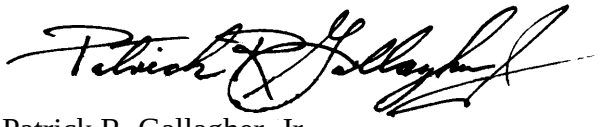
FOREWORD

The National Computer Security Center is issuing A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems as part of the "Rainbow Series" of documents our Technical Guidelines Program produces. In the Rainbow Series, we discuss in detail the features of the Department of Defense Trusted Computer System Evaluation Criteria (DOD 5200.28- STD) and provide guidance for meeting each requirement. The National Computer Security Center, through its Trusted Product Evaluation Program, evaluates the security features of commercially-produced computer systems. Together, these programs ensure that organizations are capable of protecting their important data with trusted computer systems.

A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems helps Information System Security Officers (ISSOs) understand their responsibilities for implementing and maintaining security in a system. The system may be a remote site linked to a network, a stand-alone automated information system, or workstations interconnected via a local area network. 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 regulations and standards.

I invite your suggestions for revising this document. We plan to review this document as the need arises.

May 1992



Patrick R. Gallagher, Jr.
Director
National Computer Security Center

ACKNOWLEDGMENTS

The National Computer Security Center extends special recognition for their contributions to this document to Annabelle Lee as principal author, to Ellen E. Flahavin and Carol L. Lane as contributing authors and project managers, and to Monica L. Collins as project manager.

We also thank the many representatives from the computer security community who gave of their time and expertise to review the guideline and provide comments and suggestions. Special thanks are extended to First Lieutenant Pamela D. Miller, United States Air Force, for her thought provoking suggestions and comments.

TABLE OF CONTENTS

LIST OF TABLES

TABLE NUMBER PAGE

1. INTRODUCTION

This guideline identifies system security responsibilities for Information System Security Officers (ISSOs). It applies to computer security aspects of automated information systems (AISs) within the Department of Defense (DOD) and its contractor facilities that process classified and sensitive unclassified information. Computer security (COMPUSEC) includes controls that protect an AIS against denial of service and protects the AISs and data from unauthorized (inadvertent or intentional) disclosure, modification, and destruction. COMPUSEC includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS. [1] DOD Directive (DODD) 5200.28 defines an AIS as "an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information." [2] This guideline is consistent with established DOD regulations and standards, as discussed in the following sections. Although this guideline emphasizes computer security, it is important to ensure that the other aspects of information systems security, as described below, are in place and operational:

- *Physical security* includes controlling access to facilities that contain classified and sensitive unclassified information. Physical security also addresses the protection of the structures that contain the computer equipment.

- *Personnel security* includes the procedures to ensure that access to classified and sensitive unclassified information is granted only after a determination has been made about a person's trustworthiness and only if a valid need-to-know exists.

  Need-to-know is the necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services. The custodian, not the prospective recipient(s), of the classified or sensitive unclassified information determines the need-to-know.

- *Administrative security* addresses the management constraints and supplemental controls needed to provide an acceptable level of protection for data. These constraints and procedures supplement the security procedures implemented in the computer and network systems.

- *Communications security* (COMSEC) defines measures that are taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security and to ensure the authenticity of such telecommunications. [1]

- *Emissions security* is the protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment, AISs, and telecommunications systems.

All these security areas are vital to the operation of a secure system. This guideline focuses on computer security, with discussions of the other security topics, as applicable.

1.1 SECURITY REGULATIONS, POLICIES, AND STANDARDS

This section provides an overview of regulations, policies, and criteria that address security requirements.

1.1.1 FEDERAL REGULATIONS

National mandates require the protection of sensitive information, as listed below:

- Title 18, U.S. Code 1905, makes it unlawful for any office or employee of the U.S. Government to disclose information of an official nature except as provided by law, including data processed by computer systems.
- Office of Management and Budget (OMB) Circular No. A-1 30 establishes requirements for Federal agencies to protect sensitive data.
- Public Law 100-235, *The Computer Security Act of 1987,* creates a means for establishing minimum acceptable security practices for systems processing sensitive information.
- Executive Order 12356 prescribes a uniform system for classifying, declassifying, and safeguarding national security information.

1.1.2 DEPARTMENT OF DEFENSE SECURITY POLICY

DODD 5200.28, *Security Requirements for Automated Information Systems (AISs),* is the overall computer security policy document for the DOD. The document identifies mandatory and minimum AIS security requirements. Each agency may issue its own supplementary instructions. For DOD agencies, these instructions fall within the scope of the DOD guidelines and add more specificity. Additional requirements may be necessary for selected systems, based on risk assessments.

Additional security documents are:

- Department of Defense 5220.22-M, *Industrial Security Manual for Safeguarding Classified Information.*
- Defense Intelligence Agency Manual (DIAM) 50-4, *Security of Compartmented Computer Operations (U).*
- Director of Central Intelligence Directive (DCID) 1/16, *Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U).*
- The Supplement to DCID 1/16, *Security Manual for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U).*
- National Security Agency/Central Security Service (NSA/CSS) Manual 130-1, *The NSA/ CSS Operational Computer Security Manual.*
- Air Force Regulation (AFR) 205-16, *Computer Security Policy.*
- Army Regulation (AR) 380-19, *Security: Information Systems Security.*

- Chief of Naval Operations Instruction (OPNAVINST) 5239.1A, *Automatic Data Processing Security Program.*

1.1.3 SECURITY STANDARDS

The National Computer Security Center (NCSC) is responsible for establishing and maintaining technical standards and criteria for the evaluation of trusted computer systems. As part of this responsibility, the NCSC has developed the *Trusted Computer System Evaluation Criteria (TCSEC),* also known as the "Orange Book" after the color of its cover, which defines technical security criteria for evaluating general purpose AISs. [3] In 1985, the *TCSEC* became a DOD standard (DOD 5200.28-STD) and is mandatory for use by all DOD components. The *TCSEC* rates computer systems based on an evaluation of their security features and assurances. The *Trusted Network Interpretation (TNI)* interprets the *TCSEC* for networks and provides guidance for selecting and specifying other security services (e.g., communications integrity, denial of service, and transmission security). [4]

1.2 PURPOSE

The primary purpose of this guideline is to provide guidance to ISSOs, who are responsible for implementing and maintaining security in a system. The system may be a remote site linked to a network, a stand-alone AIS, or workstations interconnected via a local area network. Throughout this guideline, the term "site" will be used to refer to the AIS configuration that is the responsibility of the ISSO. The ISSO may be one or more individuals who have the responsibility to ensure the security of an AIS excluding, for example, guards, physical security personnel, law enforcement officials, and disaster recovery officials. 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 DOD component regulations and standards.

This guideline provides general information and does not include requirements for specific agencies, branches, or commands. Therefore, the information included in this document should be considered as a baseline with more detailed security guidelines provided by each agency, branch, or command.

Finally, it is assumed that individuals who will be using this document have some background in security. This guideline presents some terms and definitions to provide a common framework for the information it presents; however, it does not provide a complete tutorial on security.

1.3 STRUCTURE OF THE DOCUMENT

Section 2 of this document identifies the operational environment. Section 3 presents the role and responsibilities of the ISSO and the environment in which the ISSO performs these tasks. Section 4 discusses the role and responsibilities of security personnel within an organization and the position of the ISSO. A bibliography and a reference list of security regulations, standards, and guidelines that provide additional information on system security are included following section 4. An acronym list and a glossary of computer security terms are included at the end of this document.

2. OPERATIONAL ENVIRONMENT

The ISSO performs security tasks for a site that may support several different user

communities. Therefore, the ISSO must understand the operational characteristics of the site. Documentation on the site configuration should be available and should, at a minimum, contain the following:

- Overall mission of the site.
- Overall floor layout.
- Hardware configuration at the site, identifying all the devices and the connections between devices and location, number, and connections of remote terminals and peripherals.
- Software at the site, including operating systems, database management systems, and major subsystems and applications.
- Type of information processed at the site (e.g., classified, sensitive unclassified, and intelligence).
- User organization and security clearances.
- Operating mode of the site (e.g., system high, dedicated, and multilevel secure).
- Interconnections to other systems/networks of users, e.g., the Automatic Digital Network (Autodin).
- Security personnel and associated responsibilities.

This documentation may be prepared jointly by the operations management and the ISSO. The following subsections provide additional information on the type of information processed and the operating mode of the site.

2.1 TYPE OF INFORMATION PROCESSED

The information that is stored, processed, or distributed at the site will be included in one of the following classification levels that designates the sensitivity of the data.

2.1.1 UNCLASSIFIED

Unclassified information is any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse. [2] Life-critical and other types of critical process control data that are unclassified also must be protected.

2.1.2 SENSITIVE UNCLASSIFIED

The loss, misuse, or unauthorized access to, or modification of this information might adversely affect U.S. national interest, the conduct of DOD programs, or the privacy of DOD personnel. [2] Examples include financial, proprietary, and mission-sensitive data.

