



---

# **INFORMATION SYSTEMS SECURITY OFFICER (ISSO) GUIDEBOOK**

## **MODULE 07**

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



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 <http://infosec.nosc.mil/infosec.html/>.

Stocked: Additional copies of NAVSO P-5239-07 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-208-8230.

Local reproduction is authorized.



## FOREWORD

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. It consists of a series of modules providing procedural, technical, administrative, and supplemental guidance for all information systems, whether business or tactical. It applies to information systems 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 Information Systems Security Officer (ISSO) Guidebook, provides a description of the roles and responsibilities of the ISSO 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 ISSO. (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 ISSO 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 role of the ISSO 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 Unclassified But Sensitive 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. Security personnel at Commander-in-Chief, U.S. Atlantic Fleet (CINCLANTFLT), the Space and Naval Warfare Systems Command (SPAWAR), Naval Sea Systems Command Automated Data System Activity (SEAADSA), Headquarters, U.S. Marine Corps (HQMC), the Office of Naval Intelligence (ONI), Naval Security Group (NAVSECGRU), and Naval Command, Control and Ocean Surveillance Center, In-Service Engineering (NISE)-East were extremely helpful in providing information and guidance.



## TABLE OF CONTENTS

<b>1.0 INTRODUCTION .....</b>	<b>1</b>
Purpose .....	1
Policy and Guidance .....	1
Document Structure .....	1
<b>2.0 INFORMATION SYSTEMS SECURITY OFFICER ROLE .....</b>	<b>3</b>
Defined Roles .....	3
Qualifications and Prerequisites .....	4
Relationships .....	5
<b>3.0 INFORMATION SYSTEMS SECURITY OFFICER RESPONSIBILITIES .....</b>	<b>7</b>
<b>3.1 Security Management .....</b>	<b>7</b>
<b>SECURITY POLICY AND PROCEDURES APPLICATION .....</b>	<b>7</b>
Responsibility .....	7
Implementation .....	7
Policies and Procedures .....	7
Key Document Development .....	8
User Guidance .....	8
<b>COORDINATION WITH SECURITY PERSONNEL .....</b>	<b>9</b>
Responsibility .....	9
Implementation .....	9
Coordination Tools .....	9
Coordination with the ISSM .....	9
Coordination with and Oversight of the TASO .....	9
Coordination with Other ISSOs and NSOs .....	10
<b>COORDINATION WITH THE SYSTEM ADMINISTRATOR(S) .....</b>	<b>10</b>
Responsibility .....	11
Implementation .....	11
Formal Coordination .....	11
Daily or Routine Coordination .....	11
<b>POC FOR USERS .....</b>	<b>12</b>
Responsibility .....	12
Implementation .....	12
<b>3.2 Administrative Functions .....</b>	<b>13</b>
<b>ACCOUNTS ADMINISTRATION .....</b>	<b>13</b>
Responsibility .....	13
Implementation .....	13
Account Establishment .....	13
Account Termination .....	13
<b>IS ASSET ADMINISTRATION .....</b>	<b>14</b>
Responsibility .....	14
Implementation .....	14

## TABLE OF CONTENTS

IS Resources Control .....	14
Purging, Declassifying, and Downgrading Procedures .....	15
<b>MALICIOUS SOFTWARE CONTROL AND REPORTING .....</b>	<b>16</b>
Responsibility .....	16
Implementation.....	16
Malicious Software Control .....	16
User Guidance .....	16
<b>SECURITY “WATCHDOG” .....</b>	<b>17</b>
Responsibility .....	17
Implementation.....	17
<b>COMPUTER SECURITY TOOLBOX .....</b>	<b>18</b>
Responsibility .....	18
Implementation.....	18
<b>3.3 Training and Awareness .....</b>	<b>20</b>
<b>IS USER SECURITY TRAINING .....</b>	<b>20</b>
Responsibility .....	20
Implementation.....	20
Course Development and Conduct .....	20
Course Curriculum .....	20
Course Attendance .....	22
<b>SECURITY AWARENESS .....</b>	<b>22</b>
Responsibility .....	22
Implementation.....	22
<b>3.4 Physical Security .....</b>	<b>23</b>
<b>FACILITY ACCESS .....</b>	<b>23</b>
Responsibility .....	23
Implementation.....	23
<b>USER IDENTIFICATION AND AUTHENTICATION PROCEDURES .....</b>	<b>24</b>
Responsibility .....	24
Implementation.....	24
Data Control and Protection .....	24
System Utilities Protection .....	24
Authorized Use .....	24
Password Management .....	25
<b>DATA ACCESS .....</b>	<b>25</b>
Responsibility .....	25
Implementation.....	26
<b>ENVIRONMENTAL HAZARDS PROTECTION .....</b>	<b>26</b>
Responsibility .....	26
Implementation.....	26
<b>3.5 Auditing .....</b>	<b>27</b>
Responsibility .....	27
Implementation.....	27

## TABLE OF CONTENTS

Monitoring System Activity .....	27
Audit Trail Review .....	28
<b>3.6 Incident and Violations Reporting .....</b>	<b>29</b>
Responsibility .....	29
Implementation.....	29
Functions in Support of Reporting Mechanism .....	29
Incident Analysis .....	29
<b>3.7 Risk Management .....</b>	<b>31</b>
RISK MANAGEMENT PROGRAM .....	31
Responsibility .....	31
Implementation.....	31
REVIEW OF RISK ASSESSMENT .....	32
Responsibility .....	33
Implementation.....	33
SECURITY TEST AND EVALUATION .....	34
Responsibility .....	34
Implementation.....	34
<b>3.8 Accreditation .....</b>	<b>35</b>
Responsibility .....	35
Implementation.....	35
<b>3.9 Security Configuration Management .....</b>	<b>36</b>
Responsibility .....	36
Implementation.....	36
Inventory List Review .....	36
Library Maintenance .....	36
Change Management .....	37
Change Testing .....	37
<b>3.10 Contingency Planning .....</b>	<b>38</b>
Responsibility .....	38
Implementation.....	38
<b>3.11 Security Documentation .....</b>	<b>39</b>
System Security Plan (SSP) .....	39
Security Operating Procedures (SOP) .....	40
Authorized User List .....	41
Training and Awareness Documentation .....	41
IS Incident Report .....	41
Risk Assessment.....	41
ST&E Documentation .....	41
Plan and Procedures .....	41
Checklist.....	41
Report.....	42
Checklist.....	41
Report.....	42
Contingency Plan .....	42

**TABLE OF CONTENTS**

APPENDIX 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 to information systems. 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 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.

