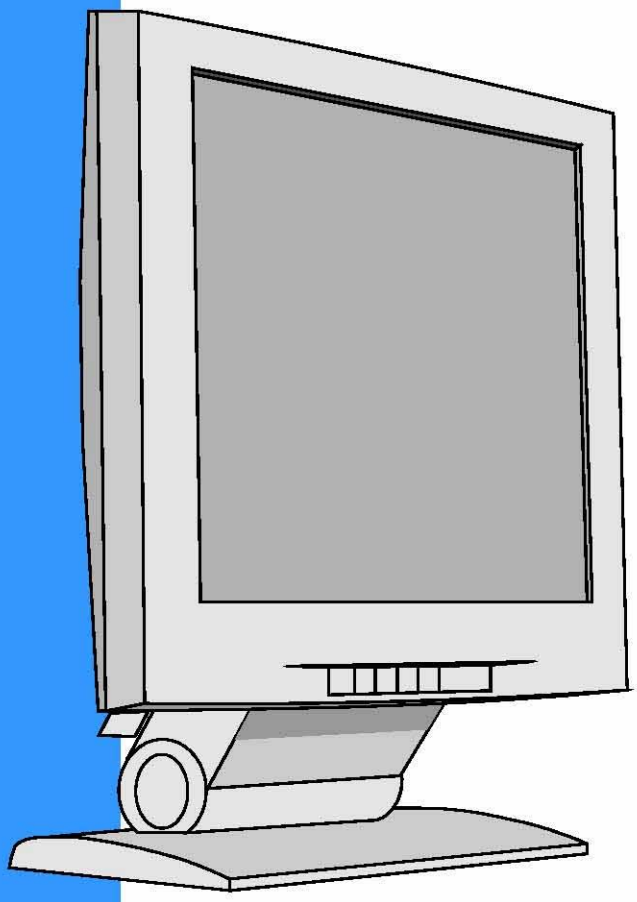

NISPOM Chapter 8 Requirements for Industry Online Course Notes

Table of Contents

Module 1: Classified IS Environment 3
Lesson 1: Introduction to the National Industrial Security Program 3
Topic 1: Introduction to the National Industrial Security Program Overview 3
Topic 2: Introduction to Roles and Responsibilities 6
Topic 3: Introduction to ISSM/ISSO Roles and Responsibilities 7
Topic 4: Introduction to Information Systems Users 9

Module 2: IS Threats and Vulnerabilities 12
Lesson 1: Introduction to Information System Threats and Vulnerabilities 12
Topic 1: Introduction to Information System Threats 12
Topic 2: Introduction to Information System Protection Strategies 15
Topic 3: Lesson Summary 17

Module 3: Accreditation Process 18
Lesson 1: Introduction to Protection Measures 18
Topic 1: Introduction to Levels of Concern 18
Topic 2: Introduction to Protection Levels 19
Lesson 2: Introduction to Information System Security Documentation 21
Topic 1: Introduction to Information System Security Documentation 21
Topic 2: Introduction to Common Requirements 27
Lesson 3: Introduction to Certification and Accreditation 32
Topic 1: Identify the System Security Plan (SSP) process 32
Topic 2: Introduction to the Accreditation Process 33
Topic 3: Introduction to Master System Security Plan 38

Module 4: Non-Technical Requirements 41
Lesson 1: Introduction to Physical Security and Maintenance 41
Topic 1: Introduction to Physical Security Controls 41
Topic 2: Introduction to Physical Security Requirements 43
Topic 3: Introduction to Protected Distribution Systems (PDS) 46
Topic 4: Introduction to Maintenance 50
Lesson 2: Introduction to Hardware and Software Controls 54
Topic 1: Introduction to Software Security Procedures 54
Topic 2: Introduction to Hardware Examination Requirements 56
Topic 3: Introduction to Marking Requirements 57
Lesson 3: Introduction to Information Systems Operation 59
Topic 1: Introduction to Clearing and Sanitizing Requirements 60
Topic 2: Introduction to Trusted Downloading 64
Topic 3: Introduction to Periods Processing 68