2.1.3 CONFIDENTIAL

The unauthorized disclosure of this information or material could reasonably be expected to

cause damage to the national security. [5]

2.1.4 SECRET

The unauthorized disclosure of this information or material could reasonably be expected to cause serious damage to the national security. [5]

2.1.5 TOP SECRET

The unauthorized disclosure of this information or material could reasonably be expected to cause exceptionally grave damage to the national security. [5]

2.2 SECURITY MODE OF OPERATION

The Designated Approving Authority (DAA) accredits an AIS to operate in a specific security mode. The security mode selected reflects whether or not all users have the necessary clearance, formal access approval, and need-to-know for all information contained in the AIS.

Formal access approval is the documented approval by a data owner to allow access to a particular category of information. [2] The modes are defined below with the distinctions noted in italics for emphasis. The definitions are based on DODD 5200.28, except for compartmented security mode, which is based on DCID 1/16. Note that some terms that appear in *Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments,* CSC-STD-003-85, are no longer defined in DODD 5200.28. (Limited access mode and compartmented mode fall under the heading of partitioned mode. Controlled mode comes under the heading of multilevel security mode. In DODD 5200.28, partitioned mode is used in place of compartmented mode.) In addition, other modes of operation may be stipulated by the organization or agency that includes the site.

2.2.1 DEDICATED SECURITY MODE

An AIS operates in dedicated security mode when each user with direct or indirect individual access to the AIS, its peripherals, remote terminals, or remote hosts has the clearance or authorization, documented formal access approval, if required, *and* need-to-know for *all* information handled by the AIS. [2] An AIS operating in dedicated mode does not require any additional technical capability to control access to information. When in the dedicated security mode, the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. [6]

2.2.2 SYSTEM HIGH SECURITY MODE

System high security mode is a mode of operation wherein all users having access to the AIS possess a security clearance or authorization as well as documented formal access approval, *but not necessarily* a need-to-know, for all data handled by the AIS. [2] An AIS operating in system high security mode must have the technical capability to control access to information based on a user's need-to-know. Need-to-know may be specified using access control lists (ACLs) or non-hierarchical schemes for categorizing information.

2.2.3 PARTITIONED SECURITY MODE

In partitioned security mode, all users have the clearance but not necessarily formal access approval and need-to-know for all information contained in the system. This means that *some* users *may not* have need-to-know and formal access approval for *all* data processed by the AIS. [2]

An AIS operating in partitioned mode must have the technical capability to control access to information based on need-to-know and the sensitivity level of the data in the system.

2.2.4 COMPARTMENTED SECURITY MODE

DCID 1/16 defines compartmented security mode wherein each *user* has a valid clearance for the *most restricted* intelligence information processed in the AIS. Each user also has formal access approval, a valid need-to-know, and a signed nondisclosure agreement for that intelligence information to which the user is to have access. [7]

2.2.5 MULTILEVEL SECURITY MODE

Multilevel security (MLS) mode is a mode of operation wherein *not all* users have a clearance or formal access approval for all data handled by the AIS. This mode of operation can accommodate the concurrent processing and storage of (a) two or more levels of classified data, or (b) one or more levels of classified data with unclassified data depending upon the constraints placed on the system by the DAA. [2] An AIS operating in multilevel mode must have the technical capability to control access to information based on need-to-know, formal access approval, and sensitivity level of the data in the system. (Note: Controlled mode is not separately defined in DODD 5200.28. It is included in multilevel mode.)

3. ISSO AREAS OF RESPONSIBILITY

Within an organization, the ISSO may be one or more individuals who have the responsibility to ensure the security of an AlS. “ISSO” does not necessarily refer to the specific functions of a single individual. Also, additional responsibilities may be defined by the ISSO’s specific organization. The administration of system security can be centralized or decentralized depending upon the needs of the organization. Where multiple data center locations are involved, the decentralized approach may be more appropriate. However, one focal point should coordinate all information security policy. Also, the responsibility for information security rests with all members of the organization and not just the security personnel.

The ISSO supports two different organizations: the user organization and the technical organization. The user organization is primarily concerned with providing operations and the technical organization focuses on protecting data. It is recommended that the ISSO not report to operational elements of the Al5 that must abide by the security requirements of the applicable directives, policies, etc. The objective is to provide a degree of independence for the ISSO. The ISSO shall report to a high level authority who is not the operational manager. Also, the rank or grade of the ISSO shall be commensurate with the assigned responsibilities.

3.1 ISSO TECHNICAL QUALIFICATIONS

The DAA, or a designee, ensures an ISSO is named for each AIS. This individual and the

ISSO's management should ensure that the ISSO receives applicable training to carry out the duties. The ISSO position requires a solid technical background, good management skills, and the ability to deal well with people at all levels from top management to individual users. At a minimum, the ISSO should have the following qualifications:

- Two years of experience in a computer related field.
- One year of experience in computer security, or mandatory attendance at a computer security training course.
- Familiarization with the operating system of the AIS.
- A technical degree is desirable in computer science, mathematics, electrical engineering, or a related field.

3.2 OVERVIEW OF ISSO RESPONSIBILITIES

The ISSO acts for the Component Information System Security Manager (CISSM) to ensure compliance with AIS security procedures at the assigned site or installation. DODD 5200.28 summarizes the duties of the ISSO as follows:

- Ensure that the AlS is operated, used, maintained, and disposed of in accordance with internal security policies and practices.
- Ensure the AIS is accredited if it processes classified information.
- Enforce security policies and safeguards on all personnel having access to the AIS for which the ISSO has responsibility.
- Ensure that users and system support personnel have the required security clearances, authorization and need-to-know; have been indoctrinated; and are familiar with internal security practices before access to the AIS is granted.
- Ensure that audit trails are reviewed periodically, (e.g., weekly or daily). Also, that audit records are archived for future reference, if required.
- Initiate protective or corrective measures if a security problem is discovered.
- Report security incidents in accordance with DOD 5200.1 -R and to the DAA when an AIS is compromised.
- Report the security status of the AIS, as required by the DAA.
- Evaluate known vulnerabilities to ascertain if additional safeguards are needed.
- Maintain a plan for site security improvements and progress towards meeting the accreditation.

3.3 ISSO SECURITY RESPONSIBILITIES

Command-specific duties of the ISSO have been well-defined in many regulations, directives,

and documents, e.g., AFR 205-16, AR 380-19, and OPNAVINST 5239.1A. This guideline provides a more general discussion of ISSO responsibilities, which may be tailored to a particular environment. The remainder of section 3 details ISSO responsibilities. Some of these responsibilities are necessary to support the security duties as summarized above. The material is not presented in a specific order.

3.4 SECURITY REGULATIONS AND POLICIES

The ISSO shall be aware of the directives, regulations, policies, and guidelines that address the protection of classified information, as well as sensitive unclassified information. The overall security documents are discussed in section 1. Also, each command and agency may have additional requirements that provide more detailed guidance on protecting sensitive information. It may be necessary for the ISSO to prepare, or have prepared, a list of the applicable directives, regulations, etc., if one is not available.

Security Documentation. The ISSO participates in the development or revision of site-specific security safeguards and local operating procedures that are based on the above regulations. The objective is to include the ISSO during the development and writing rather than only at the implementation phase. The overall site security document is the security plan. It contains the security procedures, instructions, operating plans, and guidance for each AIS at the site.

The ISSO also provides input to other security documents, for example, security incident reports, equipment/software inventories, operating instructions, technical vulnerabilities reports, and contingency plans.

Two documents that the ISSO should be familiar with, required for products with security features at the C1 level or above, are discussed below:

- The Trusted Facility Manual (TFM) details security functions and privileges. It is designed to support AIS administrators (e.g., the ISSO, the database administrator, and computer operations personnel). It addresses the configuration, administration, and operation of the AIS. It provides guidelines for the consistent and effective use of the protection features of the system. (Additional information is provided in the TCSEC.)

- The Security Features User's Guide (SFUG) assists the users of the AIS. It describes how to use the protection features of the AIS correctly to protect the information stored on the system. The SFUG discusses the features in the AIS that are available to users, as well as the responsibilities for system security that apply to users.

3.5 MISSION NEEDS

The ISSO shall understand the organization's mission needs, that is, the goals and objectives of the organization and the resources required to accomplish these goals. Requirements are specified by analyzing the organization's current capabilities, available resources, facilities, funds, and technology base, and by determining whether they are sufficient to fulfill the mission. If not, the mission needs should be evaluated and prioritized and a plan developed to address these needs. Because security requirements should be included in the mission needs and current assets assessment, it is important for the ISSO to become involved in the mission definition process.

3.6 PHYSICAL SECURITY REQUIREMENTS

In general, physical security addresses facility access and the protection of the structures and components that contain the AIS and network equipment. Physical security also addresses contingency plans and the maintenance and destruction of storage media and equipment. These physical safeguards must meet the minimum requirements established for the highest classification of data stored at the site. The ISSO in coordination with site security personnel is responsible for ensuring that physical safeguards are in place. Facility access and maintenance are further discussed in section 3.10. Contingency planning and declassification are discussed in sections 3.6.1 and 3.6.2.