---

### **Purpose**

This guidebook is a module within the NAVSO P-5239 series of documents which have 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 ISSOs in implementing INFOSEC programs. Specifically, it describes the responsibilities of the ISSO and provides instruction for implementing these responsibilities.

---

### **Policy and Guidance**

Module NAVSO P-5239-07 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.

---

### **Document Structure**

Section 2 briefly describes the ISSO's role, qualifications and prerequisites, and working relationships. Section 3 describes the ISSO's responsibilities, which are 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 task areas are as follows:

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

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

## 2.0 INFORMATION SYSTEMS SECURITY OFFICER ROLE

The ISSO 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 Information System Security Manager (ISSM) provides input to the program manager regarding the appointment decision. If requested, the ISSM may provide technical assistance in the development of appointment memos or letters. The ISSO appointment letter briefly summarizes the duties and responsibilities of the ISSO. Depending on the Command structure, more than one ISSO may be appointed. Commands having complex ISs may need more ISSOs to perform day-to-day activities and to respond to security problems and IS user needs. For example:

- Multiple ISSOs may be assigned to a single, large IS
- Site-specific ISSOs may be assigned for geographically distributed ISs
- A single ISSO may be assigned within a Command for multiple ISs.

The ISSO is responsible for implementing and maintaining security for an IS on behalf of the ISSM. The ISSO reports to the Command's ISSM for INFOSEC matters and implements the overall INFOSEC program approved by the Designated Approving Authority (DAA).

---

### Defined Roles

The ISSO is responsible for the following:

- Ensuring that the IS is operated, used, maintained, and disposed of in accordance with Command security policies and practices (see Sections 3.1 through 3.10)
  - Enforcing security policies and safeguards on all personnel having access to the IS (see Sections 3.1 through 3.10)
  - Reporting the security status of the IS to the ISSM, as required by the DAA (see Sections 3.1 through 3.10)
  - Maintaining a System Security Plan (SSP) (see Sections 3.1 and 3.11)
  - Ensuring that TEMPEST measures have not been altered (see Section 3.2)
  - Ensuring that users and system support personnel have the required security clearances, authorizations (i.e., have been approved by a designated person of authority [e.g., Program Manager, Division Head, Commanding Officer] to perform work on the IS), and need-to-know (see Sections 3.2 and 3.4)
- 
- Ensuring that all computers display access warning banners (see Sections 3.2 and 3.3)
-

- 
- Conducting user training and awareness activities under the direction of the ISSM (see Section 3.3)
  - Working with physical security personnel to ensure the physical protection of IS assets (see Section 3.4)
  - Conducting security audits and ensuring that audit trails are reviewed periodically and that audit records are archived for future reference (see Section 3.5)
  - Creating a security incident reporting mechanism and reporting incidents to the ISSM when the IS is compromised (see Sections 3.6 and 3.11)
  - Initiating protective or corrective measures if a security problem is discovered (see Section 3.6)
  - Conducting the Risk Assessment of the IS using the methodology determined by the ISSM and approved by the DAA (see Sections 3.7 and 3.11)
  - Ensuring that the IS is accredited (see Section 3.8)
  - Assisting the ISSM in IS configuration management activities to ensure that implemented changes do not compromise the security of the system (see Section 3.9)
  - Providing technical contributions to the ISSM for the development of contingency plans for the IS for which he or she is responsible (see Sections 3.10 and 3.11).
- 

**Qualifications and Prerequisites**

No specific formal college or other degree program is required for the ISSO. 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 ISSO must associate with staff at all levels of the organization. An ISSO should have:

- Two years of experience in a computer-related field
- One year of working experience in INFOSEC
- An understanding of the operational characteristics of the IS
- Education and training in computer science, mathematics, electrical engineering, and related fields
- Periodic attendance at an appropriate-level INFOSEC training course.

The ISSO'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 courses. Some Commands offer computer based training

---

---

(CBT). The ISSO should be familiar, through work experience, with the needs and responsibilities of the Terminal Area Security Officer (TASO) and Network Security Officer (NSO).

---

**Relationships**

In executing security responsibilities, the ISSO interacts with personnel both 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.

---

**Personnel/Activity**

**INFOSEC Role**

DAA

The DAA is responsible for ensuring compliance with the DON INFOSEC Program for the activities and ISs under the DAA's jurisdiction. The DAA grants interim and final approval to operate an 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.

ISSM

The ISSM acts as the focal point and primary point of contact for all security matters pertaining to the IS under the purview of the ISSM. 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 ISSO reports to the ISSM for security matters.

NSO

The NSO acts on behalf of the Network Security Manager (NSM) or ISSM to implement the network security policy of the activity across all data networks at the activity under his/her authority, and serves as the point of contact for all network security matters .

TASO

The TASO is responsible to the ISSO for compliance with security procedures at an assigned remote terminal area. Depending on the Command size and structure, multiple TASOs are typically assigned.