Module 5: Technical Protection Measures 70
Lesson 1: Introduction to Identification and Authentication 70
Topic 1: Introduction to Identification and Authentication Technologies 70
Topic 2: Introduction to I&A Requirements 73
Topic 3: Introduction to Session Controls 75
Lesson 2: Introduction to Audit Requirements 77
Topic 1: Introduction to Audit Trails, Records, and Logs 77
Topic 2: Introduction to Auditable Events 79

Topic 3: Introduction to Audit Analysis 82
Lesson 3: Introduction to Interconnected Systems Management 84
Topic 1: Introduction to Types of Networks 84
Topic 2: Introduction to Interconnected Network Requirements 88
Topic 3: Introduction to Securing Network Interconnections 93

Module 6: IS Administrative Inquiries 95
Lesson 1: Introduction to Administrative Inquiries 95
Topic 1: Introduction to Administrative Inquiries Overview 96
Topic 2: Introduction to the Administrative Inquiry Process 98

Module 1: Classified IS Environment

Lesson 1: Introduction to the National Industrial Security Program

National security depends on the proper protection of classified information. Information systems that are used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information or loss of data. Ensuring that information systems (IS) with access to classified information are properly managed and protected by all contractors is a primary responsibility of the National Industrial Security Program (NISP).

In this lesson, you will learn about the NISP and the Government's and contractors'[1] roles and responsibilities in the NISP.

Lesson Objectives

At the end of this lesson, you will be able to:

- Identify the purpose and organization of the NISP
- Identify the Government's and contractor's roles in certification and accreditation
- Identify the responsibilities of the ISSM and ISSO
- Identify privileged and general information system users

Topic 1: Introduction to the National Industrial Security Program Overview

A company becomes involved in the National Industrial Security Program (NISP) when it is contracted to provide research, products or services requiring access to classified information. The NISP establishes the guidelines to ensure that the classified information entrusted to industry - government contractors - is adequately safeguarded.

In this topic, you will learn about the purpose and organization of the National Industrial Security Program.

The National Industrial Security Program

The National Industrial Security Program (NISP) was established by Executive Order 12829 in 1993. The NISP is a partnership between Government and industry designed to create a single, integrated and cohesive industrial security program to protect classified information within government contractors and to preserve our nation's economic and technological interests.

The authority to accomplish this task was established by:

- Executive Order 12829, National Industrial Security Program

In addition there are Legislative Acts, (e.g., the Arms Export Control Act and the Atomic Energy Act of 1954), Judicial decisions, (e.g., those involved with the adverse reporting requirements) and other executive orders, (e.g., 12958, Classified National Security Information) that play a part in the administration and implementation of the NISP.

The NISP applies to all executive branch departments and agencies and to all cleared contractor facilities located within the United States, its Trust Territories and Possessions.

National Industrial Security Program Organization

Responsibility for the NISP rests with the following organizations and agencies:

- The National Security Council

  The National Security Council (NSC) provides policy and program guidance for the NISP.

- Information Security Oversight Office

  Under Executive Order 12829, the Director of the Information Security Oversight Office (ISOO) is responsible to the President for policy oversight of the Government-wide security classification system and the NISP.

- Secretary of Defense

  The Secretary of Defense serves as executive agent under the NISP and in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission and the Director of Central Intelligence is responsible for issuance and maintenance of the NISPOM (National Industrial Security Program Operating Manual). The Secretary of Defense is also responsible for granting facility and personnel security clearances and conducting inspections of non-Government facilities.

- Defense Security Service

  The Defense Security Service (DSS) administers the NISP on behalf of the Department of Defense (DoD). This means that DSS administers the policy decided at the DoD and NSC level. DSS does not create policy.

National Industrial Security Program Operating Manual

NISP requirements, restrictions and safeguards are documented in the National Industrial Security Program Operating Manual (NISPOM). The NISPOM serves as a guide to the activities of contractors accessing classified information released by U.S. Government Executive Branch Departments and Agencies. The Secretary of Defense is responsible for issuing the NISPOM.