3.6.1 CONTINGENCY PLANS

The Information System Security Manager (ISSM) is responsible for the formulation, testing, and revision of site contingency plans because of the manager's accountability for ensuring continuity of operations. The contingency plans document emergency response, backup operations, and post-disaster recovery procedures. While the ISSM has overall responsibility for the plans, the ISSO provides technical contributions concerning the overall security plans to ensure the availability of critical resources and to facilitate system availability in an emergency situation. It is also important that all responsibilities under the plan are adequately documented, communicated, and tested.

3.6.2 DECLASSIFICATION AND DOWNGRADING OF DATA AND EQUIPMENT

Declassification is a procedure and an administrative action to remove the security classification of the subject media. Downgrading is a procedure and an administrative action to lower the security classification of the subject media. The procedural aspect of declassification is the actual purging of the media and removal of any labels denoting classification, possibly replacing them with labels denoting that the storage media is unclassified. The procedural aspect of downgrading is the actual purging of the media and removal of any labels denoting the previous classification, replacing them with labels denoting the new classification. The administrative aspect is realized through the submission to the appropriate authority of a decision memorandum to declassify or downgrade the storage media.

The ISSO must ensure that:

- Purging, declassification, and downgrading procedures are developed and implemented.
- Procedures are followed for purging, declassifying, downgrading, and destroying storage media.
- Procedures are followed for marking, handling, and disposing of the computer, its peripherals, and removable and nonremovable storage media.
- Any special software needed to overwrite the site-unique storage media is developed or acquired.
- Any special hardware, such as degaussers, is available.

3.7 ADMINISTRATIVE SECURITY PROCEDURES

Administrative security includes the preparation, distribution, and maintenance of plans, instructions, guidelines, and operating procedures regarding security of AISs. It is the responsibility of the ISSO to assist in the development of administrative procedures, if required, and to conduct periodic reviews to ensure compliance.

3.7.1 PERSONNEL SECURITY

One component of administrative security is personnel security. In general, it is the responsibility of the ISSO to:

- Ensure that all personnel and, when required, specified maintenance personnel who install, operate, maintain, or use the system, hold the proper security clearances and access authorizations.
- Ensure that all system users, including maintenance personnel, are educated by their respective security officer in applicable security requirements and responsibilities.
- Maintain a record of valid security clearances, physical access authorizations, and AIS access authorizations for personnel using the computer facility.
- Ensure that maintenance contractors who work on the system are supervised by an authorized knowledgeable person.

3.7.2 SECURITY INCIDENTS REPORTING

A security incident occurs whenever information is compromised, when there is a risk of compromise of information, when recurring or successful attempts to obtain unauthorized access to a system are detected, or where misuse of the system is suspected.

The ISSO creates a reporting mechanism, as part of the security incident reporting procedure, for users to keep the ISSO informed of security-relevant activity that they observe on the system. This reporting mechanism shall not use the AIS to report security-relevant activity about the AIS.

The mechanism, at a minimum, includes the following:

- Description of incident.
- Identification of the individual reporting the security incident.
- Identification of the loss, potential loss, access attempt, or misuse.
- Identification of the perpetrator (if possible).
- Notification of appropriate security and management personnel and civil authorities, if required.
- Reestablishment of protection, if needed.
- Restart of operations, if the system had been taken down to facilitate the investigation.

The ISSO performs the following in support of this task:

- Prepares procedures for monitoring and reacting to system security warning messages and reports.
- Develops, reviews, revises, and submits for approval to the DAA and technical supervisor, procedures for reporting, investigating, and resolving security incidents at the site.
- Immediately reports security incidents through the appropriate security and management channels (e.g., ISSM and Program Manager). The ISSO submits an analysis of the security incident to the appropriate authority for corrective and disciplinary actions.
- Performs an initial evaluation of security problems, and, if necessary, temporarily denies access to affected systems. The ISSO ensures that Terminal Area Security Officers (TASOs) evaluate, report, and document security problems and vulnerabilities at their respective remote terminal areas.
- Partially or completely suspends operations if any incident is detected that affects security of operations. This would include any system failure. (Note: this may be unrealistic if the system performs a critical operational mission. Alternative procedures may be required in this situation. The DAA must weigh the risk of a security incident against the potential damage in shutting down the system.)
- Ensures that all cases of actual or suspected compromise of classified passwords are investigated.
- Ensures that occurrences within the system that may affect the integrity and security of the data being processed are investigated. If the system malfunctions, it is important to account for the data.
- Assists the investigating officials in analyzing actual or suspected compromises of classified information.

3.7.3 TERMINATION PROCEDURES

The ISSO is responsible for performing the following tasks whenever any user's access is terminated. Prompt action is required, particularly if the termination or knowledge of the pending termination might provoke a user to retaliate.

- Removes the user from all access lists, both manual and automated.
- Removes the individual's account from all systems, including the user's password.
- Ensures that the individual has turned in all keys, tokens, or cards that allow access to the AIS.
- Ensures that combinations of any combination locks, associated with the AIS and its physical space, that the individual accessed are changed.
- Ensures that all remaining personnel using systems processing classified data change their

passwords to prevent unauthorized access.

3.8 SECURITY TRAINING

Because personnel are an integral part of the security protection surrounding an AIS, they must understand the vulnerabilities, threats, and risks inherent with AIS usage. Therefore, computer security shall be included in briefings given to all new personnel. To reinforce this initial training and to introduce new concepts, periodic training and security awareness programs should be conducted. The ISSO shall continue training to keep current in security products and procedures. The ISSO is responsible for ensuring that:

- All personnel (including management) have computer security awareness training and have read applicable sections of the AIS security plan. This includes training in security procedures and the use of security products.
- All users are educated regarding password management (e.g., generating unique passwords, keeping passwords adequately protected, not sharing passwords, changing passwords on a regular basis, and generating different passwords for each system accessed).
- Users understand the importance of monitoring their successful and unsuccessful logins, if possible. If these do not correspond to the user's actual usage, the user should know the proper procedures for reporting the discrepancy.

The ISSO can keep users informed about security in many different ways. Some approaches follow:

- Periodically display messages on the AIS when the user logs on to the system.
- Develop and distribute security awareness posters to foster interest.
- Disseminate new security information about the system and issue reminder notices about protection procedures.
- Issue memos to notify users of changes.
- Provide "hands-on" demonstrations of AIS security features and procedures.

3.9 SECURITY CONFIGURATION MANAGEMENT

Configuration management controls changes to system software, firmware, hardware, and documentation throughout the life of the AIS. This includes the design, development, testing, distribution, and operation of modifications and enhancements to the existing system. The ISSO or other designated individual aware of the security issues shall be included in the configuration management process to ensure that implemented changes do not compromise security. It is particularly important for the ISSO to review and monitor proposed changes to the trusted computing base (TCB) as defined in the security architecture. Appropriate tests should be conducted to show that the TCB functions properly after changes are made to it. Configuration management tasks that are the responsibility of the ISSO are as follows:

- Maintain an inventory of security-relevant hardware and security-relevant software and their locations.
- Maintain documentation detailing the AIS hardware, firmware, and software configuration and all security features that protect it.
- Evaluate the effect on security of proposed centrally developed and distributed and site-unique modifications to software and applications. Submit comments to appropriate personnel.
- Identify and analyze system malfunction. Prepare security incident reports.
- Assist in the development of system development notifications and system change proposals.
- Monitor DAA-approved site procedures for controlling changes to the current system.
- Ensure that any system connectivity is in response to a valid operational requirement.
- Ensure that continuing tests of the site security features are performed, and maintain documentation of the results.
- Coordinate AS security changes with the ISSM. Review all site configuration changes and system component changes or modifications to ensure that site security is not compromised.
- Review physical inventory reports of security-relevant AIS equipment.

Hardware and Software Installation and Maintenance. The ISSO ensures that the design and development of new Systems or the maintenance or replacement of existing systems includes security features that will support certification and accreditation or reaccreditation. In support of this effort, informal reviews with the site certifiers can help identify potential problems, thus enabling potential security risks to be identified early. Before installing any new system release, the site shall complete sufficient testing to verify that the system meets the documented and approved security specifications and does not violate existing security policy. The ISSO shall, at a minimum, observe the testing of new releases. Specific ISSO tasks are:

- Ensure that all security-relevant development and planning activities are reviewed and approved.
- Participate in the acquisition planning process for proposed acquisitions to ensure that the site security policy has been considered. This applies to both the acquisition of new systems or the upgrade of existing systems.
- Ensure that security features are in place (by testing) to prevent applications programs from bypassing security features or from accessing sensitive areas of the system.
- Develop procedures to prevent the installation of software from unauthorized or questionable sources.

- Ensure that system support personnel know how to install and maintain security features.

3.10 ACCESS CONTROL

Access is considered from different perspectives: physical access to the facility and system (facility access), logical access to the system (identification and authentication), and logical access to the system's files and other objects (data access). Each of these is discussed separately below.

3.10.1 FACILITY ACCESS

Procedures shall be developed for controlling access to the site and the site's resources. In accordance with applicable security policy, system access shall be denied to any user, customer, or visitor who has not been granted specific authorization. General guidance for the ISSO follows:

- Establish procedures to ensure that only personnel who have a need-to-know have access to classified or sensitive but unclassified information.
- Establish procedures to ensure that only personnel who have the proper clearances and formal access approval are allowed physical access to any system containing classified information. All individuals who have routine access to the system should be properly cleared and have a valid operational requirement for access.
- Deny access to any user, customer, or visitor who is unauthorized or suspected of violating security procedures.
- Ensure all visitors are signed-in and escorted, if necessary. Visitors shall be under visual observation by an authorized person.
- Keep records of maintenance performed at the site.
- Establish and implement procedures to control AIS equipment coming into and going out of the site, including, for example, test devices, cable, and system disks.
- Develop and maintain a facility security plan that contains at least architectural drawings and building plans, floor plans, and inventories.
- Ensure that maintenance contractors who work on the system are supervised by an authorized knowledgeable person.

3.10.2 IDENTIFICATION AND AUTHENTICATlON (I&A)

The identification component of an I&A system consists of a set of unique user identifiers. Authentication involves verifying the identity of a user. If a user's identifier does not remain unique, a subsequent user may gain the access rights of a previous user on the system. General guidance to the ISSO follows:

- Ensure that the databases required to support the I&A function are accessible only by the ISSO.
- Obtain a list of all identifications (IDs) preset at the factory. Change or delete all user IDs and passwords that come with vendor software to prevent unauthorized access. Default

passwords shall be checked and changed, as necessary, at system installation and modification, when the ISSO first assumes responsibility of the system, and after any maintenance to the system.

- Develop and administer a password management system that includes the generation of system passwords and development of procedures for addressing password loss or compromise.
- Ensure that only authorized persons execute system utility programs and routines that bypass security checks or controls.
- Maintain a site user list that contains the name, user ID, access level, and whether the user is to have operator or administrative privileges.

3.10.3 DATA ACCESS

The focus of data access procedures is to prevent disclosure of information to unauthorized individuals. General guidance for the ISSO follows:

- Ensure that the site-specific discretionary access control (DAC) policy is defined and implemented. The policy should define the standards and regulations that the ISSO must implement to ensure that data is disclosed only to authorized individuals.
- Control access to all functions that can affect the security or integrity of the system. Access of this type shall be kept to the absolute minimum number of personnel.
- Ensure that any required access control software subsystems or other security subsystems are installed and operated in a manner that supports the security policy of the AIS.

3.11 RISK MANAGEMENT

Risk management identifies, measures, and minimizes the effect of uncertain events on system resources. Risk management determines the value of the data, what protection already exists, and how much more protection the system needs. The process includes risk analysis, cost benefit analysis, safeguard selection and implementation, appropriate security tests, and systems review. Risk management is an ongoing process that will reaffirm the validity of previous analysis. The ISSO supports the risk management process by performing the following tasks:

- Assist in the development of the risk management plan.
- Perform a risk assessment and analysis by analyzing threats to the site and vulnerabilities of the site in relationship to the sensitivity of the information on the system. Document the results and prepare appropriate countermeasures. (This is expanded below.)
- Ensure a contingency plan is in place for continuity of operations in an emergency situation and that the developed plans are exercised.
- Ensure that approved countermeasures are implemented.
- Periodically review the risk assessment for new threats due to a changed configuration or

changes in the operational environment and review contingency plans to ensure that they are still applicable.

- Ensure that security tests, risk analysis, TEMPEST tests, and other inspections are conducted as required. Maintain a file of working papers concerning security tests, risk analysis, and other facets of the risk management program.

- Maintain a file of all site security-related waivers.

The ISSO documents and reports computer security technical vulnerabilities detected in AISs, in accordance with DOD Instruction 5215.2. The report includes information regarding technical solutions or administrative procedures implemented to reduce the risk. Each ISSO administers the technical vulnerability reporting program and:

- Reports identified technical vulnerabilities. As a further way of sharing information about vulnerabilities, maintains contact with other system security officers and with other users of the same type of system.

- Assumes responsibility for recommending any necessary and feasible action to reduce risks presented by the vulnerabilities.

- Develops local procedures for reporting and documenting technical vulnerabilities, and ensures that all users and operators receive training for carrying-out the procedures.

- Ensures that vulnerability information is properly classified and protected.

3.12 AUDITS

The ISSO has the primary responsibility to conduct security audits for operational systems as well as for systems under development. Monitoring of variances in security procedures is also important and is best controlled by the ISSO. As part of variance monitoring, the ISSO reviews any relevant audit trail data from the system. Finally, the ISSO provides senior management with reports on the effectiveness of security policy, with identification of weaknesses and recommendations for improvements.

3.12.1 AUDIT TRAILS

The audit trail provides a record of system security-related activity and allows the ISSO to monitor activities on the system. To be an effective security tool, the audit trail should be able to monitor, for example, successful and unsuccessful access attempts, file accesses, type of transaction, and password changes. If manual audits are necessary, the ISSO shall document random checks made to verify that users are recording system usage. Audit trail files must be protected to prevent unauthorized changes or destruction.

3.12.2 AUDITING RESPONSIBILITIES

Appropriate audit trail data shall be reviewed by the ISSO. Besides the system audit trail, network audit reports can provide detailed information on network traffic and provide summary accounting information on each user ID, account, or process. The responsibilities of the ISSO follow:

- Review specifications for inclusion of audit trail reduction tools that will assist in audit trail analysis.
- Select security events to be audited. Ensure that the audit trail is reviewed and have the capability to audit every access to controlled system resources (e.g., very sensitive files). Archive audit data.
- Develop and implement audit and review procedures to ensure that all AIS functions are implemented in accordance with applicable policies and programs. Existing policies and programs usually establish the minimum amount of material that shall be audited.
- Conduct audits and maintain documentation on the results.
- Supervise review of security audit parameters. Develop, review, revise, submit for approval, and implement procedures for monitoring and reacting to security warning messages and reports.
- Conduct random checks to verify compliance with the security procedures and requirements of the site.
- Gather information from audit trails to create profiles of system users. Observe user patterns such as the terminal usually used, files accessed, normal hours of access, and permissions usually requested, to determine which actions are unusual and shall be investigated.
- Review user access reports generated by the audit trail, in compliance with policies and practices.
- Review audit trail reports for anomalies:
    - Look for multiple unsuccessful logon attempts. This could be an indication of an inexperienced user, a user who has recently changed passwords and forgotten the new one, or an attempted intrusion.
    - Look for an attempt by a user, who is already logged in at a terminal, to log in again to the same system from a second terminal. This could be caused by an inadvertent failure to log out, an intentional logon to both terminals, or an attempted intrusion.
    - Be alert to individuals logging in after normal hours. This may mean the user has a deadline to meet and is working overtime or that an intruder is attempting access.
    - Look for high numbers of unsuccessful file accesses. This could be prompted by the user' failure to remember file names or by an attempted intrusion.
    - Look for unexplained changes in system activity.
    - Look for covert channel activity.

3.13 CERTIFICATION AND ACCREDITATION

Certification is the technical evaluation of an AIS's security features, including non-AIS

security features (e.g., administrative procedures and physical safeguards), against a specified set of security requirements. The objective is to determine how well the AIS design and implementation meet this pre-defined set of security requirements. Certification is performed as part of the accreditation process. Accreditation is the formal management decision made by the DAA to implement an AIS or network in a specific operational environment at an acceptable level of risk. The certification package specifies the following in support of accreditation:

- Security mode.
- Set of administrative, environmental, and technical security safeguards.
- Operational environment.
- Interconnections to other AIS or networks.
- Vulnerabilities as well as procedural and physical safeguards.

The ISSO is frequently responsible for the following list of tasks in preparation for accreditation of a particular AIS:

- Assist in preparing the accreditation material required by the DAA.
- Assist in the evaluation of the accreditation package.
- Assist in the site surveys.
- Prepare a statement to the DAA about the certification report. The report should include a description of the system and its mission; the results from the testing, document reviews, and hardware and software reviews; remaining system vulnerabilities; and any additional controls or environmental requirements that may be necessary.
- Ensure that the site maintains the system security baseline through audits.
- Notify the DAA or the DAA's representative of all configuration changes that may change the site's security baseline.

4. SECURITY PERSONNEL ROLES

Although this guideline focuses on the role and responsibility of the ISSO, it is important to understand how the ISSO position relates to other positions that have some security responsibility within an organization. This section outlines these other positions with security responsibilities.

DOD regulations define security roles and responsibilities for personnel responsible for AIS security. Overall roles and responsibilities are similar across DOD, but are assigned different titles in each service/agency. Table 1 summarizes the titles and positions across the DOD components.

One of the roles not addressed in Table 1 or 2 is that of the Program Manager (PM). While this is not specifically a security function, the PM must be aware of the AIS security requirements. The PM should establish a computer security working group (CSWG) consisting of individuals from the program office, users, procurement specialists, consultants, local computer security

organizations, and the developers. During the acquisition process, this group shall review and evaluate security-related documents and issues such as specifications, security test plans and procedures, and risk management plans and procedures. The following sections list responsibilities for each of the identified security roles. Depending on the size, geographical distribution, and complexity of the site, the role of the ISSM (Information System Security Manager)/NSM (Network Security Manager) may be filled by the same individual(s) as the lSSO/NSO (Network Security Officer).

Table 1

Service and Agency Security Personnel Titles

Level	Air Force[1]	Army[1]	Navy[1]	DIA
System Wide	MAJCOM[2,3] MCSSM	MACOM[2] ISSPM	COMNAVCOMTELCOM[2]	MDIC or SIO[2]
AIS Site	BCSSM CFM[4] CSSO TASO	ISSM ISSO TASO	ADPSO ADPSSO/ISSO MSO TASO	 ISSO
Network Site	NM NSM NSO	 NSO	NSO	NSO

1. Not SCI (Sensitive Compartmented Information), SIOP-ESI (Single Integrated Operational Plan-Extremely Sensitive Information)
2. DAA
3. There many be multiple MAJCOMs at a base, each with one or more AIS sites
4. There is only one BCSSO per base to which all CFMs provide information

ADPSO	ADP Security Officer
ADPSSO	ADP System Security Officer
BCSSM	Base Communications-Computer Systems Security Manager
BCSSO	Base Communications-Computer Systems Security Officer
CFM	Computer Facility Manager
COMNAVCOMTELCOM	Commander, Naval Computer and Telecommunications Command
CSSM	Communications-Computer System Security Manager
CSSO	Computer System Security Officer
DAA	Designated Approving Authority/Designated Accreditation Authority
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISSPM	Information System Security Program Manager
MACOM	Major Army Command
MAJCOM	Major Command (Air Force)
MCSSM	MAJCOM CSSM
MDIC	Military Department Intelligence Officer
MSO	Media Sanitation Officer
NM	Network Manager
NSM	Network Security Manager
NSO	Network Security Officer
SIO	Senior Intelligence Officer
SSM	System Security Manager
TASO	Terminal Area Security Officer

Table 2 presents a uniform set of security roles and titles that will be used throughout this guideline.

Table 2
Uniform Security Personnel Titles

LEVEL	STAFF POSITION
System Wide (Not SCI, SIOP-ESI)	DAA CISSM
AIS Site	ISSM ISSO TASO
Network Site	NSM NSO

CISSM	Component Information System Security Manager
DAA	Designated Approving Authority
ISSM	Information System Security Manager
ISSO	Information System Security Officer
NSM	Network Security Manager
NSO	Network Security Officer
SCI	Sensitive Compartmented Information
SIOP-ESI	Single Integrated Operational Plan Extremely Sensitive Information
TASO	Terminal Area Security Officer

4.1 DESIGNATED APPROVING AUTHORITY (DAA)

The DAA grants final approval to operate an AIS or network in a specified security mode. [2] Before accrediting a site, the DAA reviews the accreditation documentation and confirms that the residual risk is within acceptable limits. The DAA also verifies that each AIS complies with the AIS security requirements, as reported by the ISSOs. Specific security responsibilities are as follows:

- Establish, administer, and coordinate security for systems that agency, service, or command personnel or contractors operate. Assist the PM in defining system security requirements for acquisitions.
- Appoint the individuals who will directly report to the DAA.
- Approve the classification level that is required for applications that are implemented in a network environment. Also, approve additional security services that are necessary (e.g., encryption and non-repudiation) to interconnect to external systems.
- Review the accreditation plan and sign the accreditation statement for the network and each AIS and define the criticality and sensitivity levels of each AIS.

- Review the documentation to ensure that each AIS supports the security requirements as defined in the AIS and network security programs.

4.2 COMPONENT INFORMATION SYSTEM SECURITY MANAGER (CISSM)

The CISSM is the focal point for policy and guidance in AIS and network security matters and reports to and supports the DAA. The CISSM administers both the AIS and network security programs within the component (defined as the Office of the Secretary of Defense, the military departments and the military services within those departments, the Joint Chiefs of Staff, the Joint Staff, the Unified and Specified Commands, the Defense agencies, the DOD field activities, and other such offices, agencies, activities, and commands as may be established by law, by the President, or by the Secretary of Defense that process data on AISs). [2] Additionally, the CISSM is responsible for subcomponents such as the MAJCOM, MACOM, or COMNAVCOMTELCOM, which are identified in Table 1. The CISSM, therefore, may be responsible for multiple AISs. Security responsibilities should include:

- Develop and administer AIS and network security programs that implement policy and regulations and are consistent with the accreditation plan. The network program shall define intrasystem and intersystem connectivity.
- Establish a risk management program for the entire AIS life cycle. This includes addressing network-wide security and problems associated with interconnecting to external systems.
- Identify the DAA for each unclassified system and each classified system.
- Identify each system in the certification and accreditation plan or in the system security plan.
- Advise the DAA about the use of specific security mechanisms.
- Provide periodic briefings to the component management and to the DAA.
- Report security vulnerabilities, maintain a record of security-related incidents, and report serious and unresolved violations to the DAA.
- Administer a security and training awareness program.
- Oversee maintenance of accreditation documentation.
- Provide for overall key distribution and encryption management.
- Enforce, through policy, compliance with component computer security program.

4.3 INFORMATION SYSTEM SECURITY MANAGER (ISSM)

The ISSM reports to the CISSM and implements the overall security program approved by the DAA. The ISSM focuses on AIS security. There may be multiple ISSMs. The ISSM should not participate in the day-to-day operation of the AIS.

Specific security responsibilities are:

- Ensure that the AS security program requirements are met, including defining the security mode, specific security requirements, protocols, and standards. Develop applicable AIS security procedures.
- Implement the risk management program defined by the CISSM. Verify that the risk assessment is performed and that threats and vulnerabilities are reviewed to evaluate risks properly.
- Verify that appropriate security tests are conducted and that the results are documented.
- Review the accreditation plan and the reaccreditation activities, develop a schedule for the reaccreditation tasks, and initiate recertification and reaccreditation tasks under the direction of the DAA.
- Assist in site configuration management by reviewing proposed system changes and reviewing implemented system modifications for adverse security impact.
- Ensure that AIS security is included in all the contingency plans.
- Provide the DAA with the certification package to show that the AIS satisfies the security specifications for the data it processes, stores, or transmits. Document and maintain the evidence contained in the certification package.
- Monitor AIS personnel security procedures to ensure that they are being followed; coordinate and monitor initial and follow-up security training for AS personnel.
- Maintain a current AIS security plan.

4.4 NETWORK SECURITY MANAGER (NSM)

The NSM is responsible for the overall security operation of the network and is the focal point for policy, guidance, and assistance in network security matters. In addition, the NSM ensures that the network complies with the requirements for interconnecting to external systems. The NSM reports to the CISSM and shall not participate in the day-to-day operation of the network. The tasks of the NSM are comparable to those of the ISSM. The security responsibilities are listed in the same order as those for the ISSM, for ease of comparison, with differences indicated by italics:

- Ensure that an *NSO* is appointed for each *network.*
- Ensure that the AIS security program requirements are met, including defining the security mode, specific security requirements, protocols, and standards. Develop applicable *network* security procedures.
- Implement the risk management program defined by the CISSM. Verify that the risk assessment is performed and that threats and vulnerabilities are reviewed to evaluate risks properly.
- Verify that appropriate security tests are conducted and that the results are documented.

- Review the accreditation plan and the reaccreditation activities, develop a schedule for the reaccreditation tasks, and initiate recertification and reaccreditation tasks under the direction of the DAA.

- Assist in site configuration management by reviewing proposed system changes and reviewing implemented system modifications for adverse system impact.

- Ensure that *network* security is included in all the contingency plans.

- Provide the DAA with the certification package to show that the network satisfies the security specifications for the data it processes, stores, or transmits. Document and maintain the evidence contained in the certification package.

- Provide the DAA with written certification that the satisfies the security specifications for the data it processes, stores, or transmits. Ensure that the documentation to support the certification is developed and maintained.

- Monitor implementation of AIS personnel security procedures to ensure that they are being followed; coordinate and monitor initial and follow-up security training for AIS personnel.

- Maintain a current AIS security plan.

- *Manage routing control for security within the network (specify links or subnetworks that are considered to be trusted based on specific criteria).*

4.5 INFORMATION SYSTEM SECURITY OFFICER (ISSO)

The ISSO acts for the CISSM to ensure compliance with AIS security procedures at the operational site or installation. Depending on the size and complexity of the AIS, the ISSO also may function as the ISSM and NSO. The duties of the ISSO are detailed in section 3.

4.6 NETWORK SECURITY OFFICER (NSO)

The NSO implements the network security program and acts as the point of contact for all network security matters. The responsibilities of the NSO are similar to those of the ISSO, with the NSO concentrating on network security and the ISSO concentrating on AIS security. The security responsibilities of the NSO are:

- Obtain written approval from the DAA to process classified or sensitive unclassified information on the network.

- Maintain the security processing specifications for the network.

- Ensure that standard security procedures and measures that support the security of the entire network are developed and implemented. Conduct periodic reviews to ensure compliance with network security procedures.

- Ensure that network security is included in all the contingency plans and that the contingency plans are tested.

- Maintain the site-specific portion of the accreditation documentation.

- Ensure that physical measures to protect the facility are in effect and that measures to protect mission-essential, sensitive data processing activities are implemented. Maintain liaison with organizations that are responsible for physical security, e.g., military police, fire control officials, base power plant officials, and emergency services.

- Review network configuration changes and network computer changes or modifications to ensure that network security is not degraded (including interfaces to separately accredited AISs). Ensure that network components (i.e., hardware, software, and firmware) are included in the configuration management program.

- Select security events that are to be audited or remotely collected; establish procedures for collecting the audit information; and review audit reports.

- Verify security clearances and access approval for personnel using the network.

- Coordinate and monitor initial and periodic security training for network personnel. Verify that all users receive network security training before being granted access to the network.

- Provide users with plans, instructions, guidance, and standard operating procedures regarding network operations. Conduct periodic reviews to ensure compliance.

- Verify that personnel security procedures applicable to the operation of the computer facility are followed.

- Report physical, personnel, and AIS security violations to the NSM. Report system failures that could lead to unauthorized disclosure.

- Review reported security problems and inform the NSM of security difficulties. Ensure that TASOs evaluate, document, and report security problems and vulnerabilities at their respective sites.

- Recommend partial or complete suspension of operations if any incident is detected that may affect security of the operation.

- Monitor the system recovery processes to assure that security features are correctly restored.

- Maintain guidelines that ensure that the physical, administrative, and personnel security procedures are followed.

4.7 TERMINAL AREA SECURITY OFFICER (TASO)

The TASO reports to the ISSO and is responsible for security procedures in an assigned remote terminal area. System access from the TASO's assigned remote terminals will not be allowed without authorization from the cognizant security officer. The TASO has the following security responsibilities:

- Ensure that there are written instructions specifying security requirements and operational procedures for each terminal area.

- Ensure access to a terminal is only to users with the need-to-know, clearance, and access approval for data that may be accessed from that terminal.
- Perform an initial evaluation of security problems in the assigned terminal area(s) and notify the ISSO of all security violations and any practices that may compromise system security.
- Verify that the physical security controls are in place and operational, for example, physically protecting the network interfaces (hardware connections).
- Collect and review selected remote facility audit records, document any reported problems, and forward them to the ISSO.
- Participate in security training and awareness.
- Ensure that the equipment custodian has all the component serial numbers written down and stored in a secure place.

4.8 SECURITY RESPONSIBILITIES OF OTHER SITE PERSONNEL

Because the overall security of a site is subject to the cooperation of everyone involved in the system, the discussion of roles and responsibilities would not be complete without mentioning the system administrator, the computer facility personnel, the data administrator, the maintenance personnel, and the users. Everyone is responsible for knowing the security procedures and mechanisms that are in effect for a particular system, for following all procedures applicable to security, and for reporting potential security incidents. In addition, specific responsibilities for other individuals are listed below.

The data administrator and classifier shall:

- Coordinate with the ISSO on information security requirements and with the NSO for network security requirements.
- Establish or confirm the overall security classification of the applicable resources and establish restrictions or special conditions for the use of the data.
- Periodically review the data to verify that the security classification is correct. Recommend downgrading data, if applicable.
- Authorize individual or group access to specific resources.
- Participate in the development of a formal need-to-know policy.

The users shall:

- Use the system only for authorized purposes and in accordance with security procedures and guidelines.
- Maintain individual accountability (e.g., do not share passwords).
- Protect classified and other sensitive material.

4.9 ASSIGNMENT OF SECURITY RESPONSIBILITIES

Table 3 presents a sample chart for identifying the roles and responsibilities of the various individuals who have security tasks. The primary goal is to identify all the tasks and ensure that at least one individual is assigned to perform each task.

Table 3

Function Matrix

Function	DAA	CISSM	ISSM	NSM	ISSO	NSO	TASO
Overall Security	PR	IM	IM	IM	IM	IM	IM
Accreditation Process	PR	IM	IM	IM	IN	IN	
Recertification and Reaccreditation	PR	IM	IM	IM	IN	IN	
AIS Security Program	PR	IM	IM	IM	IM		
Network Security Program	PR	IM		IM		IM	
Network Access	PR			PR		VE	DO, VE
SecurityThreats/ Vulnerabilities	PR	DO	DO	DO	IN, DO	DO, IN	DO
Security Regulations and Policies	IM	IM	IM	IM	IM	IM	IM
Security Documentation	VE	DO	DO	DO	IN	IN	IN
Risk Management Program		PR	IM	IM	IM, IN	IM, IN	
Security Training and Awareness Program		PR	VE	VE	IM,VE	IM,VE	IM
Security Violations		DO	DO	DO	DO	DO	DO
Security Configuration Management		VE	IM	IM	IM	IM	
AIS Security Procedures			PR		IM, VE	IM, VE	IM, VE
Contingency Plans			PR, VE	PR, VE	IM, IN	IM, IN	IM
Network Security Procedures				PR		IM,VE	
Audit					PR	PR	PR,DO
Access Control					IM	IM	VE
Physical Security					VE	VE	VE
Declassification and Downgrading					VE		

PR: has primary responsibility
IM: implements enforces task or program
DO: prepares documentation and submits to appropriate authority, if applicable
VE: verifies compliance or performance of activities
IN: assists in the preparation of reports, plans, procedures, etc.

BIBLIOGRAPHY

This bibliography includes documents that may be useful to the ISSO. Included are directives, regulations, manuals, circulars, etc. Cited references are also included. This list is not intended to be comprehensive; that is, additional readings may apply to a particular organization and system, and the ISSO should identify all the relevant security documents.

Computer Security Act of 1987, Public Law 100-235, 101 STAT. 1724, 8 January 1988.

Defense Intelligence Agency, *Physical Security Standards for Construction of Sensitive Compartmented Information Facilities,* Defense Intelligence Agency (DIA) Manual 50-3, February 1990.

Defense Intelligence Agency, Security of Compartmented Computer Operations (U), DIA Manual 50-4, CONFIDENTIAL, 1980.

Defense Intelligence Agency, *Security Requirements for Automatic Data Processing (ADP) Systems,* DlA Regulation 50-23, 14 March 1979.

Defense Intelligence Agency, *Sensitive Compartmented Information Contractor Administrative Security,* DlA Manual 50-5, FOR OFFICIAL USE ONLY (FOUO), VoI. 1,10 May 1983.

Department of the Air Force, *Computer Security Policy,* AF Regulation 205-16, FOUO, 28 April 1989.

Department of the Army, *Security: Information Systems Security,* Army Regulation No. 380-19,4 September 1990.

Department of Defense, *Automated Data Processing Security Manual - Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating,* Department of Defense (DOD) 5200.28-M, 1 January 1973 with change pages in June 1979 (now under revision).

Department of Defense, *Communications Security (COMSEC)* (U), Department of Defense Directive (DODD) C-5200.5, CONFIDENTIAL, 21 April 1990.

Department of Defense Computer Security Center, *Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments,* CSC-STD-003-85, 25 June 1985.

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

Department of Defense Computer Security Center, *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,* CSC-STD-004-85, 25 June 1985.

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

Department of Defense, Control of Compromising Emanations (U), DODD S-5200.19, SECRET, 23 February 1990.

Department of Defense, *DOD Information Security Program,* DODD 5200.1, 7June1982.

Department of Defense, *DOD Personnel Security Program,* DODD 5200.2, 20 December 1979.

Department of Defense, *Industrial Security Manual for Safeguarding Classified Information,* DOD 5220.22-M, 3 January 1991.

Department of Defense, *Industrial Security Program,* DODD 5220.22, 1 November 1986.

Department of Defense, *Industrial Security Regulation,* DOD Regulation 5220.22-R, December 1985.

Department of Defense, Information Security Program Regulation, DOD Regulation 5200.1-R, June 1986.

Department of Defense, *Information Security Program Regulation,* DOD 5200.1 -R/AFR 205-1, April 1987.

Department of Defense, *Security Requirements for Automated Information Systems (AISs),* DODD 5200.28,21 March 1988.

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

Department of the Navy, *Department of the Navy Automatic Data Processing Security Program,* Chief of Naval Operations Instruction (OPNAVlNST) 5239.1A with change 1,3 August 1982.

Department of the Navy, *Department of the Navy Automated Information Systems (AIS) Security Program,* SECNAVINST 5239.2,15 November 1989.

Department of the Navy Sensitive Compartmented Information (SCl)/lntelligence, *Automated Information System (AIS) Security Program,* NAVlNTCOMlNST 5239.3,23 July 1990.

Director of Central Intelligence, *Security Manual for the Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U), Supplement to Director of Central Intelligence Directive (DCID) 1/16 (U),* SECRET, 19 July 1988.

Director of Central Intelligence, *Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U),* Director of Central Intelligence Directive (DClD) 1/16, SECRET, 19 July 1988.

Executive Order, *National Security Information,* Executive Order 12356, 2 April 1982.

Ferdman, Mauro and Harriet G. Goldman and John A. Gunter, "Proposed Management Plan for Computer Security Certification of Air Force Systems," MTR-1 0774, The MlTRE Corporation, Bedford, MA, November 1989.

Headquarters Department of the Air Force, *Information Systems: Information Systems Security,* AFR 700-10,15 March 1985.

Joint Chiefs of Staff, *Safeguarding the Single Integrated Operational Plan (SIOP) (U),* Memorandum MJCS 75-87, SECRET, 20 May 1987.

Joint Chiefs of Staff, *Security Policy for the WWMCCS Intercomputer Network,* JCS Pub. 6-03.7, April 1988.

National Computer Security Center (NCSC), *Computer Viruses: Prevention, Detection, and Treatment,* C1 -Technical Report-001,12 March 1990.

National Computer Security Center (NCSC), *Glossary of Computer Security Terms,* NCSC-TG-004, 21 October 1988.

National Computer Security Center, *A Guide to Understanding Data Remanence in Automated Information Systems,* NCSC-TG-025, September 1991.

National Computer Security Center, *A Guide to Understanding Trusted Facility Management,* NCSC-TG-01 5, 18 October 1989.

National Computer Security Center, *Trusted Network Interpretation Environments Guideline,* NCSC-TG-01 1, 1 August 1990.

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

National Institute of Standards and Technology, United States Department of Commerce, *Computer Data Authentication,* Federal Information Processing System Publication (FIP5 PUB) 113,30 May 1985.

National Institute of Standards and Technology, United States Department of Commerce, *Glossary for Computer Systems Security,* FIPS PUB 39, February 1976.

National Institute of Standards and Technology, United States Department of Commerce, *Guideline for Automatic Data Processing Risk Analysis,* FIPS PUB 65, August 1979.

National Institute of Standards and Technology, United States Department of Commerce, *Guideline for Computer Security Certification and Accreditation,* FlPS PUB 102,27 September 1983.

National Institute of Standards and Technology, United States Department of Commerce, *Guidelines for ADP (Automatic Data Processing) Contingency Planning,* FlPS PUB 87, 27 March 1981.

National Institute of Standards and Technology, United States Department of Commerce, *Guidelines for Security of Computer Applications,* FlPS PUB 73, 30 June 1980.

National Institute of Standards and Technology, United States Department of Commerce, *Overview of Computer Security Certification and Accreditation,* Special Publication (SPEC

PUB) 500-109, April 1984.

National Institute of Standards and Technology, United States Department of Commerce, *Security of Personal Computer Systems: A Management Guide*, SPEC PUB 500-120, January 1985.

National Institute of Standards and Technology, United States Department of Commerce, *Technology Assessment: Methods for Measuring the Level of Computer Security*, SPEC PUB 500-133, October 1985.

National Security Agency/Central Security Service (NSA/CSS), *The NSA/CSS Operational Computer Security Manual*, NSA/CSS Manual 130-1, FOUO, l7October 1990.

National Security Agency/Central Security Service, *Security for Automated Information Systems and Networks*, NSA-CSS Directive 10-27, 4 January 1990.

National Security Agency, *Information System Security Products and Services Catalogue*, quarterly updates. The catalogue contains the following:

Cryptographic Products List

Endorsed Data Encryption Standard (DES) Products List

Protected Services List

Evaluated Products List

U.S. Government Preferred Products List

Degausser Products List

National Telecommunications and Information Systems Security Committee, *Advisory Memorandum on Office Automation Security Guideline, National Telecommunications and Information Systems Security Advisory Memorandum* (NTISSAM) COMPUSECN -87, 16 January 1987.

National Telecommunications and Information Systems Security Committee, *TEMPEST Countermeasures for Facilities (U)*, National Telecommunications and Information Systems Security Instruction (NTISSI) 7000, SECRET, l7 October 1988.

Office of Management and Budget (OMB), *Internal Control Systems*, OMB Circular No. A-123, 1983.

Office of Management and Budget, *Management of Federal Information Resources*, OMB Circular No. A-I 30, December 1985.

Office of the President, *National Policy for the Security of National Security Telecommunication and Information Systems (U)*, National Security Directive (NSD) 42, CONFIDENTIAL, 5 July 1990.

Office of the President, *National Policy on Telecommunications and Automated Information Systems Security*, National Security Decision Directive (NSDD) 145, 17 September 1984.

Office of the Secretary of Defense, *Automated Information System Security*, Memorandum for the Members of the Military Departments, Chairman of the Joint Chiefs of Staff, Under Secretaries of Defense, General Counsel, Inspector General, Assistants to the Secretary of Defense, and Directors of the Defense Agencies, 1985.

REFERENCES

1. National Computer Security Center (NCSC), *Glossary of Computer Security Terms*, NCSC-TG-004, Version-I, 21 October 1988.

2. Department of Defense (DOD), *Security Requirements for Automated Information Systems (AISs)*, DOD Directive 5200.28, 21 March 1988.

3. Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, 15 August 1983.

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

5. Department of Defense, *Information Security Program Regulation*, DOD 5200.1 -R, June 1986.

6. Department of Defense Computer Security Center, *Computer Security Requirements — Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments*, CSC-STD-003-85, 25 June 1985.

7. Director of Central Intelligence, *Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)*, DClD 1/16, SECRET, 19 July 1988.

ACRONYMS

ADP	Automatic Data Processing
ADPSO	ADP Security Officer
ADPSSO	ADP System Security Officer
AFR	Air Force Regulation
AS	Automated Information System
AR	Army Regulation
BCSSM	Base Communications-Computer Systems Security Manager
BCSSO	Base Communications-Computer Systems Security Officer
CFM	Computer Facility Manager
CISSM	Component Information System Security Manager
COMNAVCOMTELCOM	Commander, Naval Computer and Telecommunications Command
COMPUSEC	Computer Security
COMSEC	Communications Security
COTS	Commercial-Off-The-Shelf
CSSM	Communications-Computer System Security Manager
CSSO	Computer System Security Officer
CSTVRP	Computer Security Technical Vulnerability Reporting Program
CSWG	Computer Security Working Group
DAA	Designated Approving Authority/ Designated Accreditation Authority
DAC	Discretionary Access Control
DCID	Director of Central Intelligence Directive
DES	Data Encryption Standard
DIA	Defense Intelligence Agency
DIAM	Defense Intelligence Agency Manual
DOD	Department of Defense
DODD	Department of Defense Directive
EO	Executive Order
EPL	Evaluated Products List
FIPS PUB	Federal Information Processing System Publication
FOIA	Freedom of Information Act
I&A	Identification and Authentication
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISSPM	Information System Security Program Manager
MAC	Mandatory Access Control
MACOM	Major Army Command
MAJCOM	Major Command (Air Force)

MCSSM	MAJCOM CSSM
MDIC	Military Department Intelligence Officer
MLS	Multilevel Security
MSO	Media Sanitation Officer
N	Not Classified but Sensitive
NACSI	National Communications Security Instruction
NCSC	National Computer Security Center
NM	Network Manager
NSA	National Security Agency
NSD	National Security Directive
NSDD	National Security Decision Directive
NSM	Network Security Manager
NSO	Network Security Officer
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory Memorandum
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTCB	Network Trusted Computing Base
NTISSAM	National Telecommunications and Information Systems Security Advisory Memorandum
NTISSD	National Telecommunications and Information Systems Security Directive
NTISSI	National Telecommunications and Information Systems Security Instruction
NTISSP	National Telecommunications and Information Systems Security Policy
OMB	Office of Management and Budget
OPNAVINST	Chief of Naval Operations Instruction
PM	Program Manager
RI	Risk Index
SAPI	Special Access Program for Intelligence
SCI	Sensitive Compartmented Information
SFUG	Security Features User's Guide
SIO	Senior Intelligence Officer
SIOP-ESl	Single Integrated Operational Plan-Extremely Sensitive Information
SPEC PUB	Special Publication
SPM	Security Program Manager

SSM	System Security Manager
TASO	Terminal Area Security Officer
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria
TEMPEST	(Not an acronym)
TFM	Trusted Facility Manual
TNI	Trusted Network Interpretation
TNIEG	Trusted Network Interpretation Environments Guideline
WWMCCS	Worldwide Military Command and Control System

GLOSSARY

After each definition, the source is listed.

Access. A specific type of interaction between a subject (i.e., person, process, or input device) and an object (i.e., an AIS resource such as a record, file, program, or output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified, sensitive unclassified, or unclassified information. (DODD 5200.28)

Accountability. The property that enables activities on an AIS to be traced to individuals who may then be held responsible for their actions. (DODD 5200.28; AFR 205-16)

Accreditation. A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. (DODD 5200.28)

Administrative Security. The management constraints and supplemental controls established to provide an acceptable level of protection for data. Synonymous with procedural security. (NCSC-TG-004-88)

Audit Trail. A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. (DODD 5200.28; FlPS PUB 39)

Authenticate. To establish the validity of a claimed identity. (DOD 5200.28-STD; JCS PUB 6-03.7)

Authorization. Granting the right of access to a user, a program, or a process. (FlPS PUB 39)

Automated Information System (AIS). An assembly of computer hardware, firmware, and software configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. (DODD 5200.28; DClD 1/16)

Certification. The technical evaluation, made as part of and in support of the accreditation process, that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. (AR 380-19; DODD 5200.28)

Classified Information. Information or material that is (a) owned by, produced for or by, or under the control of the U.S. Government; and (b) determined under Executive Order 12356, or prior order, DOD 5200.1 -R, to require protection against unauthorized disclosure; and (c) so designated. (DODD 5200.28)

Closed Security Environment. An environment that includes those systems in which both of the following conditions hold true:

a. Application developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of data to

be processed is Confidential or below, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of data to be processed is Secret or above, developers have at least a Secret clearance.

b. Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during operation of system applications. (CSC-STD-003-85; CSC-STD-004-85)

Communications Security (COMSEC). The protection that insures the authenticity of telecommunications and which results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunications. (FlPS PUB 39)

Compartmented Mode. An AIS is operating in compartmented mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following:

a. A valid personnel clearance for the most restricted information processed in the AIS.

b. Formal access approval for, and has signed nondisclosure agreements for that information to which he/she is to have access.

c. A valid need-to-know for that information to which he-she is to have access. (NCSC-TG-004-88)

Compromising Emanations. Unintentional data related or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmission received, handled or otherwise processed by any information processing equipment. (AR 380-19; NCSC-TG-004-88; AFR 205-16)

Controlled Mode. The mode of operation that is a type of multilevel security mode in which a more limited amount of trust is placed in the hardware/software base of the system, with resultant restrictions on the classification levels and clearance levels that may be supported. (CSC-STD-003-85)

Countermeasure. Any action, device, procedure, technique or other measure that reduces the vulnerability of or threat to a system. (NCSC-TG-004-88)

Covert Channel. A communications channel that allows a process to transfer information in a manner that violates the system's security policy. (DOD 5200.28-STD; AFR 205-16)

Data. A representation of facts, concepts, information, or instructions suitable for communication, interpretation or processing by humans or by an AIS. (DODD 5200.28)

Data Owner. The authority, individual, or organization who has original responsibility for the data by statute, executive order, or directive. (DODD 5200.28)

Declassification. An administrative decision or procedure to remove or reduce the security classification of the subject media. (NCSC-TG-004-88)

Dedicated Security Mode. A mode of operation wherein all users have the clearance or authorization, documented formal access approval, if required, and the need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. (DODD 5200.28)

Degauss. To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media, usually tapes. The process involves increasing the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media. (FlPS PUB 39)

Denial of Service. Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability. (DODD 5200.28)

Designated Approving Authority (DAA). The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level such that he or she has authority to evaluate the overall mission requirements of the AIS and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS. (DODD 5200.28)

Emission Security. The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and from an analysis of compromising emanations from systems. (NCSC-TG-004)

Evaluated Products List (EPL). A documented inventory of equipments, hardware, software, and/or firmware that have been evaluated against the evaluation criteria found in DOD 5200.28-STD. (DODD 5200.28)

Formal Access Approval. Documented approval by a data owner to allow access to a particular category of information. (DODD 5200.28)

Identification. The process that enables, generally by the use of unique machine- readable names, recognition of users or resources as identical to those previously described to an AIS. (DOD 5200.28-M)

Information System Security Officer (ISSO). A person responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal. (DODD 5200.28)

Information Systems Security (INFOSEC). A composite of means to protect telecommunications systems and automated information systems, and the information they process. (AR 380-19)

Isolation. The containment of users and resources in an AIS in such a way that users and processes are separate from one another as well as from the protection controls of the operating system. (FlPS PUB 39)

Least Privilege. This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. (DOD 5200.28-STD)

Multilevel Secure. A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and need-to-know, but prevents users from obtaining access to information for which they lack authorization. (DOD 5200.28-5TD)

Multilevel Secure Mode. A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance, authorization, or formal access approval for all information handled by the AIS. (DODD 5200.28)

Need-To-Know. The necessity for access to, knowledge of, or possession of specific information required to carry out official duties. (NCSC-TG-004-88)

Network. A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices. (DODD 5200.28)

Network Trusted Computing Base (NTCB). The totality of protection mechanisms within a network system-including hardware, firmware, and software-the combination of which is responsible for enforcing a security policy. The NTCB is the network generalization of the trusted computing base (TCB). (NCSC-TG-01 1)

Open Security Environment. An environment that includes those systems in which one of the following conditions holds true:

a. Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic. (See Closed Security Environment for an explanation of sufficient clearance.)

b. Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications. (NCSC-TG-004-88)

Orange Book. Common name for *Department of Defense Trusted Computer System Evaluation Criteria,* DOD 5200.28-STD.

Partitioned Mode. A mode of operation in which all persons have the clearance, but not necessarily the need-to-know and formal access approval, for all data handled by the AIS. This mode encompasses compartmented mode as defined by DCID 1/16. (DODD 5200.28)

Password. A private character string that is used to authenticate an identity. (DOD 5200.28-STD)

Periods Processing. A security mode of operation and/or maximum classification of data handled

is established for an interval of time, then changed for the following interval of time. The period extends from the time when the system is securely initialized to the time when the system is purged of all sensitive data handled during the processing period. (DODD 5200.28)

Personnel Security. The procedures established to insure that all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances. (FlPS PUB 39)

Physical Security. (1) The use of locks, guards, badges, and similar administrative measures to control access to the computer and related equipment. (2) The measures required for the protection of the structures housing the computer, related equipment and their contents from damage by accident, fire, and environmental hazards. (FlPS PUB 39)

Procedural Security. Synonym for administrative security.

Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk. (DODD 5200.28)

Risk Analysis. An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. (DODD 5200.28)

Risk Management. The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review. (DODD 5200.28)

Security Features. The security-relevant functions, mechanisms, and characteristics of AIS hardware and software (e.g., identification, authentication, audit trail, and access control). (DODD 5200.28)

Security Mode. A mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, and partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the AiS. (DODD 5200.28)

Security Policy. The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. (DOD 5200.28-STD)

Security Safeguards. The protective measures and controls that are prescribed to meet the security requirements specified for an AIS. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices. (NCSC-TG-004-88)

Sensitive Compartmented Information (SCI). Classified information about or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director, Central Intelligence. (DODD 5200.28)

Sensitive Unclassified Information. Any information the loss, misuse, or unauthorized access to, or modification of which, might adversely affect U.S. national interest, the conduct of DOD programs, or the privacy of DOD personnel (e.g., FOIA exempt information and information whose distribution is limited by DOD Directive 5230.24). (DODD 5200.28)

Special Access Program. Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance of investigative requirements, special designation of officials authorized to determine need-to-know, or special lists of persons determined to have a need-to-know. (DODD 5200.28)

System High Security Mode. A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval. (DODD 5200.28; AFR 205-16)

Technical Vulnerability. A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system. (NCSC-TG-004-88; AR 380-19)

TEMPEST. The study and control of spurious electronic signals emitted from AIS equipment. (DOD 5200.28-STD)

Threat. Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. (NCSC-TG-004-88)

Trusted Computing Base (TCB). The totality of protection mechanisms within a computer system - including hardware, firmware, and software - the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user s clearance) related to the security policy. (NCSC-TG-004-88; AFR 205-16)

Trusted Products. Products evaluated and approved for inclusion on the Evaluated Products List (EPL). (DODD 5200.28)

Users. People or processes accessing an AIS either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual). (DODD 5200.28; AFR 205-16; AR 380-19)

Vulnerability. A weakness that may be exploited by a threat agent to cause harm to the AIS. The totality of susceptibilities to specific attack and the opportunity available to a hostile entity to mount that attack. (NCSC-TG-004-88)

Q U S. GOVERNMENT PRINTING OFF/GEI 993-718-426161075

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	May 1992	Final

4. TITLE AND SUBTITLE
A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems

5. FUNDING NUMBERS

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Security Agency
Attention: C81; Standards, Criteria, and Guidelines Division
9800 Savage Road
Fort George G. Meade, MD 20755-6000

8. PERFORMING ORGANIZATION REPORT NUMBER
NCSC-TG-027

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
Library No. S-238,461

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release: Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This guideline helps Information System Security Officers (ISSOs) understand their responsibilities for implementing and maintaining security in a system. It introduces security regulations, policies, and standards. The operational environment is discussed, specifically the type of information processed and the security modes of operation. The guideline focuses on the ISSO's responsibilities related to physical and administrative security, training, configuration management, access control, risk management, audits, and certification and accreditation. 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 Department of Defense component regulations and standards. This document should be considered as a baseline with more detailed security guidelines provided by each agency, branch, or command. An extensive bibliography is included.

14. SUBJECT TERMS
Mode of Operation, Physical Security, Administrative Security, Configuration Management, Access Control, Risk Management, and Audit.

15. NUMBER OF PAGES
71

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	