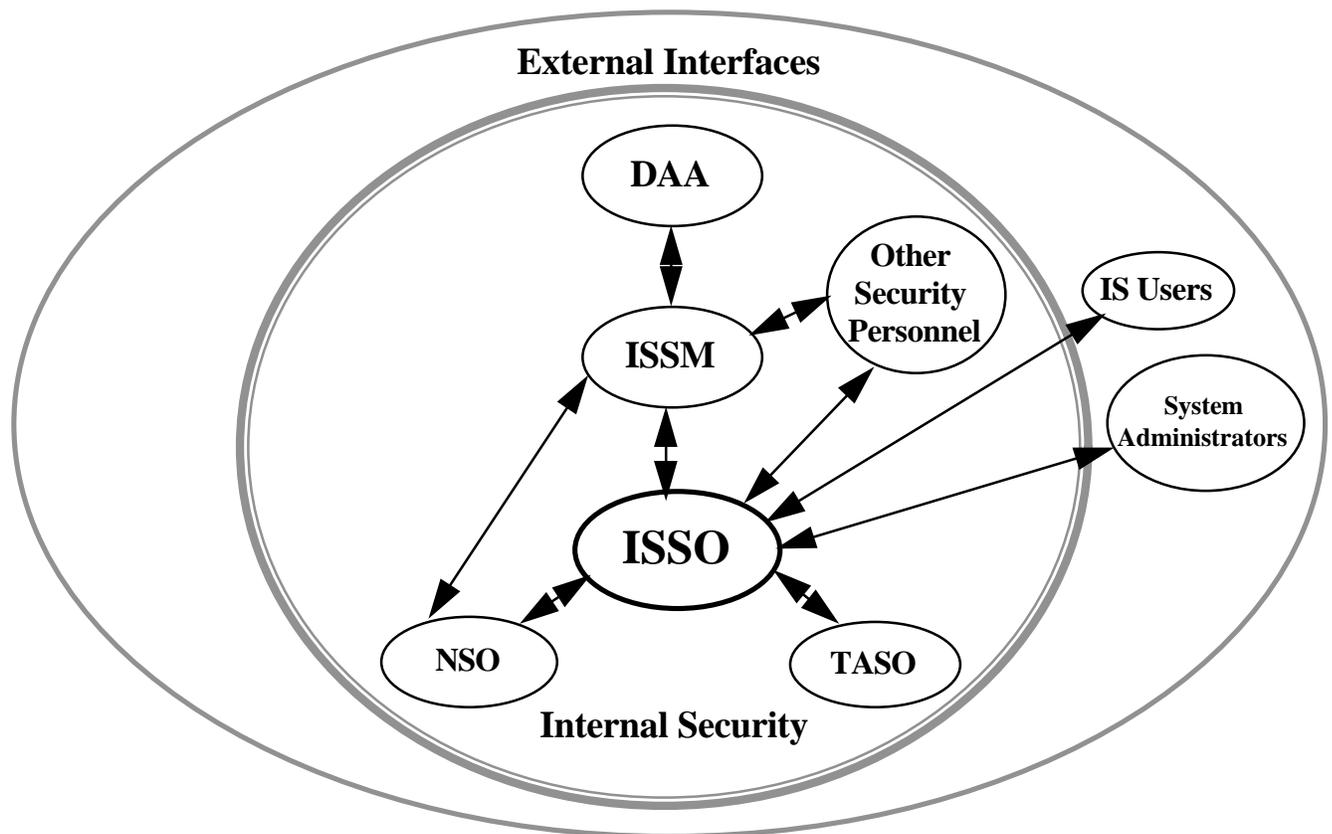
Other Site Security  
Personnel

Other security-related billets are filled 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 ISSO coordinates with other security personnel to ensure the consistent implementation of security policies and procedures.

**User** In this document, the term “user” refers to all personnel who access the IS for authorized purposes and in accordance with security procedures and guidelines (i.e., users, operators, and maintainers). The ISSO ensures that the IS users are aware of their security responsibilities and are trained in the user security features of the IS.

**System Administrator** The System Administrator, who is responsible for the administration and operation of an IS, works with the ISSO to ensure that the IS operates in accordance with Command security policies and procedures. The System Administrator may also be the ISSO for his or her particular ISs.

Figure 1 illustrates the working relationship of the ISSO with these other security and nonsecurity personnel.



**Figure 1**  
**ISSO Relationships to Other Personnel**

### **3.0 INFORMATION SYSTEMS SECURITY OFFICER RESPONSIBILITIES**

The ISSO is responsible for ensuring that users comply with the INFOSEC program requirements and procedures. The ISSO accomplishes this by performing, directing, coordinating, administering, and overseeing various activities and personnel. This section defines the responsibilities of the ISSO in each of the task areas previously identified.

#### **3.1 Security Management**

This section describes the responsibilities of the ISSO 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 INFOSEC program.

---

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

---

**Responsibility** The ISSO maintains a thorough understanding of security policy and procedures applicable to the specific IS. If required, the ISSM, or higher authority, clarifies the application of security policy and procedures. The ISSO disseminates INFOSEC policies and procedures to IS users and ensures that users abide by these policies and procedures.

#### **Implementation**

**Policies and Procedures** The ISSO researches and analyzes current DOD, DON, and any Command-level directives, guidelines, regulations, and policies that address INFOSEC and that apply to his or her specific Command or activity. This ensures that the ISSO is aware of and abides by applicable security requirements. As guided by the ISSM, the ISSO applies knowledge of DOD and DON policies through participation in the development of key IS-specific documentation (discussed in the following paragraphs). Additionally, the ISSO reviews site and/or system-specific technical documentation, such as the Trusted Facility Manual (TFM) and the Security Features User's Guide (SFUG). The ISSO may be delegated to provide input to the update of the TFMs and SFUGs or other site or system-specific security documentation. The

---

ISSO maintains a data repository of all applicable policy, procedures, guidelines, and other related technical documentation to serve as an easy reference for all IS users. The use of on-line documentation (e.g., Hyper Text Markup Language [HTML]) is encouraged.

---

**Key Document  
Development**

The ISSO is responsible for developing and maintaining System Security Plans (SSP) for every DON IS under his or her cognizance.

The ISSO also develops and maintains site-specific Security Operating Procedures (SOP). Some Commands may require the development of multiple SOPs for each IS because the subject matter of each SOP may be geared for different audiences (e.g., an SOP for system administrators and an SOP for system users).

---

**User Guidance**

The ISSO provides guidance and oversight to IS users in the interpretation and implementation of 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 ISSO also supervises IS user work practices to ensure that policies and procedures are adhered to 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 (commonly referred to as “the Rainbow Series”), respectively. For more information concerning the SSP and the SOP, see Section 3.11, Documentation. NAVSO P-5239-11, System Security Requirements Development, provides guidance for developing system-specific security policy and requirements. For more information concerning the ISSO’s role regarding IS users, see “POC for Users” (in this section), and Section 3.3, Training and Awareness.

---

---

## COORDINATION WITH SECURITY PERSONNEL

---

**Responsibility**      The ISSO coordinates with INFOSEC personnel to ensure that security policies and procedures are uniformly implemented. Other security personnel include ISSMs, TASOs, NSOs, other ISSOs, and personnel in other security departments within the Command, such as personnel, physical, industrial, and operations.

---

### Implementation

**Coordination Tools**      The ISSO participates in security status meetings to keep informed of all activities, problems, and issues relevant to INFOSEC and to report 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 employees and employee terminations
- Recent computer virus attacks
- New procedures required to access a particular system
- Combination lock changes
- Command reorganizations
- Needed and/or new security services.

The ISSO will also formally coordinate activities among security departments through internal memos.

---

**Coordination with the  
ISSM**

The ISSO interacts regularly with the ISSM to:

- Report status concerning ISSO work efforts
  - Seek guidance concerning work activities, problems, and issues
  - Provide input to documentation developed primarily by the ISSM, such as risk assessments, contingency plans, and accreditation documentation
  - Receive input on documentation developed primarily by the ISSO, such as SSPs, SOPs, Access Lists, and Incident Reports.
- 

**Coordination with and**

The TASO, if appointed at the specific Command, is responsible for

---

---

**Oversight of the TASO** security procedures in an assigned remote terminal area. The ISSO maintains administrative authority over the TASO for INFOSEC matters and ensures that the TASO receives adequate security training and written security requirements and SOPs for the remote area. The ISSO oversees the TASO's INFOSEC efforts and provides guidance and direction to the TASO as needed for correct implementation of Command security policies and procedures applicable to remote operation.

The ISSO ensures that the TASO understands and maintains responsibility for the following duties:

- Verifies that physical security controls are in place and operational (i.e., ensures protection against physical hazards, fire, water, theft, or abuse)
- Allows IS terminal access only to users with the appropriate "need-to-know" clearances, and formal access approvals
- Ensures that terminal users follow and implement Command IS policies and procedures
- Performs an initial evaluation of security problems in the assigned terminal area(s) and notifies the ISSO of security incidents or violations
- Collects and reviews remote facility audit records and forwards this data to the ISSO for analysis and further action
- Notifies the ISSO of personnel who have transferred, been terminated, or who, for other reasons, no longer require IS access.

Should a TASO not be assigned, the ISSO is responsible for implementing the TASO INFOSEC role and associated tasks.

---

**Coordination with Other ISSOs and NSOs**

In some cases, Commands have multiple ISSOs and/or NSOs, either geographically distributed or within a single, large IS. In these instances, coordination among ISSOs and NSOs is inherently necessary to ensure the consistent implementation of Command policies and procedures. This coordination and cooperation may take the form of meetings and memos, as discussed above, or may simply be informal exchanges, depending on the Command structure and preference.

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

---

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

---

**Responsibility** The ISSO coordinates with system administrators to ensure that operation and administration of the IS are in accordance with Command security policies and procedures. Coordination with system administrators is of utmost importance because they are responsible for maintaining the IS.

---

## **Implementation**

**Formal Coordination** The ISSO participates in periodic status meetings with system administrators to stay apprised of all activities affecting INFOSEC. To avoid excess meetings, the system administrators may be invited to attend internal security meetings (discussed previously) as applicable (i.e., information relevant to IS administration is discussed). The meetings will focus on such topics as:

- Proposed changes to the system
  - Proper implementation of changes
  - User status
  - Recent computer virus attacks and actions required to combat them
  - New policy and procedures implementation
  - IS problems and issues relating to security.
- 

**Daily or Routine Coordination** On a daily or otherwise routine basis, the ISSO coordinates with system administration staff to follow through on meeting action items and to coordinate routine operations.

These activities include:

- Coordinating the addition of new user accounts and the termination of accounts
- Reviewing system administrator-generated computer inventory list(s)
- Coordinating actions required for incidents and violations (e.g., virus management/reporting)
- Coordinating and overseeing implementation of ISSM/DAA-

approved system changes and changes in security operating procedures

- Ensuring that system backups are performed regularly
-

- 
- Coordinating and overseeing the implementation of purging and clearing requirements
  - Coordinating audit trail review efforts
  - Coordinating or providing input to miscellaneous administrative tasks relating to the security of the system.

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

---

## **POC FOR USERS**

---

**Responsibility**      The ISSO provides assistance and direction to users regarding INFOSEC matters, questions, and problems.

---

**Implementation**      The ISSO is responsible for:

- Conducting user training (if delegated by the ISSM) and ensuring that users are aware of, understand, and correctly implement all 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 IS (e.g., new/replacement software, relocating components, upgrading classification labeling of system/component) without prior approval from the ISSO
- Ensuring that departing users' accounts are terminated and that data is examined for evidence of tampering.

*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 ISSO performs a variety of administrative tasks related to the IS. The activities within the administrative functional area range from ensuring that accounts are opened, maintained, and closed correctly to protecting the IS and its information.

---

### ACCOUNTS ADMINISTRATION

---

**Responsibility** The ISSO coordinates new IS user accounts establishment and termination procedures to ensure the security of the IS.

---

#### Implementation

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

- 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 PERSEC data bases, avoid replication of existing data bases)
- 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 system administrators to open new accounts and verifies that new accounts are added correctly
- Ensures that new users are trained in applicable INFOSEC requirements, responsibilities, and procedures.

**Account Termination** The ISSO ensures the expeditious closure and termination of IS accounts of departing personnel. The ISSO:

- Coordinates with the Command's physical and personnel security departments to delete users from physical and IS authorized user lists
  - Coordinates with the Command's physical and personnel security departments to ensure that all physical access materials (e.g., tokens and cards) are returned by the user
  
  - Coordinates with the Command's physical security department to ensure that locks are changed each time a user is terminated,
-

---

and on a routine periodic basis in accordance with the Command's security policies

- Coordinates with the system 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 Security.

---

## IS ASSET ADMINISTRATION

---

### **Responsibility**

The ISSO ensures the accountability and protection of IS 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**

#### **IS Resources Control**

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

The ISSO coordinates with the system administrators for controlling IS media resources and maintaining an inventory of IS components. The ISSO:

- Provides guidance, based on Command policy, to the system administrators regarding the protection of IS media resources, such as:
    - Securing classified components, software, and other material
    - Preventing unauthorized access to the system
    - Preventing damage of IS equipment due to natural hazards (water, fire, extreme temperatures, etc.)
  - Ensures that system administrators perform regular (in accordance with Command policies) total and differential backups on a schedule based on deliberate consideration of probable failures leading to losses and costs
-

- Ensures that periodic copies of mission-critical file backups are rotated to a secure off-site location
- Reviews the system administrator-developed inventory list regularly to keep abreast of IS component changes or relocation. (The ISSO maintains a current copy of the IS inventory list.)
- Reviews system change plans (e.g., relocation of components, software upgrades, disposal of components) and provides guidance regarding the implementation of changes
- Ensures that maintenance personnel do not alter TEMPEST characteristics of applicable equipment and have been granted only those privileges required to perform maintenance.

The ISSO ensures that IS users are educated in the Command's policies and procedures for marking, handling, storing, disposing of, and accounting for classified and unclassified IS hardware, software, and firmware by:

- Disseminating SOPs
- Providing instruction and demonstration during IS user training sessions
- Providing assistance and oversight to users on a daily or as-required basis
- Conducting unannounced spot checks of IS media resources and log books to ensure correct implementation of security policies and procedures.

---

**Purging, Declassifying,  
and Downgrading  
Procedures**

The ISSO coordinates with the system administrators and cognizant security department(s) to develop and implement purging, clearing, and media labeling procedures. The ISSO 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 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, the application of these degaussers, and manufacturer information.

---

---

## MALICIOUS SOFTWARE CONTROL AND REPORTING

---

**Responsibility** The ISSO ensures that proper measures are taken to protect the IS from computer viruses and other malicious software.

---

**Implementation** The ISSO, as directed by the ISSM, works with system administrators to implement DON-approved software to protect the IS against viruses and other malicious software. This includes using VKIT, from the Computer Security Toolbox, to create and distribute virus scanner disks and utilities.

**Malicious Software Control** The ISSO works with system administrators to implement procedures for reporting actual or suspected incidents of malicious code or virus attacks. This reporting mechanism ensures that virus attacks are expeditiously dealt with and reported to the Naval Incident Response Team (NAVCIRT) (which is a component of the Fleet Information Warfare Center [FIWC]) by the ISSM. Suspected virus attacks should be reported to NAVCIRT at (800) 628-8893 or e-mail: *navcirt@fiwc.navy.mil*.

**User Guidance** The ISSO ensures that IS user training sessions include pertinent discussion of malicious code, including computer viruses. The discussion should cover:

- The dangers of malicious code, how it is spread or transmitted, and what it affects
  - Types of system occurrences that imply possible malicious code infection
  - Malicious code protection methods, for example:
    - Using automated detection tools
    - Using authorized software only
    - Installing “safe” software (scanned for malicious code) only
    - Storing virus-free, write-protected backup disk copies of vital executable programs and operating software
-

- Performing regular backups
- Preventing unauthorized access to system
- Malicious code reporting procedures
- Virus attack process
  - Tracking a virus (determining origin and type, who or what has been affected)
  - Cleanup (who conducts, estimated downtime, 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 ISSO monitors system use and conducts random floor and system component checks to ensure that Command security policies and procedures are followed.

**Implementation** When conducting floor checks, the ISSO should be alert to the following:

- Are SOPs and other Command-specific policies and procedures being adhered to?
- Does the system software configuration match the documented configuration?
- Is virus scanning software used consistently?
- Are log-on warning banners at every entry point and are forms signed indicating users’ consent-to-monitoring in accordance with current, applicable DON policy?
- Are computers left in the “active” mode (users logged on), leaving

the system vulnerable to misuse?

- Are unauthorized persons on the premises or using the system?
  - Are personnel following procedures when using classified systems? For example:
    - Are physical administrative security measures being followed before each use of the IS?
    - Are terminals disconnected from networks and/or peripherals that are not approved for classified processing?
    - Are classified operating system and applications software
-

- 
- 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 (including magnetic media and hardware components)?

The ISSO reports incidents and violations through the 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 ISSO ensures adequate control, dissemination, and use of the DON Computer Security Toolbox. 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 ISSO aides the user in implementing the Toolbox, a set of automated software programs (tools), for the performance of various security functions. These tools range from password generating programs to tools to eliminate "object reuse" issues faced by MS-DOS users. The Toolbox aids in complying with Controlled Access Protection (CAP) requirements. The Toolbox consists of the following.

- **TOOLBOX:** The "TOOLBOX" program is the controlling program for the Computer Security Toolbox. Its basic function is to create 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 important, they may contain hidden classified information or files. The person generating the data or information has the responsibility to 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 may be edited using any editor and contains one word or phrase per line. Typically, it contains all the paragraph markings used in classified documents. These may be spelled out completely or abbreviated. Additionally, project coverterms, covernames, nicknames, SPECAT Codewords, etc., may be entered into LIMITS.TXT. When a match occurs, the program pauses for review of the "matched" item(s).
- VKIT: The Virus Kit (VKIT) Generation process can be used to create a virus scanning disk. It 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 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 ISSO receives position/Command-specific security training from the 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 System Security Specialist Course offered by the USMC Computer Sciences School, and the National Institute of Standards and Technology/National Computer Security Center National Computer Security Conferences. If delegated, the ISSO conducts user training and awareness activities under the direction of the ISSM.

---

#### IS USER SECURITY TRAINING

---

**Responsibility** In accordance with the Computer Security Act of 1987, all IS users must receive periodic INFOSEC training. If delegated by the ISSM, the ISSO develops (or participates in the development of) user training curriculum and conducts user training sessions as guided by the ISSM.

---

#### 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. Soft copy versions of documents on removable computer media can serve as cost-effective substitutes for hard-copy versions. The Command or Activity may use CBT, if available and applicable.

---

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

- Value of computer-based information
    - Historical data
    - Personnel files, payroll data, legal records
    - Trade secrets/proprietary data
    - Documentation vital to national security
  
  - Computer vulnerabilities
    - Human errors
-

- Misuse of the system (e.g., procedures not followed, data used for illegal purposes, “browsing”)
  - Computer viruses
  - Unauthorized use (e.g., hackers using networks to steal information)
  - Natural hazards (e.g., fire, smoke, static electricity, extreme temperatures, humidity, magnetic forces)
  - Basic safe computing
    - Accessing data (use only data/software/systems needed for particular job)
    - Using keyboard or system locks
    - Leaving computers unattended
    - Disposing of unneeded data
    - Using classified and sensitive unclassified data
    - Handling sensitive information
    - Backing up data
    - Using unauthorized software
    - Protecting software
  - Password management
    - Generating unique password
    - Protecting passwords (i.e., confidentiality)
    - Changing passwords
  - Command-specific security procedures ; for example:
    - Using security products (e.g., safes, cipher locks, burn bags, classified disks)
    - Relocating system components
    - Changing system software and hardware
    - Reporting security violations/suspected violations (e.g., point of contact, reporting process)
  - Explanation and demonstration of security mechanisms and safeguards on the IS
  - Explanation of the purpose of log-on warning banners
  - Importance of self-monitoring (e.g., identify successful and unsuccessful logons to aid in monitoring attempts by unauthorized personnel to access the system)
  - Importance of being alert to suspicious or unusual activity.
-

**Course Attendance** Training attendees should be required to sign attendance sheets acknowledging their role in protecting IS assets. The ISSO maintains this information and can use it as the basis for annual refresher training.

---

## **SECURITY AWARENESS**

---

**Responsibility** The ISSO assists the ISSM in fostering user security awareness.

---

**Implementation** The following are commonly used approaches to heighten user security awareness:

- Develop and distribute security awareness posters
- Display warning messages or log-on warning banners on the IS. Ensure that users are aware that all activity on the IS is monitored by requiring users to sign monitoring consent forms (in accordance with current, applicable DON policy)
- Disseminate new security information and security reminders through memos, newsletters, and automated bulletin boards
- Provide hands-on demonstrations of INFOSEC features and procedures.

---

### 3.4 Physical Security

This section describes the ISSO's roles and responsibilities in the physical protection of IS assets. Physical security is the protection and preservation of informational, physical, and human assets through the reduction of exposure to various threats that can produce a disruption or denial of IS services or unauthorized disclosure. These measures include protections against loss or damage from:

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

Measures implemented depend on the site-specific environment and the classification level of the data being handled by the IS.

The ISSO works with physical security personnel to ensure that facility access controls (i.e., physical access to the system, logical system access [identification and authentication], and logical access to files and other objects [data access] are in place. The ISSO also works with physical security personnel to ensure that the IS is adequately protected against natural hazards.

---

#### FACILITY ACCESS

---

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

---

**Implementation** The ISSO is responsible for:

- Establishing and implementing procedures to control IS equipment entering and exiting the IS site
- Ensuring that authorized user lists are posted at entrances and continually updated
- Ensuring that restricted area/authorized personnel-only signs are appropriately posted, if required

---

- 
- Providing input to the Security Manager for the development and maintenance of a facility security plan that includes architectural drawings and building plans, floor plans, and inventories
  - Ensuring that maintenance contractors are supervised by an authorized person
  - Ensuring that locks, bars, and other physical safeguards are sufficient and in place as required by Command policy (including the routine changing of locks and combinations in accordance with Command policies and security operating procedures).
- 

## **USER IDENTIFICATION AND AUTHENTICATION PROCEDURES**

---

**Responsibility**            The ISSO implements Command policies and procedures to accurately authenticate the claimed identity of IS users to protect the IS from unauthorized use.

---

### **Implementation**

**Data Control and Protection**            The ISSO ensures that identification & authentication (I&A) data is accessible by an absolute minimal number of authorized personnel, including the ISSM, ISSO, and, if necessary, system administrators. The authentication database contains user authentication information, such as passwords, and must be tamper proof to protect the integrity of the system.

---

**System Utilities Protection**            The ISSO works with system administrators to ensure that only authorized personnel (i.e., ISSO and system administrators) have access to and are able to execute system utilities capable of circumventing or damaging INFOSEC data or executables.

---

**Authorized Use**            The ISSO works with the personnel security department to maintain an accurate list of authorized IS users, including contractors and visitors. This list contains the user name, user identifier, access level, and whether the user has administrator privileges. The ISSO ensures that the monitoring of visitors and contractors is conducted with a higher level of

---

---

scrutiny than that of permanently assigned personnel. The ISSO:

- Ensures that all users, including visitors or contractors, have the necessary clearances and authorized access only to that data for which “need-to-know” is established
- Ensures that all visitors or contractors are monitored while using the IS
- Ensures that accounts for personnel leaving the Command are terminated expeditiously.

---

**Password  
Management**

The ISSO provides guidance to IS users for developing and using passwords. The ISSO instructs users to:

- Choose nondictionary-unique passwords (birth dates and common names should be avoided)
- Keep passwords confidential at all times
- Memorize passwords (ensure that they are not accessible by others)
- Change passwords periodically, in accordance with Command policy, or immediately if compromise is suspected
- Notify the TASO or ISSO if a password does not work or if unauthorized use is suspected.

The use of automated password generators, such as PASSGEN, from the Computer Security Toolbox, is 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. For additional I&A guidance, see NAVSO P-5239-15, Controlled Access Protection (CAP) Guidebook.

---

**DATA ACCESS**

---

**Responsibility**

The ISSO implements measures to prevent disclosure of information to unauthorized individuals.

---

**Implementation**

The ISSO ensures that procedures are in place to:

- Ensure that site-specific discretionary access control (DAC) and mandatory access control (MAC) policy is defined and implemented. The policy should define the standards and regulations that the ISSO must implement to ensure data is disclosed only to authorized individuals.
- Control access to all functions that affect security or integrity of the system. Access of this type should be limited to a minimum number of personnel.
- Ensure that access control mechanisms or software is installed and operated in a manner that supports the INFOSEC policy.

*Reference:* For additional guidance see NAVSO P-5239-15, Controlled Access Protection (CAP) Guidebook.

---

**ENVIRONMENTAL HAZARDS PROTECTION**

---

**Responsibility**

The ISSO coordinates with the Physical Security Department to ensure that measures are in place to protect the IS from environmental or natural hazards.

---

**Implementation**

At a minimum, the ISSO works with the Physical Security and Facility Maintenance/Public Works personnel to ensure that:

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

### 3.5 Auditing

Practices inconsistent with the security policy of the IS must be identified and eliminated. Monitoring the security activities of the IS and conducting an audit of security-related activity on the IS 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 limit or eliminate such practices through user education and, if necessary, administrative discipline. This section describes the ISSO's role in monitoring security-related activities on the IS.

---

**Responsibility** The ISSO is responsible for conducting security audits on the IS and for monitoring variances in security procedures. The ISSO ensures that security alarms are in place and functioning properly. Additionally, the ISSO reviews audit logs and audit trail data to identify and analyze security-related weaknesses and opportunities for refinement and efficiency. Further, the ISSO reports to the ISSM on the effectiveness of security policy and procedures, and recommends improvements.

---

#### Implementation

**Monitoring System Activity** The ISSO uses automated audit mechanism to monitor actions such as:

- Successful and unsuccessful logon attempts
- File accesses
- Types of file access (create, write, read, change, delete)
- Password changes.

The ISSO ensures that:

- Audit and review procedures are developed and implemented to ensure that all IS functions are performed in accordance with IS 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
-

- Unusual system activities are identified and investigated
- Random floor checks are conducted.

*Reference:* See Section 3.2, Administrative Functions, for information on the ISSO Security “Watchdog” role.

---

**Audit Trail Review**

The audit trail provides a record of security-related activity on the IS. The ISSO reviews the audit trail reports for:

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

The ISSO also uses the audit trail report to create user profiles from information such as:

- Records of user logons and logoffs
- Access attempts on servers, folders, and files.

*Reference:* For additional guidance on C2 requirements, see NAVSO P-5239-15, Controlled Access Protection (CAP) Guidebook.

---

### 3.6 Incident and Violations Reporting

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

- Suspected or confirmed viral infection
- Intrusion attempts and successes within the IS, such as:
  - Remote users logging in with compromised passwords
  - Compromised administrative privileges, allowing the creation and utilization of false user accounts.
- Access denials, such as:
  - Incorrect password violations
  - Incorrect account/user names
  - Unauthorized access to certain files, directories, servers, or other resources on the IS
- Unauthorized modification of DAC and audit procedures.

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

---

#### Responsibility

All suspected incidents or violations must be reported immediately, first by the ISSO to the ISSM and then, after analysis by the 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 ISSO is responsible for creating the incident reporting mechanism.

---

#### Implementation

##### Functions in Support of Reporting Mechanism

The ISSO supports the successful and effective review of reported incidents by:

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

#### Incident Analysis

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

---

---

actions:

- Analyzing the effects of an incident in the context of risk and degree of compromise
- Reporting results of analysis to the DAA via the ISSM
- Recommending appropriate action to the DAA via the ISSM, such as:
  - Termination of user privileges
  - Increasing auditing activity
  - Increasing protection levels and security mechanisms
  - Suspension of all noncritical IS activity
  - Complete system shutdown.

*Reference:* For more information, see Section 11, Documentation, for a description of an incident report and NAVSO P-5239-19, Computer Incident Response Guidebook.

---

### 3.7 Risk Management

The Risk Management Program includes the process of identifying, measuring, and minimizing events affecting IS resources. The program includes the security activities that span the life cycle of an IS. Risk management determines the value of the data, which protections exist, and how much more protection (if any) the system needs. Risk management determines the value of all system 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 system security features. Risk management includes risk assessment, countermeasure selection, security test and evaluation, contingency planning, and system review. The results of these activities provide the information on which a DAA can base an accreditation decision. Risk management activities do not end with an accreditation decision. Ongoing analysis throughout the life cycle ensures that security requirements are always met. The ISSO performs risk management activities under the direction of the ISSM.

---

#### RISK MANAGEMENT PROGRAM

---

##### **Responsibility**

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

- Specific threats and vulnerabilities to the IS are identified
- Countermeasures to mitigate the identified risk are identified and applied
- The effectiveness of the implemented security controls is tested
- The continued effectiveness of the implemented security measures is reviewed.

The primary responsibility of the ISSO is to conduct the Risk Assessment of the IS using the methodology determined by the ISSM and approved by the DAA.

---

##### **Implementation**

The ISSO performs the risk assessment according to the methodology prescribed by the 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 a stand-alone system, local

area networks (LAN), wide area networks (WAN), and integrated site

---

ISs. The ISSO:

- Recommends the risk assessment type to the ISSM based on the risk assessment selection chart
- Receives approval of the type from the ISSM
- Performs the approved risk assessment using one of the following risk types:
  - Survey risk assessment
  - Basic risk assessment
  - Intermediate risk assessment
  - Full risk assessment.
- Performs the risk assessment by completing the checklist and forms indicated for the specific type. The result of the assessment is the identification of risk to the IS.
- Submits the completed risk assessment to the 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 ISSM, the ISSO recommends safeguards to counteract the vulnerabilities identified in the risk assessment.

The ISSO recommends countermeasures based on risk level and cost effectiveness. The level of risk, the severity of the security problem, and the level of impact on resources will dictate the need for the countermeasure. The countermeasures examined should include:

- Technical safeguards
- Physical safeguards
- Administrative safeguards.

If, for instance, the risk assessment indicates that weak access controls create a risk of compromise of information, the ISSO 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 mainframe security product would be a technical software countermeasure; the use of a room key would be a physical countermeasure; the use of a guard checking an access control list would be an administrative countermeasure. When directed, the ISSO provides a countermeasure selection recommendation to the 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. An updated risk assessment is performed, at a minimum, every 3 years. The ISSO periodically reviews the risk assessment and modifies it to accommodate new threats because of changed configuration or changes in the operational environment. When a modification to the system invalidates 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 changes.

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

---

## **Implementation**

The ISSO documents and reports the INFOSEC technical vulnerabilities detected in ISs to the ISSM.

The ISSO administers the technical vulnerability reporting program and:

- 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, 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 an IS. ST&E is a process that determines if the installed countermeasures identified in the Risk Assessment are working effectively. The risk assessment type performed defines the level of detail.

---

**Implementation** The ISSO assists the ISSM in the planning and execution of the ST&E. The activities may include:

- Compiling resources (including the team, the hardware, software, media, the functioning system)
- Establishing the security baseline
- Providing system documentation ( e.g., user, operator, administrator manuals) and security regulations (the use of on-line network resident documentation [e.g., HTML] is encouraged)
- Ensuring work space and storage for the team
- Ensuring the development of ST&E plans and procedures
- Monitoring the ST&E inspections
- Ensuring that the ST&E log that records daily activities is maintained
- Witnessing the testing
- Ensuring the development of ST&E reports
- Maintaining a file of working papers concerning the security tests.

The ISSO may participate in the development of the ST&E plans, procedures, and report. The risk of unintentional bias by the ISSO in test writing is mitigated by the review of the ISSM.

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

---

### 3.8 Accreditation

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

---

<b>Responsibility</b>	The ISSO provides support to the ISSM and the DAA throughout the accreditation process.
<b>Implementation</b>	<p>The ISSO assists in the accreditation of an IS by providing the following support:</p> <ul style="list-style-type: none"><li>• By assisting in the preparation of the accreditation material, such as the identification of residual risk to the IS. This identification is based on the results of the risk assessment conducted on the IS. The results of the ST&amp;E are also included in the accreditation package.</li><li>• By assisting in site surveys. The ISSO provides support to the DAA if the DAA elects to visit the site to inspect the IS before making the accreditation decision.</li><li>• By assisting in the evaluation of the accreditation package. The ISSO examines the contents of the accreditation package to be provided to the ISSM and the DAA to ensure that the documentation supports the recommendations for an accreditation decision.</li><li>• By coordinating the accreditation package with the ISSM. The ISSO provides the contents of the accreditation package to the ISSM for delivery to the DAA.</li></ul>

---

### 3.9 Security Configuration Management

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

---

#### Responsibility

In accordance with the DAA's policies and procedures for controlling changes to the IS, the ISSO assists the ISSM in providing input to, or actively participating in, IS configuration management activities to ensure that implemented changes do not compromise the security of the system.

---

#### Implementation

##### Inventory List Review

The ISSO reviews the IS inventory, as documented by the system administrator, to ensure that system components have not changed, been relocated, or otherwise been tampered with in any way that may alter the overall security of the IS. The ISSO then highlights changes and provides a status report to the ISSM that summarizes the nature (estimated security impact, if any) of changes along with a copy of the inventory list.

---

##### Library Maintenance

The ISSO maintains a library of the documentation detailing the IS hardware, software, and firmware configuration and security features. On-line libraries are encouraged. This material may be useful when determining the impact of security problems or flaws in the system and the necessary corrective measures.

---

**Change Management** The ISSO conducts an initial review of IS change proposals regarding the following criteria:

- How will the change impact the security of the IS?
- If new software is proposed, is it from an authorized source?
- Have security features and mechanisms been considered and included in system change plans?
- Do system support personnel know how to install and maintain new security features/mechanisms?
- Will reaccreditation be necessary?

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

---

**Change Testing** The ISSO witnesses and conducts, where possible, tests to ensure that:

- Implemented changes have not degraded the security of the system
  - Security features and mechanisms are fully functional .
-

### 3.10 Contingency Planning

Contingency Planning requires the formulation of the strategy (plan) and the procedures for implementation to respond to the unplanned disruption of service to an IS. This planning ensures that the impact of incidents, accidents, or disasters on the mission is measured. The plan documents emergency response, backup procedures, and postdisaster recovery procedures. Activities develop a Contingency Plan for each IS for which unplanned disruption of service would have a critical impact on mission accomplishment. A Contingency Plan is not required for ISs for which the unplanned disruption of service would not have a critical impact on mission accomplishment. In these cases, a written statement eliminating the requirement should be included in the accreditation package.

---

**Responsibility**

Although the ISSM is responsible for the development of a contingency plan for each IS, the ISSO provides technical contributions concerning contingency planning for the IS for which he or she is responsible.

---

**Implementation**

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

*Reference:* See Section 11, Documentation, for a description of a contingency plan and Federal Information Processing Standards (FIPS) Publication 87, dated 27 March 1981.

---

### 3.11 Security Documentation

The following documents, appearing in the order in which they are referenced in this guidebook, are typically prepared by INFOSEC personnel. The use of on-line IS resident documentation (e.g., HTML) is encouraged.

---

#### **System Security Plan (SSP)**

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 to 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 to be requested)
  - Support Personnel (ISSM, ISSO, System 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 & 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 (SOP)**

Current DON policy requires that security procedures be developed, documented, and presented to all users of ISs. Topics of discussion should include, but are not limited to policy statement, 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 ensures that SOPs are reviewed annually for accuracy.

---

---

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

---

**Training and Awareness Documentation** The purpose of training and awareness documentation is to continually 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 can consist of posters, newsletters, videos, warning messages, etc., to reinforce the need for protection.

---

**IS Incident Report** The IS incident report provides an explanation of the type of incident, the individuals involved, the estimated cost of the incident, a summary of the incident, and the investigation results, along with the supervisor's recommendations and the local action to prevent reoccurrence.

---

**Risk Assessment** A Risk Assessment identifies the threats, vulnerabilities, and risks to an IS. 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.

---

**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 deemed unnecessary by the DAA, as determined by the complexity of the IS and the level of risk. The checklists help ensure that the 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:* NAVSO P-5239-18, Security Test and Evaluation Guidebook, provides guidance and procedures for conducting ST&E.

---

**Contingency Plan**

The Contingency Plan, developed primarily by the ISSM, 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. Activities develop a Contingency Plan for each IS for which unplanned disruption of service would have a critical impact on mission accomplishment. A Contingency Plan is not required for ISs 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 system determines details of Contingency Plan.

---

## **APPENDIX A**

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



## 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 that 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 (Changes 1 and 2, June 1986).

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 document 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. It emphasizes the importance of a life cycle management approach for implementing computer security requirements.

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

This document, 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 standard also serves as a basis for specifying 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 Information Systems (IS) ; 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*, 03 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 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; 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; 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.

**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 automatic data processing 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 been either evaluated against established standards or endorsed by NSA as having met the requirements and standards set for these products by the Government.

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 generally to apprise those persons responsible 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 both 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. It 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. For the purpose of the directive, an INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during each phase of the life cycle.

**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 virtually eliminating, by 2000, their dependence on paper-based/non electronic keying methods and with a goal of 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 provides guidance for administrators of multiple user automated information systems. Specifically, when all 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, automated Controlled Access Protection shall be provided 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. This circular includes 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 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 summaries 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 synopsis of certification and accreditation process. 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 assigned responsibility for INFOSEC implementation and operation at Navy activities . Illustrates the need for management involvement and support for the security program.

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

This document aids those who conduct and administer INFOSEC programs for specific ISs and Local Area Networks (LAN). 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 need from Program Managers and other developers who have managerial and technical responsibilities for acquiring or certifying computer systems. Oriented primarily towards Program Managers, it focuses on the processes and requirements needed to certify and accredit information systems.

**5239-13, *Certification & 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 responsible for accomplishing a risk analysis on systems. 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. 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. It pertains to both classified and sensitive unclassified information. 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 (PC's & LANs). The key consideration in protecting the computer systems, which contain sensitive data, is for users/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 (P.L. 100-235), and OMB Bulletin 90-08.