Cognizant Security Agencies

The four Cognizant Security Agencies (CSA) are Agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are;

- The Central Intelligence Agency (CIA)
- The Nuclear Regulatory Commission (NRC)
- The Department of Energy (DOE)
- The Department of Defense (DoD)

Heads of the Executive Branches are required to enter into agreements with the Secretary of Defense that establish the terms of the Secretary of Defense's responsibilities on behalf of these agency heads for administration of industrial security on their behalf.

Cognizant Security Offices

The offices responsible for administering the NISP for the CIA, NRC, DOE and DoD are known as Cognizant Security Offices (CSOs). The CIA, NRC and DOE serve as both Cognizant Security Agencies and Cognizant Security Offices (administering the NISP). The Defense Security Service (DSS) is the Cognizant Security Office responsible for administering the NISP on behalf of DoD. DSS also administers the NISP for non DoD agencies with which DoD has agreements. Cognizant Security Offices are responsible for performing:

- Oversight
- Program review
- Training
- Certification and accreditation of contractor information systems

Government Contracting Activity

A Government Contracting Activity (GCA) is an element of a Federal department or agency that is designated to issue classified contracts for that department or agency.

DSS provides oversight on behalf of the DoD Government Contracting Activities to ensure the classified information they have released to contractors is properly protected.

The Defense Security Service (DSS)

The Defense Security Service (DSS) is responsible for:

- Implementation of NISP policy and NISPOM procedures for DoD and DoD signatories
- Monitoring and coordinating program support for:
  - Facility Clearance Branch
  - The Industrial Security Program Field Operation
  - Defense Security Service Academy (DSSA)

Certification and Accreditation

One of the key activities in implementing the NISP policy and the NISPOM procedures is to Certify and Accredit contractor information systems.

The NISP requires that contractor information systems be certified and accredited before classified information can be stored, processed or transmitted on their information system.

The ISSM is responsible for certifying to DSS, in writing, that each System Security Plan has been implemented; that the specified security controls are in place and properly tested; and that the IS is functioning as described in the SSP.

As the Cognizant Security Office for DoD and its GCAs, the Defense Security Service (DSS) is responsible for performing certification and accreditation of contractor information systems.

DSS Staff: The Industrial Security Representative

Contractors work closely with DSS both during and after the certification and accreditation process. The greatest involvement is with the DSS Industrial Security Representative (IS Rep).

The DSS Industrial Security Representative:

- Provides advice and assistance to improve the contractor's overall security posture
- Provides education and motivation to enhance program knowledge and performance
- Surveys, inspects and, in some cases certifies/validates, the contractor's information system to assess its compliance with NISP requirements.

DSS Staff: Additional Defense Security Service Professionals

The DSS Industrial Security Representative (IS Rep) is supported by the following DSS professionals in the NISP:

- Information System Security Professionals (ISSP) - responsible for complex technical information system security certifications and review
- Counterintelligence Specialists - support Local and National DoD Counterintelligence (CI) objectives through their support to DSS missions and prepare threat awareness briefings for contractors as a result of their coordination and liaison with Federal and DOD Counterintelligence entities

• Regional DAA - serve as the Designated Approving Authority (DAA)[2] for NISP contractor information systems and provide technical assistance to Information System Security Professionals (ISSPs).

Contractor Staff and the National Industrial Security Program

Contractor personnel also have a role in the NISP process. The NISP requires contractors to appoint a Facility Security Officer (FSO) and Information System Security Manager (ISSM) to supervise and direct security measures necessary for safeguarding classified information. This individual(s) is instrumental in the NISP certification/accreditation process.

Topic 2: Introduction to Roles and Responsibilities

In the previous topic, you learned about the purpose and organization of the NISP.

Before being allowed to capture, create, store, process or distribute classified information on its information system, a contractor must demonstrate that the system is properly managed and protected.

In this topic, you will learn about the Government's and contractor's roles and responsibilities in the NISP certification and accreditation process.

Reference: NISPOM Chapter 8 Section 1

Cognizant Security Office Roles and Responsibilities

As the CSO for DoD, the Defense Security Service (DSS) is responsible for performing the oversight; program review; training; and certification and accreditation of information systems used by DoD contractors.

As a part of the official certification and accreditation process for contractor information systems (IS), DSS appoints IS Reps and (if the complexity warrants) ISSPs as the Certifying/Validating officials. The Designated Approving Authority (DAA) will be the DSS Office of Designated Approving Authority (ODAA).

Note: If complexity warrants, a DSS ISSP may work in conjunction with the IS Rep.

Designated Approving Authority Responsibilities

Within the NISP, the Designated Approving Authority (DAA) is the government official with the authority to formally accredit operation of the contractor's IS. The DAA formally accepts security responsibility for the operation of the IS and officially declares that the contractor's IS environment effectively protects classified information from unauthorized disclosure. The DAA's accrediting decision shows that adequate care has been taken to fulfill the security requirements of the NISPOM.

Defense Security Service Certification/Accreditation Responsibility

DSS has established an internal program for conducting official Certifications and Accreditations for contractor IS. The IS Rep is the certifying/validating official for standalone systems with no technical features at Protection Level 1.

For all other systems (e.g., wide area networks, local area networks or standalone systems with technical features such as automated Identification & Authentication and automated auditing), the certifying official is the IS Rep or ISSSP, depending on the level of complexity, and the DAA is the DSS assigned Regional Designated Approving Authority (RDAA). The RDAA is part of the ODAA.

Contractor Management Roles and Responsibilities

Contractor management has two very important responsibilities within the NISP. The first is to publish and promulgate an information system (IS) Security Policy addressing the classified processing environment. This IS Security Policy provides direction for all company personnel and is a requisite part of the certification and accreditation process.

A second important contractor responsibility is to appoint an Information System Security Manager (ISSM). The ISSM is appointed by the FSO to supervise and direct the security measures necessary for safeguarding classified information on information systems. Contractor management must ensure that the ISSM is trained to administer the responsibilities identified in the NISPOM, paragraph 8-103.

Topic 3: Introduction to ISSM/ISSO Roles and Responsibilities

In the previous topic, you learned about the Government's and contractor's roles and responsibilities in safeguarding classified information. You learned that one of the responsibilities of contractor management is to appoint an Information System Security Manager (ISSM). In some cases, an Information System Security Officer (ISSO) must also be appointed.

In this topic, you will learn about the roles and responsibilities of the ISSM and the ISSO.

Reference: NISPOM Chapter 8, Section 4

The Information System Security Manager

The ISSM plays a key role in the information system security process. The ISSM has oversight responsibility for the development, implementation and evaluation of the facility's information system security program and is instrumental in developing the System Security Plan (SSP) required for certification and accreditation. The ISSM is also responsible for daily supervision of the facility's IS Security Program.

The ISSM can be the Facility Security Officer (FSO) or another person in the facility. If the ISSM and FSO are two different people, the ISSM reports security issues to the FSO. In this case, the FSO, who has overall security responsibility, relies on the ISSM for technical issues regarding the accredited information systems within the company.

The Information System Security Manager Requirements

The ISSM must meet the following requirements:

- Be an employee of the company
- Have the appropriate personnel security clearance
- Have all formal access approvals (if applicable) and

- Have a need-to-know for all classified information processed on the company's information systems

The ISSM must have a working knowledge of system functions, security policies, technical security safeguards and operational security measures. If necessary an alternate ISSM may be appointed with all the same rights and privileges of the Primary ISSM.

Information System Security Managers at Multiple Facility Organizations

In a multiple facility organization, the ISSM can be assigned oversight responsibility for multiple facilities, provided the travel time between these facilities is reasonable travel time. The ISSM must be able to effectively manage the IS and be trained to a level commensurate with the overall complexity of all facilities. If the facilities cannot be effectively managed local ISSM's must be appointed.

Information System Security Manager Responsibilities: Inspection

One of the ISSM's responsibilities includes ensuring that periodic self-inspections of the facility's information system security program are conducted as part of the overall facility self-inspection program, and that corrective action is taken for all identified findings and vulnerabilities. Self-inspections are conducted to ensure that the information system is operating as accredited and that accreditation conditions have not changed.

The link below will launch a tool that can be used when preparing for and conducting a self-inspection of the information system program. The tool contains an IS (Information System) portion within the Self-Inspection Handbook for NISP Contractors that can be tailored to an Information System program.

Go to "www.dss.mil" DSS Academy "downloads" and select "Self Inspection Handbook for NISP Contractors" from the list.

Information System Security Manager Responsibilities: Education, Training & Awareness

Education, training and awareness are essential elements in the effective implementation of a contractor information system security program. Another ISSM responsibility is to develop, document and present IS security education within the company. A variety of methods can be used to include:

- Passive reinforcement, provided by posters and brochures
- The use of awareness products (DSS web site, http://www.dss.mil, provides a variety of security awareness products and resources)
- Formal classroom environment and computer based training courses (DSS Academy provides a variety of security courses both classroom as well as computer based)

Regardless of the method used, IS security training and awareness must be provided to all users of the system, including system administrators, all personnel involved with system operations, maintenance as well as management. All must be aware of their security responsibilities with IS.

The Information System Security Officer

In certain cases, an Information System Security Officer is appointed by the Information System Security

Manager. The ISSO(s) is appointed by the ISSM when:

- A facility has multiple accredited information systems
- The information system is in a multiple facility organization in which the ISSM has oversight responsibility for multiple locations, or
- The technical complexity of the facility's information system program warrants the appointment.

The ISSO(s) is an individual appointed by the ISSM, who is responsible for monitoring the contractor's IS on a continuing basis. The ISSO(s) ensures that the hardware; software; installation; and maintenance, as applicable, conform to appropriate requirements. The ISSO(s) also monitors access to each assigned information system.

NISPOM paragraph 8-104 lists the duties to which ISSOs can be assigned.

Information System Security Officer Requirements

An ISSO is not required to be an employee of the contractor. However, an ISSO must have:

- A personnel security clearance equal to the highest level of classified information on the system(s) he/she is responsible for
- Need-to-know for all classified information on the system(s)
- Formal access approvals for all classified information processed on the system(s) for which the ISSO has responsibility.

Topic 4: Introduction to Information Systems Users

In the previous topic, you learned about the roles and responsibilities of the ISSM and ISSO.

While we have been discussing how NISP affects information systems, it is the privileges and activities of the users that determine whether classified information is protected or compromised.

Care must be given to ensure that only those users who are authorized to access classified information are able to capture, process, and store material.

In this topic, you will learn the difference between privileged and general IS users and identify the requirements IS users must meet.

Reference: NISPOM, paragraph 8-105

Information System Users

Personnel who access information systems play an integral role in protecting (or potentially damaging) the security of that system. Their access to information must be carefully controlled and monitored to ensure that only those users who are authorized to access classified information are able to do so. This process begins by identifying the user by type.

Privileged Users

Privileged users are individuals with access to information systems control, monitor, or administrative functions (e.g. system administrators, system operators, system analysts). These individuals must have a personnel security clearance, need-to-know, and formal access approvals for all classified information on the applicable systems.

Privileged users report to the ISSM or ISSO on all security matters. Contractors need to limit the number of users with privileged access to the minimum number necessary.

General Users

General users are individuals who can input information to and/or modify information on an IS and are authorized by the ISSM or ISSO to process classified information on an accredited IS. General users must have personnel clearance, need-to-know and formal access approvals appropriate to the protection level of the IS he or she will access and are subordinate to the ISSM or ISSO on all matters related to IS Security.

Privileged and General User Requirements

Depending on the complexity and number of accredited information systems at the contractor facility, users can have one or multiple roles. Each role has separate and unique requirements that are vital to successful information systems operations. However, as specified in NISPOM 8-105, all users, regardless of type, must meet the following requirements. They must:

- Comply with the IS Security Program requirements
- Be aware of and knowledgeable about their information system security responsibilities
- Be accountable for their actions on an information system.

The Concept of Least Privilege

All information system users should be aware of the concept of least privilege, a basic tenet of computer security. The concept of least privilege means that users should be given only those rights they require to do their jobs. The more privileges a user has, the greater the potential for possible damage to the system. To ensure maximum safety of classified information on information systems, contractors are advised to:

- Keep the number of administrative accounts to a minimum
- Require administrators to use a general account (rather than an administrator account) as much as possible when performing routine activities
- Set access permissions properly. Tighten the permissions on tools that attackers might use once they gain a foothold in the system.

Lesson Summary

In this lesson, you learned:

- The purpose and organization of the NISP

The NISP establishes requirements to ensure that the classified information entrusted to industry is adequately safeguarded. The NISP organization and requirements are documented in the National Industrial Security Program Operating Manual (NISPOM).

- The Government's and contractor's roles in certification and accreditation

  The government provides a Designated Approving Authority (DAA) to conduct accreditation of contractor IS. The contractor creates an IS Security Policy and appoints an Information System Security Manager (ISSM).

- The responsibilities of the ISSM and ISSO

  The ISSM has responsibility for the development, implementation and evaluation of the facility's information system security plan. The ISSM can appoint an Information Systems Security Officer in certain cases to assist in these efforts.

- What are privileged and general information system users

  Privileged users are individuals with access to information systems control, monitor or administrative functions. General users are individuals who can input and/or modify information on an IS. Both privileged and general users must have appropriate security clearances, "need-to-know" and comply with IS Security Program requirements.

Module 2: IS Threats and Vulnerabilities

Lesson 1: Introduction to Information System Threats and Vulnerabilities

Information systems are used extensively throughout Government and industry to process, store and transmit information. Powerful, interconnected information systems enable users to access, correlate and associate more information from a greater number of sources than ever before. However, with the increased availability of more capable information systems has come an increase in the number and types of threats to these systems.

In this lesson, you will learn about several of the most common information system threats and vulnerabilities.

Lesson Objectives

After completing this lesson, you will be able to:

- Identify information system threats and vulnerabilities
- Identify strategies used to protect information systems from threats and vulnerabilities

Topic 1: Introduction to Information System Threats

The threat to information and information systems has never been greater than it is today. It is critical that you, as an Information System Security Manager (ISSM), be aware of the types of threats you may encounter and have procedures in place to deal with them.

In this topic, Information System Threats, you will learn about several of the most common types of

information system threats you may encounter.

What is a Threat?

The Department of Defense (DoD) defines a threat as "the ability of an individual or organizational entity to exceed or abuse their authorized access to exploit, attack or otherwise misuse DoD information systems."

These threats can take a number of different forms and can come from sources that are external[3] and/or internal[4] to the organization. Facilities with access to classified materials need to be prepared for threats from both sources.

Insider Threats

While internal threats, also known as insider threats, often receive less publicity than external threats, recent data indicates that they may actually be an even greater source of concern.

The reason for this is that the "insider" typically has extensive knowledge of the system and its controls and may be authorized access to sensitive information. Insiders often do not need a great deal of knowledge about computer intrusions because their knowledge of the victim system allows them to gain unrestricted access to systems and system data.

Insiders

So who is the insider? Insiders come from everywhere. The one commonality is that an "insider" works for or has a relationship with the target organization. Insiders can be:

- Employees
- Contractors
- Business partners
- Subcontractors
- Consultants
- Customers

Reasons for Insider Threats

To deal effectively with insider threats the ISSM needs to understand not only who might pose a threat, but also why. Typically, insiders cause damage for one or more of the following reasons:

- Maliciousness

  Malicious damage is the result of intentional wrongdoing on the part of an individual or organization. The source may be either external (e.g., from an agent provocateur) or internal (e.g., from a disgruntled employee). According to the Director of the National Infrastructure Protection Center at the FBI, the disgruntled insider is a principal source of computer crimes. In fact, the intentionally malicious insider threat may be one of the most challenging security

problems an ISSM faces today.

- Disdain for Security Practices

  Most computer users are hard working and aware of their responsibility to safeguard sensitive materials. However, some users are not willing to comply with required security measures. Others intentionally challenge security measures simply to prove that it can be done. An ISSM must be on the lookout for employees who seem disinclined to follow required security practices.

- Carelessness

  Even the most well-intentioned individual has the potential to become a threat. For example, an individual who forgets to secure a CD-ROM containing classified information may inadvertently allow sensitive information to fall into the hands of an unauthorized individual. Carelessness like this can present a serious threat to the integrity of an information system.

- Lack of Awareness of Security Procedures

  Over half of all insider attacks are unintentional. In many cases these "attacks" are simply mistakes, experiments or accidents rather than malicious attacks.

Social Engineering

In addition to the threats posed by insiders who are malicious, disdainful, careless or simply unaware of necessary security procedures, an ISSM also needs to be aware of the threat to information systems known as social engineering.

Social engineering is a low-tech method of cracking network security in which individuals (either inside or outside the organization) manipulate insiders into providing information needed to gain access to the organization's information system.

Social engineering plays on the human desire to be helpful and do the "right thing" and can be a very effective means of gaining access to information or an information system. Some common social engineering tactics include:

- Requesting "help" from a sympathetic and unsuspecting information system user
- Asking for information just before quitting time
- Masquerading as a valid user, manager, supervisor, or other employee from the organization
- Masquerading as a student or professional peer

Malicious Logic

A third serious threat to information system is malicious logic. Examples of malicious logic include:

- Trojan Horse
- Trap Doors
- Worms
- Bombs[5]

Computer Viruses

A computer virus is also a type of malicious logic. Viruses are generally categorized by the way they work. The three most common types are:

- Viruses that infect programs or files
- Viruses that infect the boot sector of hard disks
- Macro viruses are most common in Microsoft products, but can exist in any product, not just Microsoft

Information System Vulnerabilities

In addition to threats from insiders and malicious logic, information systems are also at risk because of inherent vulnerabilities in the technology. The contractor, Information System Security Manager (ISSM), needs to be aware of identified vulnerabilities and understand how to protect against them.

Operating System Services Vulnerabilities

Many malicious logic attacks are made possible by the vulnerabilities inherent in just a small number of common operating system services. Attackers take advantage of these known vulnerabilities to enter and exploit information systems. The rapid spread of many well-known worms[6] and viruses can be traced directly to the exploitation of these unprotected vulnerabilities.

New Product Vulnerabilities

In addition to being aware of operating system vulnerabilities, the ISSM must also be alert to the vulnerabilities of any new products[7] and new technologies[8] that come into the organization.

A device that uses wireless technology is a good example of a product that needs to be carefully reviewed before being introduced into a secure environment. Wireless technology is especially vulnerable because of the potential to transmit data beyond physical boundaries unknown to the user. Anyone who has the right software and is in the general area of the transmitter can intercept the information being transmitted.

Topic 2: Introduction to Information System Protection Strategies

In the previous topic, you learned how threats from individuals, malicious logic and inherent technological vulnerabilities can endanger information systems.

In this topic, Information System Protection Strategies, you will learn about the strategies you can use to protect an information system against these threats.

Provide Information System Security Training

The first step to ensuring that information and information systems are adequately protected from threats is to develop and deliver effective information system security training. The ISSM should ensure that all system users receive IS security training regularly and are aware of their security responsibilities with IS.

As a minimum, users should be able to:

- Recognize potential threats
- Understand required security procedures
- Recognize and quickly report any anomalies

Develop an Active Security Program

In addition to developing and delivering effective IS security training, the ISSM should also develop an active and ongoing security program. The following strategies, which are all elements of an active security program, help minimize the potential danger from IS security threats.

- Develop and Promote a Clear Security Policy

  Develop and promote a clear security policy designed to protect all identified information assets. Use state-of-practice and new technology to enforce and support the policy.

- Strengthen Personnel Security and Management Practices

  Reduce threats by establishing a high level of assurance in the trustworthiness of people, practices, systems and programs. Develop and support a motivated, skilled and security-responsive workforce.

- Detect Potential Problems Quickly

  Actively look for potential threats or problems, whether isolated or correlated, that may result in malicious activity.

- React and Respond

  Correct suspected and actual unacceptable insider behavior using sound personnel security and system management practices. Seek legal or other appropriate management remedies to support possible prosecution.

Implement Security Practices

Another security strategy is to ensure that appropriate information security practices are followed including:

- Proper implementation of security features and the regular testing of these features
- Installation and regular updating of anti-virus software
- Conduct of regular self-inspections
- Regular review of audit records
- Recognition of and quick response to signs of malicious[9] logic contamination
- Regular backup of system files

Stay Current

Even the most well-designed security program can become vulnerable if the ISSM fails to stay current and implement necessary changes. To ensure the ongoing security of an IS, the ISSM should:

- Use current version operating systems and applications

  Use the latest available and stable versions of the operating systems and the applications on all of the computers on the network.

- Install updates regularly

  Keep operating systems and applications current by installing the latest updates (e.g., patches, service packs, and hotfixes), especially updates that correct vulnerabilities that could allow an attacker to execute code.

- Review new product purchases

  Involve security personnel in the procurement process to ensure that security aspects of new purchases are considered. Exercise care with the use of wireless technologies.

  Wireless Technologies

  Implement security procedures to mitigate risks associated with wireless devices in areas where employees are working with classified information and/or where classified discussions may be held. FSOs and ISSMs must consider the capabilities of wireless devices and use sound judgment in developing appropriate security countermeasures. Depending on the device/technology, appropriate countermeasures may range from ensuring a wireless device is turned off or not used in classified areas to, in some cases, not permitting the devices in the area.

Topic 3: Lesson Summary

In this lesson, you learned about:

- Information System Threats and Vulnerabilities

  In this topic, you learned about four common types of information system threats:

  Insider Threats

  Social Engineering Threats

  Malicious Logic Threats

  Vulnerability Threats

- Information System Protection Strategies

  In this topic, you learned about some of the strategies used to protect information and information systems against threats. You learned how important it is to provide security training for all system users and reviewed guidelines for developing an active security program. You also learned how to implement security measures and ensure ongoing security for your system.

Module 3: Accreditation Process

Lesson 1: Introduction to Protection Measures

Information assurance is the discipline that includes the measures that protect and defend information and information systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.

In this lesson, you will learn about required IS protection measures as specified in the NISPOM. This course will focus on the protection requirements for Protection Level 1.

Reference: NISPOM Chapter 8 Section 4

Lesson Objectives

After completing this lesson, you will be able to:

- Identify the attributes of information assurance
- Identify the factors that determine Protection Levels

Topic 1: Introduction to Levels of Concern

The NISPOM mandates that information systems be protected and defended. In this topic, you will learn about the three attributes of information assurance included in the NISPOM.

Reference: NISPOM paragraph 8-401

Information Assurance Attributes

Measures implemented to protect and defend information and information systems must ensure that three attributes of information assurance are secure:

- Confidentiality[10]
- Integrity[11]
- Availability[12]

Note: Confidentiality is mandated by the NISPOM. Integrity and Availability are necessary only if contractually mandated. However, Integrity does apply when it has a direct impact on protection measures for Confidentiality (e.g. the integrity of the password file and integrity of the audit logs).

Level of Concern

To reflect information sensitivity level and consequence of loss, the NISPOM states that each information assurance attribute be assigned a level of concern:

- High
- