status concerning NSO work efforts
  - Seek guidance concerning work activities, problems, and issues
  - Provide input to security documentation, such as risk assessments and accreditation documentation
  - Receive input on documentation developed primarily by the NSO, such as MOAs and Incident Reports.
- 

**Coordination With  
Other NSOs and  
ISSOs**

As discussed in section 2.0, some Commands may have multiple NSOs and/or ISSOs. In these instances, coordination among NSOs and ISSOs is necessary to ensure the consistent implementation of Command policies and procedures. This coordination and cooperation may take the form of meetings and memorandums or through informal exchanges, depending on the Command structure and preference.

*Reference:* See sections 3.2, Administrative Functions; 3.4, Physical and Logical Security; and 3.6, Incident and Violations Reporting.

---

**COORDINATION WITH THE NETWORK ADMINISTRATOR(S)**

---

**Responsibility**

The NSO coordinates with Network Administrators to ensure that network operation and administration is in accordance with Command INFOSEC policies and procedures. Coordination with Network Administrators is of utmost importance because they are responsible for maintaining the operation of the network.

---

**Implementation**

**Formal Coordination**

The NSO participates in periodic status meetings with Network Administrators to stay apprised of all activities affecting network INFOSEC. To avoid excess meetings, Network Administrators may be invited to attend internal security meetings (discussed previously) as applicable (i.e., information relevant to network administration is discussed). The meetings will focus on such topics as:

- Proposed changes to the network
-

- 
- Proper implementation of changes
  - User status
  - Recent computer virus attacks and actions required to combat them
  - New policy and procedures implementation
  - Network problems and issues relating to INFOSEC
  - Network contingency plans
  - Network security test schedules.
- 

**Daily or Routine Coordination**

On a daily or otherwise routine basis, the NSO coordinates with network administration staff to follow through on meeting action items and to coordinate routine operations, including the following activities:

- Coordinating the addition of new user network accounts and the termination of network accounts
- Coordinating actions required for incidents and violations (e.g., virus management and reporting)
- Coordinating and overseeing the implementation of NSM/ISSM/DAA-approved network changes and changes in security operating procedures
- Ensuring that network backups are performed regularly
- Coordinating and overseeing the implementation of purging and clearing requirements
- Coordinating network audit trail review efforts
- Coordinating or providing input to miscellaneous administrative tasks relating to network security.

*Reference:* See sections 3.2, Administrative Functions; 3.4, Physical and Logical Security; and 3.6, Incident and Violations Reporting. Also see NAVSO P-5239-26, Remanance Security Guidebook.

---

**POC FOR USERS**

---

**Responsibility**

The NSO provides assistance and direction to users regarding network security matters, questions, and problems.

---

**Implementation**

The NSO is responsible for the following actions:

- Assisting in user training (if delegated by the NSM or ISSM) and ensuring that users are aware of, understand, and correctly implement all network INFOSEC procedures
- Instructing and providing guidance to users concerning the actions necessary for reporting suspected incidents and violations
- Ensuring that users do not make changes to the network (e.g., new or replacement software, network connection changes, relocating network components, adding modems, and changing the classification of network/components thereof) without prior approval from the NSO
- Ensuring that a departing user's account and access to the network are terminated
- Notifying the Judge Advocate General (JAG) or legal department if there is any evidence of tampering, and coordinating with the JAG or legal department before conducting any investigation beyond that which revealed a possible violation.

*Reference:* For more information, see section 3.2, Administrative Functions, section 3.3, Training and Awareness, section 3.6, Incident and Violations Reporting, and section 3.9, Security Configuration Management.

---

### 3.2 Administrative Functions

The NSO, in conjunction with the Network Administrator, performs a variety of administrative tasks related to the network. The activities within the administrative functional area range from ensuring that network accounts are opened, maintained, and closed correctly to protecting the network and its information.

---

#### ACCOUNTS ADMINISTRATION

---

**Responsibility** The NSO ensures that network user accounts are established and terminated in accordance with Command network policies.

---

#### Implementation

**Account Establishment** The NSO is responsible for ensuring that the security of the network is not jeopardized when user accounts are added to the network. The NSO:

- Works with the Command's personnel security department to maintain an accurate and up-to-date record of personnel clearances (whenever possible, use read-only access to personnel security databases to avoid replication of existing databases)
- Validates, with department heads or supervisors, the access requirements of prospective users to ensure that access is granted only to information needed for work performance
- Coordinates with Network Administrators to open new accounts and verifies that new accounts are added correctly
- Ensures that new users are trained in applicable network INFOSEC requirements, responsibilities, and procedures.

#### Account Termination

The NSO ensures the expeditious closure and termination of network accounts of departing personnel. The NSO:

- Coordinates with the Command's physical and personnel security departments to delete users from authorized area access lists, network authorized user lists, and electronic mail groups
- Coordinates with the Command's physical and personnel security departments to ensure that all physical access materials

---

(e.g., tokens and cards) are accounted for before user departure

---

---

from the activity

- Coordinates with the Network Administrators to ensure that the user's data is disposed of in accordance with user management direction, that the account is closed, and that all magnetic media and software are returned.

*Reference:* For more information, see section 3.3, Training and Awareness, and section 3.4, Physical and Logical Security.

---

## NETWORK ASSET ADMINISTRATION

---

### **Responsibility**

The NSO ensures the accountability and protection of network media resources (hardware, software [applications and associated support files], and firmware) against misuse and destruction caused by human error, malicious intent, or natural hazard.

---

### **Implementation**

#### **Security-specific Coordination**

The NSO coordinates with other cognizant security departments (e.g., document control, physical) for handling, storing, disposing of, and marking classified components, software, and documentation to ensure consistency in implementing Command policies and procedures.

#### **Administrative Coordination**

The NSO coordinates with the Network Administrators for controlling network media resources and maintaining an inventory of network components. Based on Command policy, where appropriate, the NSO:

- Provides guidance to the Network Administrators regarding the protection of network media resources, such as
  - Securing classified components, software, and other material
  - Preventing unauthorized access to the network
  - Preventing damage of network equipment caused by natural hazards (e.g., water, fire, extreme temperatures)
- Ensures that Network Administrators perform regular, total-network (or subsystems thereof) backups

- 
- Ensures that periodic copies of mission-critical file backups are
-

---

rotated to secure off-site locations

- Reviews the Network Administrator-developed inventory list regularly to keep abreast of network component changes or relocation
  - Reviews network change plans (e.g., new network connections or disconnections, software upgrades, and disposal of components) and provides guidance regarding the implementation of changes
  - Ensures that maintenance personnel do not alter TEMPEST characteristics of applicable network equipment and have been granted only those privileges required to perform maintenance
  - Verifies that no unauthorized equipment is attached to the network (i.e., walk-through actual cabling of the network or on-line monitoring equipment)
  - Verifies that there are no unapproved modems on the network
  - Verifies that no user system is acting as a bridge to disparate networks.
- 

**Purging, Declassifying,  
and Downgrading  
Procedures**

The NSO coordinates with the Network Administrators and cognizant security department(s) to develop and implement purging, clearing, and media labeling procedures. The NSO ensures that purging technology is available as necessary to sanitize system components. This technology includes FLUSH and BUSTER from the Computer Security Toolbox.

*Reference:* For more information, see sections 3.3, Training and Awareness; 3.4, Physical and Logical Security; and 3.9, Security Configuration Management. For more information concerning classifying and safeguarding classified information (e.g., marking and handling of media resources, declassification/downgrading and upgrading of classified components, destruction of classified material), see OPNAVINST 5510.1H. NAVSO P-5239-26, Remanence Security Guidebook, provides policy, guidelines, and procedures for clearing and purging IS memory and other storage media. NSA's Information Systems Security Products and Services Catalogue Supplement provides the NSA Degausser Products List that details the different degausser types, application of these degaussers, and manufacturer information. For more information on FLUSH and BUSTER, see the Computer Security Toolbox subsection at the end of this section.

---

**MALICIOUS SOFTWARE CONTROL AND REPORTING**

---

<b>Responsibility</b>	The NSO ensures that proper measures are taken to protect the network from computer viruses and other malicious software.
<b>Implementation</b>	The NSO works with the ISSO(s) and Network Administrators to implement DON-approved software to protect the network against viruses and other malicious software. This includes using VKIT from the Computer Security Toolbox to create and distribute virus scanner disks and utilities.
<b>Malicious Software Control</b>	The NSO works with the ISSO(s) and Network Administrators to implement procedures for reporting actual or suspected incidents of malicious software use and for performing periodic malicious software/virus checks. This reporting mechanism ensures that virus attacks are expeditiously dealt with and reported by the NSM or ISSM to the Naval Incident Response Team (NAVCIRT) (which is a component of the Fleet Information Warfare Center [FIWC]). Suspected virus attacks should be reported to NAVCIRT at (800) 628-8893 or E-mail: <i>navcirt@fiwc.navy.mil</i> .
<b>User Guidance</b>	<p>The NSO ensures that network user training sessions include discussion of malicious software, which covers the following topics:</p> <ul style="list-style-type: none"><li>• The dangers of computer viruses and other malicious software, how they are spread or transmitted, and what they affect</li><li>• Types of network occurrences that imply possible virus or malicious software</li><li>• Malicious software protection methods, for example:<ul style="list-style-type: none"><li>- Using automated virus detection tools</li><li>- Using authorized software only</li><li>- Installing only “safe” software (scanned for malicious software)</li><li>- Storing virus-free, write-protected backup disk copies of vital executable programs and operating software</li><li>- Performing regular backups</li><li>- Preventing unauthorized access to network</li></ul></li><li>• Malicious software reporting procedures</li><li>• Virus attack process<ul style="list-style-type: none"><li>- Tracking a virus (determining origin and type, who or what has been affected)</li><li>- Providing cleanup (who conducts, estimated downtime,</li></ul></li></ul>

---

reinstallation of software).

*Reference:* For virus reporting procedures, see section 3.6, Incident and Violation Reporting. Also see NAVSO P-5239-19, Computer Incident Response Guidebook.

---

## SECURITY “WATCHDOG”

---

### Responsibility

The NSO monitors network use and conducts random floor and network component checks to ensure that Command INFOSEC policies and procedures are followed.

---

### Implementation

When conducting floor checks, the NSO should be watchful of the following:

- Are SOPs and other Command-specific policies and procedures being adhered to?
  - Does the network configuration match the documented configuration?
  - Is virus scanning software consistently used?
  - Are computers left in the “active” mode (users logged on), leaving the network vulnerable to misuse?
  - Are network log-on warning banners at every entry point and are user consent-to-monitoring forms signed in accordance with current, applicable DON policy?
  - Are unauthorized persons using the network?
  - Are monitors positioned to effectively limit unauthorized viewing?
  - Are users running or storing unauthorized software, especially games, on their workstations?
  - Are personnel following procedures when using classified networks?
    - Are physical administrative security measures being followed?
    - Are workstations disconnected from networks and/or peripherals that are not approved for classified processing?
    - Are classified operating system and applications software and data files secured after use?
    - Is classified material in the possession of cleared and authorized personnel at all times when not in an authorized
-

---

security container or vault?

- Are audit trail logs being maintained?
- Are classified media properly marked (to include magnetic media and network hardware components)?

The NSO reports violations and incidents through the proper channels (i.e., through the NSM or ISSM) to the DAA for determination of necessary action.

*Reference:* For more information, see sections 3.5, Auditing, and 3.6, Incident and Violation Reporting.

---

## COMPUTER SECURITY TOOLBOX

---

### **Responsibility**

The NSO ensures adequate control, dissemination, and use of the DON Computer Security Toolbox, a set of automated software programs (tools), used for performing various security functions. The Toolbox aids in complying with Controlled Access Requirements (CAP) requirements. The Toolbox was prepared by the Naval Command, Control and Ocean Surveillance Center, In-Service Engineering, East Coast Division (NISE-East CHARLESTON, SC) and the Air Force Intelligence Command (AFIC).

---

### **Implementation**

The NSO aids the user in implementing the Toolbox. These tools range from password-generating programs to tools to eliminate "object reuse" issues faced by MS-DOS users. The Toolbox consists of the following:

- **TOOLBOX:** The TOOLBOX program, the controlling program for the Computer Security Toolbox, creates a user-friendly interface for selecting a program or help function in the "Toolbox." When an item has been selected, TOOLBOX creates the command line options required to execute the particular program.
  - **FLUSH:** FLUSH satisfies the object reuse CAP requirement by eliminating appended data from the target diskette. First, it overwrites the appended data within each file from the end-of-file marker to the absolute end of file by sector orientation. Then, it overwrites all unallocated space on the remainder of the diskette. This last action will overwrite all files that may have been previously deleted from the diskette by using the MS-DOS "Delete" Command. FLUSH can be used for clearing, but not for
-

- purging, diskettes.
- **SCOPY:** SECURE COPY eliminates all forms of appended data from the source disk or diskette while copying files to the target disk or diskette. SCOPY works differently from FLUSH in that it copies from one disk to another disk. FLUSH performs all of its action on a single diskette. For security purposes, SCOPY should be used on all applications to transfer files from a source disk or diskette to a target disk or diskette.
  - **BUSTER:** Just like paper, floppy disks can be incorrectly classified by the originator or more importantly, floppy disks may contain hidden classified information or files. The person generating the data or information must ensure that the outgoing diskette is properly classified. To assist in this function, BUSTER unconditionally reads all hard sectors of a diskette while checking each word found against the "LIMITS.TXT" file. LIMITS.TXT, which may be edited using any editor, contains one word or phrase per line. Typically, it contains all the paragraph markings used in classified documents. These markings may be spelled out completely or abbreviated. Additionally, project covert terms, covernames, nicknames, special category (SPECAT) codewords, etc., may be entered into LIMITS.TXT. When a match occurs, the program pauses to review the "matched" item(s).
  - **VKIT:** The Virus Kit (VKIT) Generation process can be used to create a virus scanning disk. VKIT will copy the essential virus scanning files to a single disk, which can then be used to check systems throughout the command.
  - **PASSGEN:** The PASSGEN program randomly generates pronounceable passwords. PASSGEN, through a complex set of grammar rules, generates passwords that should not be found in the dictionary, but are structured such that they can be pronounced like real words.

*Reference:* All inquiries about the Computer Security Toolbox should be directed via the NSM or ISSM to NAVCIRT (navcirt@nosc.mil or

1-800-628-8893). For additional information on controlled access requirements, see NAVSO P-5239-15, Controlled Access Protection (CAP) Guidebook.

---

### 3.3 Training and Awareness

The NSO receives role/Command-specific security training from the NSM or ISSM and attends DOD- and DON-level security training, such as the DON Introduction to Computer Security Program Course offered by the Naval Computer and Telecommunications Command, the DOD Computer Institute Information Resource Protection Course, the Computer Security Specialist Course offered by the USMC Computer Sciences School, and National Institute of Standards and Technology/National Computer Security Center National Information System Security Conferences. Additional Navy INFOSEC workshops and training are available periodically that address current issues, including Internet policy and implementation of firewalls. INFOSEC workshops and course offerings are publicized through Navy home pages and newsletters distributed via the world wide web.

If delegated, the NSO assists in user training and awareness activities under the direction of the NSM or ISSM.

---

#### IS/NETWORK USER SECURITY TRAINING

---

**Responsibility** In accordance with the Computer Security Act of 1987, all IS and network users must receive periodic security training. If delegated by the NSM or ISSM, the NSO participates in developing user training curriculum and assists in conducting user training sessions.

---

#### Implementation

**Course Development and Conduct** Formal training sessions should be developed using a briefing-style format with hands-on demonstrations. Written guidelines, handbooks, or hard copies of the briefing should be provided to, and retained by, attendees for reference purposes. Softcopy versions of documents on removable computer media can be a cost effective substitute for hardcopy versions. The Command may use CBT, if available and applicable.

---

**Course Curriculum** The training curriculum should be tailored to the specific Command and IS or network. A sample training briefing outline may include the following:

- Value of IS-based information
    - Historical data
-

- Personnel files, payroll data, and legal records
  - Trade secrets/proprietary data
  - Documentation vital to national security
  - Communication vulnerabilities
    - Human errors
    - Misuse of the system or network (e.g., procedures not followed, data used for illegal purposes, “browsing”)
    - Computer viruses
    - Internet security risks
    - Unauthorized use (e.g., hackers using networks to steal information)
    - Natural hazards (e.g., fire, smoke, static electricity, extreme temperatures, humidity, and magnetic forces)
  - Basic safe computing
    - Maintaining established network configuration
    - Accessing data (use only data/software/systems needed for particular job)
    - Warning banners/screens
    - Using keyboard or system locks
    - Leaving computers unattended
    - Disposing of unneeded data
    - Handling of sensitive information
    - Backing up data
    - Using unauthorized software
    - Explanation of classified and sensitive unclassified data
    - Explanation of the differences between classified and unclassified networks and the application of each
    - Protecting software
    - Using modems
    - Interface awareness
  - Password management
    - Generating unique passwords
    - Protecting passwords (i.e., confidentiality)
    - Changing passwords
  - Command-specific security procedures and issues
    - Using security products (e.g., safes, cipher locks, burn bags, and classified disks)
    - Relocating network components
    - Changing network software and hardware
  - Reporting security violations/suspected violations (e.g., who to contact; reporting process)
  - Using networked games, homepages, shared files, etc.
  - Explanation and demonstration of security mechanisms and
-

---

safeguards on the IS or network

- Importance of self-monitoring (e.g., identify successful and unsuccessful logons to aid in monitoring attempts by unauthorized personnel to access the system or network)
  - Importance of being alert to suspicious or unusual activity
  - Current telecommunications security issues (e.g., encryption, vulnerabilities inherent with communicating over a frame relay network compared to using a dedicated leased line, Integrated Services Digital Network [ISDN], and Asynchronous Transfer Mode [ATM]).
- 

**Course Attendance**

Training attendees should be required to sign attendance sheets that acknowledge their role in protecting IS and network assets. These attendance sheets should be checked against employee rosters to ensure that all employees have attended the applicable training.

---

**SECURITY AWARENESS**

---

**Responsibility**

The NSO assists the NSM or ISSM in fostering user security awareness.

---

**Implementation**

The following commonly used approaches heighten user security awareness:

- Develop and distribute security awareness posters
  - Display warning banners or messages on the network (in accordance with current, applicable DON policy) to ensure that users are aware that all activity on the network can be monitored
  - Disseminate new security information and security reminders through memorandums, newsletters, and automated bulletin boards
  - Provide hands-on demonstrations of network INFOSEC features and procedures.
-

### 3.4 Physical and Logical Security

This section describes the NSO's roles and responsibilities in the physical and logical protection of network assets.

---

#### Physical Security

Physical security is the protection and preservation of information and physical and human assets through the reduction of exposure to various threats that can produce a disruption or denial of network services or unauthorized disclosure. The effectiveness of all technical safeguards is based on the assumption, either explicit or implicit, that all segments on the network have adequate physical security protection. Physical security measures are protections against loss or damage from sources such as:

- Intruders
- Vandals
- Environmental hazards (e.g., fire, flood/water, and extreme temperatures)
- Accidents.

Physical security measures implemented depend on the site-specific environment, classification level of the data being handled by the network, and clearance levels of users in the facility.

---

#### Logical Security

Logical security is the protection of network resources, data, and information from unauthorized disclosure, use and tampering. Logical security measures include measures such as:

- User identification and authentication
  - Data control and protection
  - Network interconnection limitations and controls
  - Firewalls.
- 

The NSO ensures that physical and logical access controls are in place and that the network is adequately protected against natural hazards. The NSO's primary focus is on systemic (logical) security measures.

---

## PHYSICAL SECURITY

---

**Responsibility** The NSO ensures that procedures are implemented to deny access to unauthorized users, customers, or visitors. *Note:* While the NSO may not perform these specific physical security activities, coordination with other security departments such as physical, operations, personnel, etc., is necessary to ensure safeguards are in place.

---

### Implementation

**Facility Physical  
Access**

The NSO is responsible for the following actions:

- Ensuring that Authorized User Lists are posted at entrances and continually updated
  - Ensuring that restricted area or authorized personnel only signs are appropriately posted, if required
  - Ensuring that persons entering and exiting the facility are tracked (especially after hours of normal operation)
  - Providing input to the security manager for the development and maintenance of a facility security plan (with architectural drawings and building plans, floor plans, and inventories)
  - Ensuring that maintenance contractors are supervised by authorized personnel
  - Ensuring that locks, bars, and other physical safeguards are sufficient and in place as required by command policy (to include the routine changing of locks and combinations in accordance with Command policies and security operating procedures)
- 

**Environmental  
Hazards Protection**

At a minimum, the NSO works with the physical security and facility maintenance/public works personnel to ensure the following:

- Fire and smoke detection (alarms) and suppression equipment (e.g., fire extinguishers and sprinkler systems) are in place and operational
  - Sufficient quantities of plastic sheeting are available to protect equipment from water damage
  - Temperature and humidity controls are in place and operational.
- 

## LOGICAL SECURITY

---

**Responsibility**            The NSO implements Command policies and procedures to protect the network from unauthorized use.

---

**Implementation**

**User Identification and Authentication**            The NSO works with the personnel security department to maintain an accurate list of authorized network users. This list contains the user name, user identifier, access level, and whether the user has administrator privileges.

---

**Data Control and Protection**            The NSO ensures that identification and authentication (I&A) services record all connections and connection attempts. The I&A services must be tamperproof to protect network integrity.

---

**Password Management**            The NSO ensures that authentication services are in place to handle the weaknesses of traditional passwords. The NSO provides guidance to network users for developing and using unique, nondictionary passwords. The NSO guides users to:

- Choose unique passwords (avoid birth dates and common names)
- Keep passwords confidential at all times
- Memorize passwords (ensure that they are inaccessible by other users)
- Change passwords periodically, in accordance with Command policy, or immediately upon suspected compromise
- Notify the NSO if a password does not work or if unauthorized use is suspected.

The NSO utilizes password utilities, such as *crack*, to identify inadequate passwords and notify users to change their passwords. *Crack* is a password guessing utility that helps NSOs ensure that users are choosing passwords that are difficult to guess and that meet Command policy standards. Using automated password generators, such as PASSGEN, from the Computer Security Toolbox, is also encouraged.

*Reference:* For password management guidelines, see National Computer Security Center document CSC-STD-002-85, "Department of Defense Password Management Guideline," dated 12 April 1985.

---

**Data Access**

The NSO ensures that procedures are in place to:

- Define site-specific discretionary access control (DAC) and mandatory access control (MAC) policies. The policies should define the standards and regulations that the NSO must implement to ensure that data is disclosed only to authorized individuals.
- Control access to all functions that affect security or integrity of the network. Access of this type should be limited to a minimum number of personnel.
- Manage access control software installation and operation in a manner that supports the network security policy, such as
  - Tripwire, which monitors a designated set of files for any changes and can notify NSOs of corrupted or tampered files
  - COPS, which checks for network weaknesses
  - System Administrator Tool for Analyzing Networks (SATAN), which employs network intrusion to analyze system vulnerabilities and provides tutorials on how to fix the problems it uncovers.

---

**Interconnections  
and Controls**

If the network connects with another network, the NSO ensures that the following objectives are met:

- Procedures are established and implemented to control the connection and disconnection of components to the network
  - The systems have permission to connect
    - All affected organizations must establish a MOA
    - All security requirements specified in the MOAs must be implemented
  - Separately accredited networks connected to the subject network operate in a manner consistent with the subject security policy and mode of operation
  - No connection is made to a nonaccredited network without DAA approval and the following:
    - Effective means for ensuring that users cannot access network assets
    - A process that enforces review of all material before it is passed on and prevents material from being passed on if rejected
    - Safeguards to prevent the unintentional release of classified
-

---

information

- Safeguards to avoid the introduction of malicious code
- Safeguards to control secondary connections to other networks
- Procedural controls to prevent users from accidentally, or purposely circumventing technical controls.

*Reference:* For more information concerning MOAs, see section 3.11, Security Documentation, and NCSC-TG-011, version 1, Trusted Network Interpretation Environment Guideline.

---

### 3.5 Auditing

Practices that are inconsistent with the security policy of the network must be identified and eliminated. Monitoring the security activities of the network and conducting an audit of security-related activity on the network helps identify these practices. The principal goal of the security audit is to detect user and administrative practices that are inconsistent with the security policy. Audit data is then used to help limit or eliminate these inconsistent practices, often as background information in preparing for user education and, if necessary, administrative discipline. This section describes the NSO's role in monitoring security-related activities on the network.

---

#### Responsibility

The NSO is responsible for the following:

- Conducting security audits on the network
- Monitoring variances in security procedures
- Ensuring that security alarms are in place and functioning properly
- Reviewing network and network related audit logs and audit trail data to identify and analyze security-related weaknesses and opportunities for refinement and efficiency.

The NSO reports to the NSM or ISSM on the effectiveness of security policy and procedures, and makes recommendations for improvements.

---

#### Implementation

##### Monitoring Network Activity

The NSO uses automated audit mechanisms (such as *tcpdump*, *traceroute*, *bind*, *SNMP*, *NERD*, and *SNIF*) to monitor the following actions:

- All functions performed by system operators
- Successful and unsuccessful logon attempts
- Successful and unsuccessful network access attempts
- File accesses
- Types of file access (create, write, read, change, and delete)
- Password changes
- Disconnects and outages of remote workstations and peripherals
- Program aborts and anomalies.

The NSO ensures the following:

---

- Audit and review procedures are developed and implemented to ensure that all network functions are performed in accordance with network policies (e.g., audit logs of IS usage)
- Appropriate security events to be audited are selected
- Security alarms are activated and functioning properly
- Security audit parameters (i.e., what security functions are audited and how often) are reviewed
- Procedures for monitoring and reacting to security warning messages and reports are developed
- Audits are conducted and audit records are maintained and protected
- Unusual system activities are identified and investigated
- Random floor checks are conducted.

*Reference:* For additional information on network monitoring responsibilities and activities, see section 3.2, Administrative Functions, for information on the NSO “Security Watchdog” role.

---

#### **Vulnerability Checkers**

The NSO uses vulnerability checkers to evaluate network weaknesses, tampering, or other possible security incidents. The following are examples of commercially available vulnerability checkers.

- *Internet Security Scanner (ISS):* ISS is a network vulnerability auditing package that can be used to probe entire networks for vulnerabilities.
- *System Administrator Tool for Analyzing Networks (SATAN):* SATAN is also a network vulnerability auditing package. It is a “hacker tool” that is commercially available as freeware from the Internet. It employs network intrusion to analyze system vulnerabilities. It also provides tutorials on how to fix problems it uncovers.
- *TAMU:* The TAMU system is a collection of highly useful tools. Some can be used to build your own firewall, others to detect specific attack signatures. Its Tiger scripts can be used to assess the security of your own machines.
- *COPS:* COPS is a collection of short shell files and C programs that perform checks on the system to determine if certain weaknesses are present.
- *Tripwire:* Tripwire is a package that evaluates a system and checks for altered files.

- 
- *Security Profile Inspector (SPI):* SPI combines the functionality

---

of programs such as COPS and Tripwire. It also tries to track security patches on a per-platform basis. SPI is only available to certain U. S. federal and state government agencies.

---

**Intrusion Detection**

The NSO can use intrusion detection tools to monitor and prevent hackers and outside agents from accessing network assets. The following are examples of intrusion detection software.

- *Distributed Intrusion Detection System (DIDS)* monitors multiple hosts connected via a network and the network itself. Development started in 1991, at Purdue University, with later involvement of Haystack Labs, USAF-AFIWC; the University of California in Davis CA; and Trident Data Systems. DIDS, a command and control (C2) compliant tool for automating the reduction of audit information, includes hacker signature analysis and alarms/recovery procedures for actual intrusion.
- *Computer Misuse Detection System (CMDS)* monitors and analyzes networks in real-time and creates hard-copy reports that summarize suspicious activity. CMDS, developed by Science Applications International Corporation (SAIC), is hosted on any UNIX workstation; it supports VMS and UNIX systems.

---

**Password Protection**

NSOs need to recognize that password attacks are the most common attacks on a system. The top two methods of intrusion from Hacker's Hit List are default system passwords and unlimited password attempts (automated knocking). Authentication devices are the best defense. Shadow password files help but offer no defense against the eavesdropper. The *crack* program is a widely distributed and effective password cracking program.

---

**Audit Trail Review**

The audit trail provides a record of security-related activity on the network. The NSO reviews the audit trail reports for the following:

- Multiple unsuccessful logon or network access attempts
  - Users logged on at more than one workstation
  - Logons or network accesses after normal business hours
  
  - High numbers of file accesses
  - Unexplained changes in network activity.
-

---

The NSO also uses the audit trail report to create summary reports and user profiles from information such as:

- Records of user logons and logoffs
- Accesses of networks, servers, folders, and files.

NSOs should retain detailed audit trail records for no more than 60 days. After the 60-day period, the NSO should use the summary reports and user profiles. The summary reports and user profiles should be destroyed after 1 year.

*Reference:* For additional guidance on C2 requirements, see NAVSO P-5239-15, Controlled Access Protection (CAP) Guidebook. For additional information on automated network security tools, see the Navy's INFOSEC web homepage at <http://infosec.nosc.mil/>.

---

### 3.6 Incident and Violations Reporting

Security incidents or violations are occurrences that may affect the security posture of the network. Security incidents or violations include, but are not limited to, the following:

- Suspected or confirmed viral or malicious software infections, including worms, trojan horses, and cracking utilities
- Password cracker/hacker attacks
- Intrusion attempts and successes within the network, such as:
  - Remote users logging in with compromised passwords
  - Compromised administrative privileges, allowing the creation and utilization of false user accounts
- Unauthorized use of another user's account
- Access denials, such as:
  - Incorrect password violations
  - Incorrect account/user names
  - Unauthorized access to certain files, directories, servers, or other resources on the network
- Suspicious connections or connection attempts (e.g., remote users logging in and using a local network and IS)
- Unauthorized modification of discretionary access controls and audit procedures
- Unauthorized use of the network that significantly degrades network performance
- Transmitting information to or from a network that is not accredited
- Creating or spreading hoaxes (i.e., false information about incidents or vulnerabilities).

This section describes the NSO's role in evaluating and responding to security incidents or violations.

---

#### **Responsibility**

All suspected incidents or violations must be reported immediately, first by the NSO to the NSM or ISSM, and then, after analysis by the NSM or ISSM, to the NAVCIRT and DAA simultaneously. Incidents should be reported to NAVCIRT at (800) 628-8893, or E-mail: *navcirt@fiwc.navy.mil*. The NSO is responsible for creating the network incident reporting mechanism.

## Implementation

### Functions in Support of Reporting Mechanism

The NSO supports the successful and effective reviewing of reported incidents by

- Preparing procedures for monitoring and reacting to network security warning messages and reports
  - Developing procedures (for approval by the DAA and technical supervisor) for identifying, containing, eradicating, recovering from, reporting, investigating, and resolving security incidents at the site
  - Reporting security incidents immediately
  - Performing an initial evaluation of security problems.
- 

### Incident Analysis

The NSO must be aware of all security incidents and violations. The NSO participates in the incident analysis through the following actions:

- Analyzing the effects of an incident as to risk and degree of compromise
- Reporting results of analysis to the NAVCIRT and DAA via the NSM or ISSM
- Recommending appropriate action to the DAA via the NSM or ISSM, such as
  - Increasing auditing and monitoring activity
  - Increasing protection levels and security mechanisms
  - Suspension of all noncritical network activity
  - Complete system shutdown.

*Reference:* For more information, see section 11, Security Documentation, for a description of an incident report and NAVSO P-5239-19, Computer Incident Response Guidebook. The NSO can gain additional information about incident reporting by accessing the Forum of Incident Response and Security Teams (FIRST) homepage at <http://csrc.ncsl/nist.gov/nist.gov/first/> and the Computer Security home page at <http://www.deltanet.com/users/llambert/security.html>.

---

### 3.7 Risk Management

The Risk Management Program includes the process of identifying, measuring, and minimizing uncertain events affecting network resources. The program includes the security activities that span the life cycle of a network. Risk management determines the value of the data, which protections exist, and how much more protection (if any) the network needs. Risk management determines the value of all network resources and the conditions and security weaknesses that might lead to some level of loss of resource confidentiality, integrity, or availability. From this ongoing process, additional protection, when warranted, may be evaluated and added to the network security features. Risk management includes risk assessment, countermeasure selection, security test and evaluation, contingency planning, and network review. The results of these activities provide the information on which a DAA bases an accreditation decision. Risk management activities do not end with an accreditation decision. Ongoing analysis throughout the life cycle ensures that network security requirements are always met. The NSO performs risk management activities under the direction of the NSM or ISSM.

---

#### **RISK MANAGEMENT PROGRAM**

---

##### **Responsibility**

The NSO supports the DON Risk Management Program at the direction of the NSM or ISSM. The NSO provides support to ensure that these program tasks are accomplished:

- Identify specific threats and vulnerabilities to the network
- Identify and apply countermeasures to mitigate the identified risk
- Test the effectiveness of the implemented security controls
- Review the continued effectiveness of the implemented security measures.

The primary responsibility is to conduct the Risk Assessment of the network using the methodology recommended to and determined by the NSM or ISSM and approved by the DAA.

---

##### **Implementation**

A network risk assessment presents a technical challenge to the NSO because of the many possible risk combinations. The NSO performs the risk assessment according to the methodology prescribed by the NSM or ISSM and DAA. The Risk Assessment Guidebook, Module 16 of the NAVSO P-5239 series, provides the procedures to be followed for

---

---

performing a risk assessment for Local Area Networks (LAN), Wide Area Networks (WAN), and integrated site ISs. The NSO:

- Recommends the risk assessment type to the NSM or ISSM based on the risk assessment selection chart.
- Receives approval of the risk assessment type from the NSM or ISSM and the DAA.
- Performs the approved risk assessment using one of the following Risk Assessment types:
  - Survey Risk Assessment
  - Basic Risk Assessment
  - Intermediate Risk Assessment
  - Full Risk Assessment.
- Performs the risk assessment by completing the checklist and forms for the specific type of assessment selected. The risk assessment identifies the specific threats and vulnerabilities to the network and the residual risk to the network.
- Submits the completed risk assessment to the NSM or ISSM for review.
- Maintains the risk assessment documentation for inclusion in the accreditation package to be presented to the DAA.

The risk assessment yields a ranking of risk and the estimated damage or loss associated with each risk. If directed by the NSM or ISSM, the NSO recommends safeguards to counteract the vulnerabilities identified in the risk assessment.

The NSO recommends countermeasures based on risk level and cost effectiveness. The level of risk, severity of the security problem, and level of impact on resources will dictate the need for the countermeasure. There may be instances where the recommendation of a countermeasure is warranted despite a negative return on investment (ROI). Safety would be the most likely reason. Such a recommendation would include the explanation that while implementation of this countermeasure will not provide a positive ROI, it will enhance the safety of system support personnel. The potential countermeasures examined should include the following safeguards:

- Technical safeguards
- Physical safeguards
- Administrative safeguards.

---

For instance, if the risk assessment indicated that a risk of

---

---

compromise of information resulted from weak access controls, the NSO could examine the use of countermeasures in each of the areas of technical, physical, and administrative safeguards to mitigate the risk. The use of a network security product that identifies and authenticates the device from which the users attempt to access the network and the devices that originate data exchanges would each be part of a technical countermeasure; the use of a room key to control access to the server would be a physical countermeasure; and the use of a guard checking an access control list would be an administrative countermeasure. If the risk assessment indicated a risk of compromise (e.g., because of wire tapping or sniffing devices) then the use of encryption devices could provide a technical countermeasure for protection. Information pertaining to NSA-endorsed encryption devices (e.g., the Secure Telephone Unit [STU-III] and Motorola NES) can be found in NSA's Information Systems Security Products and Services Catalogue. When directed, the NSO provides countermeasure selection and residual risk statement recommendations to the NSM or ISSM.

---

## REVIEW OF RISK ASSESSMENT

---

### **Responsibility**

Assessments of risk mirror the progress of a system through its life cycle. As a system progresses, changes occur. System threats and vulnerabilities change correspondingly. DOD/DON policies dictate maximum periods between risk assessments. The NSO periodically reviews the risk assessment and modifies it to accommodate new threats caused by changed configuration, system modifications, or changes in the operational environment. DOD/DON policy dictates maximum periods between risk assessments. An updated risk assessment is performed every 3 years or earlier in cases where changes to the network might invalidate the terms of the most recent accreditation. These occurrences most likely fall under one of the following conditions:

- Major system redesigns
- Changes in the sensitivity level of the data
- Operating system or security software changes.

The review concentrates on the effectiveness of the available security safeguards and countermeasures implemented.

---

### **Implementation**

The NSO documents and reports the INFOSEC technical vulnerabilities and new threats detected in the network to the NSM or

---

---

ISSM. The NSO administers the technical vulnerability reporting program and accomplishes the following:

- Reports identified technical vulnerabilities
- Recommends feasible actions to reduce risks presented by the vulnerabilities
- Develops local procedures for reporting and documenting technical vulnerabilities
- Ensures that vulnerability information is properly classified, marked, and protected.

*Reference:* For more information, see section 11, Security Documentation, and NAVSO P-5239-16, Risk Assessment Guidebook.

---

## SECURITY TEST AND EVALUATION

---

### **Responsibility**

Security Test and Evaluation (ST&E) is a part of the DON Risk Management Program. The primary purpose for conducting an ST&E is to obtain technical information to support the DAA's decision to accredit a network activity. ST&E is a process that determines whether the installed countermeasures identified in the risk assessment are working effectively. The risk assessment type performed defines the level of detail examined in the ST&E.

---

### **Implementation**

The NSO assists the NSM or ISSM in the planning and execution of the ST&E. The activities may include the following:

- Compiling resources (including the team, hardware, software, media, and functioning system)
  - Establishing the security baseline
  - Providing system documentation (e.g., user, operator, and administrator manuals) and security regulations (the use of on-line network resident documentation [e.g., Hypertext Mark-up Language (HTML)] is encouraged)
  - Ensuring work space and storage for the development and execution team
  - Ensuring the development of ST&E plans and procedures
  - Monitoring the ST&E inspections
-

- Ensuring the ST&E log that records daily activities is maintained
- Witnessing the testing
- Ensuring the development of the ST&E report
- Maintaining a file of working papers concerning the security tests.

The NSO may participate in developing ST&E plans, procedures, and reports. The risk of unintentional bias by the NSO in test writing is mitigated by the review of the NSM or ISSM.

*Reference:* For more information concerning ST&E documentation see section 11, Security Documentation. Also see NAVSO P-5239-18, Security Test and Evaluation Guidebook.

---

### 3.8 Accreditation

Accreditation is a process that results in the formal management decision the DAA makes to implement a network in a specific operational environment at an acceptable level of risk. This decision is predicated on the risk assessment, ST&E results, and residual risk statement provided to the DAA by the NSM or ISSM, based on the analysis and testing conducted by the NSO. The information is contained in the accreditation package. This package contains, at a minimum, the results of the risk assessment, identification of residual risk to the network, results of the ST&E, and contingency plan if required for the network.

---

**Responsibility**

The NSO provides support to the NSM or ISSM and the DAA throughout the accreditation process.

---

**Implementation**

The NSO assists in the accreditation of a network by providing the following support:

- Assisting in the preparation of the accreditation material such as the identification of residual risk to the network. This identification is based on the results of the risk assessment conducted on the network. The results of the ST&E are also included in the accreditation package.
  - Assisting in site surveys. The NSO provides the necessary support if the DAA elects to visit the site to inspect the network before making the accreditation decision.
  - Assisting in the evaluation of the accreditation package. The NSO examines the contents of the accreditation package to be provided to the NSM or ISSM and the DAA to ensure that the documentation supports the recommendations for an accreditation decision.
  - Coordinating the accreditation package with the NSM or ISSM. The NSO provides the accreditation package contents to the NSM or ISSM for delivery to the DAA.
-

### 3.9 Security Configuration Management

Once security is established for a network, strict measures must be enforced to ensure that changes to the network do not disrupt this balance. Even seemingly minor changes may result in severe implications to the network security. The NSM or ISSM is ultimately responsible for controlling changes to the network and preventing changes that negatively impact the security of the network. Configuration management controls changes to network software, firmware, hardware, and documentation throughout the life of the network. This includes the design, development, testing, distribution, operation, and modifications and enhancements to the existing network. The NSM or ISSM may delegate security-related configuration management activities to the NSO as appropriate for the specific Command. This section describes the NSO's role in assisting the NSM or ISSM in configuration management activities.

---

<b>Responsibility</b>	In accordance with the DAA's policies and procedures for controlling changes to the network, the NSO assists the NSM or ISSM in providing input to network configuration management activities to ensure that implemented changes do not compromise the security of the network.
-----------------------	--

---

#### Implementation

<b>Change Review</b>	The NSO reviews the network inventory, as documented by the Network Administrator, to ensure that network components have not changed, been relocated, or otherwise been tampered with in any way that may impact the overall security of the network. The NSO also reviews network connections to ensure that additions or deletions are noted and do not adversely impact the security of the overall network. The NSO provides a status report to the NSM or ISSM that summarizes the nature (estimated security impact, if any) of changes along with a copy of the inventory list. The NSO also ensures that only authorized software is used on the network system.
----------------------	---

---

<b>Change Management</b>	The NSO conducts an initial review of network change proposals in respect to the following criteria: <ul style="list-style-type: none"><li>• How will the change impact network security?</li><li>• What network nodes are affected by the change and how?</li><li>• If new software is proposed, will it be from an authorized source?</li></ul>
--------------------------	---

---

- Have security features and mechanisms been considered and included in network change plans?
- Do network support personnel know how to install and maintain new security features/mechanisms?
- Will reaccreditation be necessary?

The NSO then submits his findings and original change proposals to the NSM or ISSM for further analysis and disposition.

---

**Change Testing**

The NSO witnesses and conducts, where possible, tests to ensure the following:

- Implemented changes have not adversely affected network security
  - Security features and mechanisms are fully functional.
-

### 3.10 Contingency Planning

Contingency Planning requires the formulation of the strategy (plan) and the procedures for responding to the unplanned disruption of service to a network. This planning ensures that the impact of incidents, accidents, or disasters on the mission is measured. The plan documents emergency response, backup procedures, and post-disaster recovery procedures. Activities develop a Contingency Plan for each network for which unplanned disruption of service would have a critical effect on mission accomplishment. A Contingency Plan is not required for networks for which the unplanned disruption of service would not have a critical impact of mission accomplishment. In these cases, a written statement eliminating the requirement should be included in the accreditation package. When required, a Contingency Plan becomes an integral part of the accreditation package. The ISSM or NSM is responsible to the DAA for the development of the plan. Usually, Contingency Plans are developed by teams composed of System and Network Administrators, program management personnel, and user group representatives. The NSO may be directed by the ISSM or NSM to contribute to this effort.

---

**Responsibility**

Although the NSM or ISSM is responsible for the development of a Contingency Plan for each network, the NSO provides technical contributions concerning Contingency Planning for the network for which he or she is responsible.

---

**Implementation**

The NSO's contributions cover the three phases of formulating, testing, and revising contingency plans. The NSO ensures that contingency plans are in place for continuity of operations in an emergency situation and that the developed plans are exercised.

*Reference:* See section 11, Security Documentation, for a description of a Contingency Plan and Federal Information Processing Standards (FIPS) Publication # 87, dated 27 March 1981. Also see IRM-5239-09 (Marine Corps), Contingency Planning.

---

### 3.11 Security Documentation

The following documents, appearing in the sequence referenced in this Guidebook, are typically prepared by INFOSEC personnel. The use of on-line, network-resident documentation (e.g., HTML) is encouraged.

---

**System Security Plan**

The SSP fulfills mandates of the Computer Security Act of 1987, which requires federal agencies to identify each computer system that contains sensitive information, and prepare and implement a plan for the security and privacy of these systems. The SSP plays a key role in the implementation of the DON INFOSEC Program and is to be maintained for all DON ISs. The SSP (also called the System Security Package) contains the protection strategy planned for the IS and describes the security controls that are implemented to safeguard the system against specified threats and risks. The SSP provides a statement of the security policy for the operation of the IS in its intended environment. The security policy will specify what is and is not permitted in the operation of the IS and network. The following outlines the SSP structure:

- Unit Identification (organization/activity for which the IS accreditation is being requested)
  - Support Personnel (ISSM, ISSO/NSO, System/Network Administrator)
  - Mission Description
    - Identity of the Accreditor; System Ownership
    - Data Sensitivity
    - Identity of System Users
    - Mode of Operation
  - Threat Analysis
    - Environment
    - Threat Summary
    - Risk Assessment Summary
  - Architectural Description
    - Hardware
    - Software
    - Accreditation Boundary
    - External Connections
  - System Security Requirements
    - Security Policy Statement
    - Security Requirements
- 
- Summary of Administrative, Technical, and Operational

- Security Features
  - Concept of Operations
- Certification
  - Security Test and Evaluation
  - Copy of Completed IS and Network Security Inspection Checklist
  - Summary of Type II Certification Effort (If Applicable)
  - Statement of Security Concerns
  - Recommendation (rationale for why residual risks should be accepted/rejected)
- Accreditation (DAA Accreditation Decision)
- Potential Enclosures (as required, or specified by DAA), for example:
  - MOAs
  - Test Results
  - Contingency Plan
  - C&A Plan
  - Security Policy
  - SFUG
  - TFM
  - Security CONOPS
  - Security Architecture.

The SSP provides a basic overview of the security and privacy requirements of the specific system(s) and the Command's plan for meeting those requirements.

---

**Security Operating Procedures**

Current DON policy requires that security procedures be developed, documented, and presented to all IS users. Topics of discussion should include, but not be limited to, policy statements, system access controls, operating procedures, audit trails, training, physical security, media protection, modes of operation, emergency procedures, enforcement, documentation, and data levels. Additional information may need to be addressed to meet site-specific needs. The ISSO or NSO is the primary author of the SOPs. The ISSM or NSM ensures that SOPs are reviewed annually for accuracy.

---

**Network  
Memorandum of  
Agreement**

An MOA, also referred to as MOU, is a management vehicle that defines all terms and conditions of the security arrangements that will govern the operation of the network. The objective of the MOA is to document the interconnection requirements and to identify any requirements that may be necessary to provide overall security safeguards for the entire network, including all interconnected subsystems, the communications devices, the users, and the data stored in the subsystem. A sister document to the MOA is the MOR. The MOR is used when the subsystems have the same DAA.

*Reference:* For MOA/MOR development guidance, see NCSC-TG-011, version 1, Trusted Network Interpretation Environment Guideline.

---

**Authorized User  
List**

The cognizant local work area security officer must be able to determine the identity of all users approved for any workstation. The exact method and format may vary. Timeliness and accuracy are most important. The Authorized User List, which identifies authorized system users, should be kept as part of the related accreditation documentation.

---

**Training and  
Awareness  
Documentation**

Training and awareness documentation should continuously reinforce the need for security of the IS and network with the users. The reinforcement satisfies the requirement to provide refresher training to the user. An awareness program provides the opportunity to update the user on any security changes. The program may consist of posters, newsletters, videos, and warning messages to reinforce the need for protection.

---

**IS Incident Report**

The IS Incident Report explains the type of incident, the individuals involved, and the estimated cost of the incident; summarizes the incident, investigation results, and supervisor's recommendations; and provides the local action to prevent recurrence.

*Reference:* For more information, see NAVSO P-5239-19, Computer Incident Response Guidebook.

---

**Risk Assessment** A Risk Assessment identifies the threats, vulnerabilities, and risks to an IS. The NAVSO P-5239-16, the Risk Assessment Guidebook, presents a methodology for conducting a risk assessment using one of four types: survey, basic, intermediate, and full risk assessment.

*Reference:* For more information, see NAVSO P-5239-16, Risk Assessment Guidebook.

---

**ST&E Documentation** The following documents are typically developed as part of the ST&E effort.

**Plan and Procedures** The ST&E plans and procedures identify each of the countermeasures to be tested and the method used to determine the effectiveness of the countermeasure. If scenarios, inspections, documentation, and review procedures are to be used, they must be linked with each countermeasure.

**Checklist** ST&E checklists can be used to evaluate the effectiveness of countermeasures implemented on an IS. The checklist approach may be appropriate when a comprehensive ST&E is considered unnecessary by the DAA, as determined by the complexity of the IS and the level of risk. The checklists help ensure that the IS is operating within an acceptable level of risk.

**Report** The ST&E report documents the execution and results of the ST&E plan/procedures. It analyzes the findings of the ST&E plan/procedures and lists the recommendations to correct any identified deficiencies.

*Reference:* For more information, see NAVSO P-5239-18, Security Test and Evaluation Guidebook.

---

**Contingency Plan** The Contingency Plan provides a decision-making process to be used during or following the occurrence of unforeseen events that adversely affect normal IS operations within the activity. A Contingency Plan is not required for ISs or components for which the unplanned disruption of service would not have a critical impact on mission accomplishment.

In these cases, the ISSM informs the DAA that no Contingency Plan

---

is required. Mission criticality of the system determines details of Contingency Plan.

*Reference:* For more information, see Federal Information Processing Standards (FIPS) Publication # 87, dated 27 March 1981, and IRM-5239-09 (Marine Corps), Contingency Planning.

---

## **APPENDIX A**

### **SECURITY POLICY, PROCEDURE, AND GUIDANCE DOCUMENTATION**



## **Appendix A**

### **Security Policy , Procedure, and Guidance Documentation**

#### Department of Defense (DOD)

**Department of Defense Instruction 5000.2** , *Defense Acquisition Management Policies and Procedures*, 23 February 1991.

This document establishes an integrated framework for translating broadly stated mission needs into stable, affordable acquisition programs that meet the operational user's needs and can be sustained, given projected resource constraints. It also establishes a rigorous, event-oriented management process for acquiring quality products. This process emphasizes acquisition planning, improved communications with users, and aggressive risk management by both Government and industry.

**Department of Defense Directive 5200.1** , *Information Security Program*, 7 June 1986.

This document reissues DOD 52001-R, *Information Security Program Regulation*, updates policies and procedures of the DOD Information Security Program, implements DOD 5200.1-H, *Department of Defense Handbook for Writing Security Classification Guidance*, delegates authority, and assigns responsibilities.

**Department of Defense Regulation 5200.1-R** , *Information Security Program Regulation*, Department of Defense, August 1982.

This document governs the DOD information security program. It establishes a system for the classification, downgrading, and declassification of classified and sensitive information. It further states the policies and procedures for safeguarding national security information from unauthorized disclosure.

**Department of Defense Directive 5200.28**, *Security Requirements for Automated Information Systems*, Department of Defense, March 1988.

This directive provides the mandatory, minimum Information Security (INFOSEC) requirements for processing classified, sensitive unclassified, and unclassified information. The directive states that information in ISs shall be safeguarded at all times by computer, communication, administrative, personnel, operations, emanations, and physical security measures. The directive emphasizes the importance of a life-cycle management approach for implementing computer security requirements.

NAVSO P-5239-08

MARCH 1996

**Department of Defense Directive 5200.28-STD** , *Department of Defense Trusted Computer System Evaluation Criteria*, Department of Defense, December 1985.

This directive, also known as the "Orange Book" and "the Criteria," provides technical security requirements and evaluation methodologies for trusted computer systems. It provides a metric with which to evaluate the degree of trust that can be placed in a computer system. This directive also specifies security requirements in computer system acquisition documentation.

**Department of Defense Instruction 5215.2** , *Computer Security Technical Vulnerability Reporting Program (CSTVRP)*, 2 September 1986.

This document establishes (1) CSTVRP under the direction of the National Security Agency, National Information Security Assessment Center (NISAC); (2) procedures for reporting all demonstrable and repeatable technical vulnerabilities of Automated Information Systems (AIS); (3) procedures for the collection, consolidation, analysis, reporting or notification of generic technical vulnerabilities and corrective measures in support of the DOD Computer Security requirements; and (4) methodologies for dissemination of vulnerability information.

Department of the Navy

**SECNAVINST 5200.32A** , *Acquisition Management Policies and Procedures for Computer Resources*, 3 May 1993.

This document provides policy for acquiring Department of the Navy (DON) computer resources and establishing the internal management processes. It authorizes the promulgation of the Open System Interface Standards List (OSISL) and the Products Accepted List (PAL) in SECNAVNOTE 5200, Subj: Acquisition Management Policies and Procedures for Computer Resources, to facilitate the acquisition of computer resources in accordance with this instruction.

**SECNAVINST 5231.1C** , *Life Cycle Management of Automated Information Systems Within the Department of the Navy*, 10 July 1992.

This document updates policy relative to Life Cycle Management (LCM) as the standard discipline for managing and obtaining approval for Information Systems (IS) projects as defined by Department of Defense Directive (DODD) 7920.1, *Life Cycle Management of Automated Information Systems (NOTAL)*, 20 June 1988 and DODI 7920, *Automated Information System Life Cycle Management Review and Milestone Approval Procedures (NOTAL)*, 7 March 1990.

**SECNAVINST 5239.3**, *Department of the Navy Information Systems Security (INFOSEC) Program*, Department of the Navy, July 1995.

This document establishes the DON INFOSEC program within the Information Warfare discipline. It defines the organizational responsibilities for implementing the security disciplines of Communications Security (COMSEC), Computer Security (COMPUSEC), and Emanations Security (TEMPEST). This instruction provides the basic policy and guidelines necessary for consistent and effective application of resources in ensuring the security of national security systems and the security and privacy of DON systems/information under the Computer Security Act of 1987.

**OPNAVINST 5239.1A**, *Department of the Navy Automated Data Processing Security Program*, Department of the Navy, August 1982. (Note: This instruction is being updated.)

This document consolidates Navy policies on the security evaluation of ISs. The instruction delineates the requirements and assigns roles and responsibilities for accreditation of ISs. It provides guidance for the risk assessment process and full accreditation requirements.

**OPNAVINST 5510.1H**, *Guidance for Marking and Handling Classified Material*, 29 April 1988.

This document provides guidance for classifying and safeguarding classified information.

**OPNAVINST 5530.14B**, *Department of the Navy Physical Security and Loss Prevention*, 30 November 1992 (change Note 4).

This document establishes and revises policy, provides guidance, and sets forth uniform standards for physical security and loss prevention measures to safeguard personnel, property, and material at Navy and Marine Corps shore installations and activities.

**Marine Corps Order P5510.14**, *Marine Corps Automatic Data Processing (ADP) Security Manual*, 2 January 1981.

This document provides centralized guidance and uniform policy on all known and recognized aspects of ADP security. It also provides realistic guidance and generalized procedures to ensure that all sensitive defense information handled by automated systems is protected against espionage, sabotage, fraud, misappropriation, misuse, or inadvertent or deliberate compromise.

**Marine Corps Order 5271.1** , *Information Resources Management (IRM) Standards and Guidelines Program*, 10 June 1993.

This document establishes the IRM Standards and Guidelines Program and authorizes the development and distribution of publications. The IRM Program is the primary means through which technical direction is exercised. The program is designed to facilitate the rapid publication of standards and guidelines covering all aspects of the management of information resources, including INFOSEC.

Executive Office/Congress and National Branch

**Executive Order 12958**, *Classified National Security Information*, 17 April 1995.

This document established a system for classifying, declassifying, and safeguarding national security information. It identifies classification authorities and describes their general responsibilities for the origination and handling of classified information.

**National Security Decision 42** , *National Policy for the Security of National Security Telecommunications and Information Systems*, Executive Office of the President, July 1990.

This document establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; and establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation.

**National Telecommunications and Information Systems Security Policy No. 200** , *National Policy on Controlled Access Protection*, National Telecommunications and Information Systems Security Committee, July 1987.

This document, under the authority of NSDD 145, *National Telecommunications and Information Systems Security Policy (NTISSP) No. 200*, defines the minimum level of protection for ISs processing classified or sensitive unclassified information. It prescribes the C2 class criteria of DOD 5200.28-STD as the minimum level of protection for such systems, with additional protection required if warranted by a system risk assessment.

**Public Law 100-235** , *Computer Security Act of 1987*, 8 January 1988.

This document redefines the role of the National Institute of Standards and Technology (formerly the National Bureau of Standards) and establishes a new Computer System Security and Privacy Advisory Board. It requires each federal agency to provide for mandatory periodic training in computer security awareness and accepted computer security practices; identify each federal computer system and system under development that contains sensitive information; and establish a plan for security and privacy of such systems.

Joint Staff

**Chairman of the Joint Chiefs of Staff Instruction CJCSI 6510.01** , *Joint and Combined Communications Security*, 1 September 1993.

This document establishes policy and procedures for planning and conducting joint and combined COMSEC, and presents the following applicable policy to joint and combined applications: Transmission of Sensitive Information, System Planning, Operational Planning, Joint Coordination, Urgent Need, Foreign Release, Foreign Sales, Radios, Special-Purpose Cryptographic equipment, Manual Systems Cryptonet Size, Cryptoperiod, Radio Frequencies, Call Signs, Field Generation and Over-the Air Distribution (OTAD) of Tactical Key, Intertheater COMSEC Package Key, Assessments, COMSEC Monitoring and TEMPEST.

**JCS Memorandum MJCS-38-89** , *Use of Standard Embedded Cryptography*, 2 March 1989.

This document encourages maximum use of standard embedded cryptography products in future communications and computer systems that require cryptographic security features.

National Computer Security Center

**CSC-STD-002-85** , *Department of Defense Password Management Guideline*, 12 April 1985.

This document assists in providing credibility of user identity by presenting a set of good practices related to the design, implementation, and use of password-based user authentication mechanisms. It is intended that the features and practices described in the guideline be incorporated into DOD ADP systems for processing classified or other sensitive information.

**CSC-STD-003-85** , *Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments*, National Computer Security Center, June 1985.

This document provides guidance for specifying computer security requirements for the DOD by identifying the minimum class of system required for a given risk index.

**CSC-STD-004-85** , *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments*, National Computer Security Center, June 1985.

This document provides background discussion and rationale for CSC-STD-003-85, and provides additional and more detailed guidance for specifying computer security requirements for the DOD by identifying the minimum class of system required for a given risk index for different environments.

NAVSO P-5239-08

MARCH 1996

**CSC-STD-005**, *Department of Defense Magnetic Remanence Security Guideline*, 15 November 1985.

This document provides procedures and guidelines for declassifying and clearing ADP magnetic memory and other ADP magnetic storage media.

**NCSC-TG-001**, *A Guide To Understanding Audit in Trusted Systems*, Version 2, 1 June 1988.

This document provides a set of good practices related to the use of auditing in ADP systems employed for processing classified and other sensitive information.

**NCSC-TG-003**, *A Guide To Understanding Discretionary Access Control in Trusted Systems*, Version 1, 30 September 1987.

This document discusses issues involved in designing, implementing, and evaluating DAC mechanisms. Its primary purpose is to provide guidance to manufacturers on how to select and build effective DAC mechanisms.

**NCSC-TG-005**, *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria*, National Computer Security Center, Version 1, July 1987.

The TNI or “Red Book” was issued by the National Computer Security Center (NCSC) as part of its program to promulgate technical computer security guidelines. The interpretation extends the evaluation classes of the “Orange Book” to trusted network systems and components.

**NCSC-TG-017**, *A Guide To Understanding Identification And Authentication In Trusted Systems*, Version 1, September 1991.

This document provides guidance to vendors on how to design and incorporate effective identification and authentication (I&A) mechanisms into their systems. It also aids vendors and evaluators in understanding I&A requirements.

**NCSC-TG-027**, *A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems*, National Computer Security Center, Version 1, May 1992.

This document helps ISSOs understand their responsibilities for implementing and maintaining security in a system. This guideline also discusses the roles and responsibilities of other individuals who are responsible for security and their relationship to the ISSO, as defined in various component regulation and standards.

**NCSC-TG-028**, *Assessing Controlled Access Protection*, Version 1, 25 May 1992.

This document explains the controlled access protection requirements of the Trusted Computer System Evaluation Criteria.

**NCSC-TG-029**, *Introduction to Certification and Accreditation*, Version 1, January 1994.

This document provides an introduction to C&A concepts, provides an introductory discussion of some basic concepts related to C&A, and sets the baseline for further documents.

National Security Agency

***Information Systems Security products and Services Catalogue***, published four times annually (January, April, July, and October).

This document is a list of INFOSEC products and services that have either been evaluated against established standards or have been endorsed by NSA as having met government requirements and standards set for these products.

National Institute of Standards and Technology

**Federal Information Processing Standard s Publication 87**, *Guidelines for Contingency Planning*, 27 March 1981.

This document provides guidelines to be used in the preparation of IS contingency plans. The objective is to ensure that IS personnel and others who may be involved in the planning process, are aware of the types of information that should be included in such plans; to provide a recommended structure and a suggested format; and to make those persons responsible aware of the criticality of the contingency planning process.

**Federal Information Processing Standard on Trusted Systems Technology**, *Minimum Security Functionality Requirements for Multi-user Operating Systems*, Issue 1, 16 January 1992.

This document provides basic commercial computer system security requirements applicable to government and commercial organizations. These requirements include technical measures that can be incorporated into multiuser, remote-access, resource-sharing, and information-sharing computer systems.

**Federal Information Processing Standard on Trusted Systems Technology** , *Federal Criteria for Information Technology Security*, Protection Profile Development, Volume 1, Version 1.0, December 1992.

This document provides a basis for developing, analyzing, and registering criteria for information technology (IT) product security development and evaluation. The document explains how to use provided generic requirements as building blocks to create unique sets of IT product security criteria, called protection profiles. There are four principal objectives:

- Develop an extensible and flexible framework for defining new requirements for IT product security
- Enhance existing IT product security development and evaluation criteria
- Facilitate international harmonization of IT product security development and evaluation criteria
- Preserve the fundamental principles of IT product security.

National Security Telecommunications and Information Systems Security Committee

**NTISSD 500**, *Information Systems Security (INFOSEC) Education, Training, and Awareness*, 25 February 1993.

This document establishes the requirement for federal departments and agencies to develop and/or implement Telecommunications and Automated Information Systems Security (TAISS) education and training programs and TAISS awareness activities.

**NTISSD 501**, *National Training Program for Information Systems Security (INFOSEC) Professionals*, 16 November 1992.

This document establishes the requirement for federal departments and agencies to implement training programs for INFOSEC professionals. In this directive, an INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during each life-cycle phase.

**NTISSD 502**, *National Security Telecommunications and Automated Information Systems Security*, 5 February 1993.

This document delineates and clarifies objectives, policies, procedures, standards, and terminology as set forth in the National Policy for the Security of National Security Telecommunications and Information Systems (National Security Decision 42), dated July 1990. The National Security Decision 42 establishes the initial national objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding, from exploitation, systems that process or communicate national security information, and establishes a mechanism for policy development, and assigns responsibilities for implementation.

**NTISSP 4**, *National Policy on Electronic Keying*, 16 November 1992.

This document declares that all U.S. Government departments and agencies shall establish and implement electronic keying programs with the objective of not only virtually eliminating, by 2000, their dependence on paper-based/nonelectronic keying methods but also implementing benign keying where appropriate. Electronic keying shall be applied to all cryptographic processes related to national security systems. U.S. Government departments and agencies shall exchange electronic keying information freely, coordinate programs, and participate in consolidated programs wherever possible.

**NTISSP 200**, *National Policy on Controlled Access Protection*, 15 July 1987.

This document states that all automated information systems that are accessed by more than one user, when those users do not have the same authorization to use all of the classified or sensitive unclassified information processed or maintained by the automated information system, shall provide automated Controlled Access Protection for all classified and sensitive unclassified information.

Office of Management and Budget

**Office of Management and Budget Bulletin No. 90-08**, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*, July 1990.

This document provides guidance to federal agencies on computer security planning activities required by the Computer Security Act of 1987. It provides instructions and format for the preparation of system security plans.

**Office of Management and Budget Circular A-130**, Revised (Transmittal Memorandum No. 2), *Management of Federal Information Resources*, Executive Office of the President, July 1994.

This document establishes general policy for the management of Federal information resources. Included in this circular is policy for the security of federal ISs. The circular establishes minimum controls for inclusion in INFOSEC programs and assigns responsibilities for the security of ISs. It also provides detailed interim guidance to Navy program managers on how to address computer security requirements during the acquisition process.

Naval Staff Office Publication 5239 Modules

**Planned Naval Staff Office Publication 5239 Modules** (Note: the modules are not listed in publication order. Modules that have been published are annotated as such.)

**5239-01, *Introduction to Information Systems Security (INFOSEC)*, Published**

This document provides a basic introduction to INFOSEC and summarizes the DON INFOSEC Program.

**5239-02, *Terms, Abbreviations, and Acronyms*, Published**

This document lists and defines INFOSEC terms, acronyms, and abbreviations that have been standardized for use within the DoN.

**5239-03, *Designated Approving Authority (DAA) Guidebook***

This document provides guidance to the DAA in focusing the efforts of the activity security staff, contains a synopsis of the C&A process, and offers the DAA a step-by-step approach to assist in reaching accreditation decisions.

**5239-04, *Information Systems Security Manager Guidebook***

This document provides guidance to the individual who is assigned responsibility for INFOSEC implementation and operation at Navy activities. The guidebook also illustrates the need for management involvement and support for the security program.

**5239-07, *Information Systems Security Officer's Guidebook***

This document aids those individuals who conduct and administer INFOSEC programs for specific ISs and Local Area Networks (LAN). The guidebook also helps ISSOs understand the requirements, identify the necessary planning, and conduct an effective INFOSEC program.

**5239-08, *Network Security Officer's Guidebook***

This document aids those who conduct and administer INFOSEC programs for specific networks and LANs. Helps Network Security Officers (NSO) understand the requirements, identify the necessary planning, and conduct an effective INFOSEC program.

**5239-10**, *Assessed Product List*, Published

This document identifies products that have been evaluated for features and assurance of trust.

**5239-11**, *System Security Requirements Development*

This document provides guidance on how to develop a security policy and security requirements for a specific system.

**5239-12**, *Acquisition Life Cycle Guidebook (PM/Developers)*

This document identifies key technical and management actions needed from program managers and other developers who have managerial and technical responsibilities for acquiring or certifying computer systems. The guidebook, which is oriented primarily towards program managers, focuses on the processes and requirements needed to certify and accredit information systems.

**5239-13**, *Certification and Accreditation (C&A) Guidebook*

This document provides procedure guidance and decision aids for conducting C&A process activities to determine the suitability of a system to operate in a targeted operational environment based on the degree of assurance required and other factors related to a system.

**5239-14**, *Security Architecture Guidebook*

This document serves as a compendium of proven solutions to DON INFOSEC problems to assist INFOSEC systems engineering and customer support professionals to determine whether there are precedents for a customer's problem and to facilitate finding reusable solutions to common INFOSEC problems.

**5239-15**, *Controlled Access Protection Guide*, Published

This document aids the user and security staff in understanding the DON Controlled Access Protection policy, its relationship to C2, and techniques activities can use to acquire CAP-compliant systems.

**5239-16**, *Risk Assessment Guidebook*

This document provides policy and step-by-step procedures to individuals who are responsible for accomplishing a risk analysis on systems. The guidebook provides methods for the determination of system sensitivity and criticality, accomplishment of risk assessment and economic analysis, and determination of environmental hazards and threats to DON information systems.

**5239-18**, *Security Test and Evaluation Guidebook*

This document provides information on how to perform security test and evaluation (ST&E) for information systems, embedded computers, and networks. It addresses microcomputers, minicomputers, mainframes, and specialized computers in both stand-alone and networked environments. The instruction provides general guidance and procedures to security managers and users for conducting ST&Es.

**5239-19**, *Computer Incident Response Guidebook*

This document aids the ISSM, ISSO, and users in responding to security incidents involving computer penetrations or malicious code. The guidebook provides general guidance for planning activity response and specific procedures for coordination with NAVCIRT.

**5239-23**, *COMSEC Embedding Guidebook*

This document provides design guidelines for embedding INFOSEC modules.

**5239-26**, *Remanence Security Guidebook*, Published

This document provides policy, guidelines, and procedures for clearing and purging information systems memory and other storage media for release outside of and for reuse within controlled environments. The guidebook pertains to both classified and sensitive unclassified information and implements DOD 5200.28-M and CSC-STD-005-85.

**5239-29**, *Controls Over Copyrighted Computer Software*, Published

This document assists DON activities in developing and implementing their own policies and procedures for controlling and using computer software programs that have licensing agreements and copyright protection within the DON.

Marine Corps Computer Security IRM-5239 Publications

**IRM-5239-06**, *Data Access Security*

This publication provides guidance and information for accessing the ISs residing at the Marine Corps MegaCenter, St. Louis. Detailed procedures address the use of the resident security software packages (Top Secret/TSS and National Security/NSS) that limits access to authorized users only.

**IRM-5239-08**, *Computer Security Procedures*

This publication provides background information, guidelines, and policy referenced or contained in Public Laws, DoD, DON, and Marine Corps-related directives that are necessary to administer computer security practices in the Marine Corps.

**IRM-5239-09**, *Contingency Planning*

The publication provides procedures to effectively develop, maintain, and test the contingency/backup processing plan for essential ISs.

**IRM-5239-10**, *Small Computer Systems Security*

This publication discusses a wide scope of security considerations associated with the use of small computer systems (PCs and LANs). The key consideration in protecting the computer systems, which contain sensitive data, is for users and managers to develop a computer security mind-set.

**IRM-5239-12**, *Project Manager's Security Handbook*

This publication is used by a project manager or an acquisition sponsor to provide guidelines for ensuring that INFOSEC requirements are satisfied in the development and acquisition of computer resources.

**IRM-5239-13**, *System Security Plan (SSP)*

This publication provides the guidelines to prepare an SSP to ensure the security and privacy of each IS containing sensitive information. The SSP is a mandatory requirement under the Computer Security Act of 1987 Public Law [P.L.] 100-235) and OMB Bulletin 90-08.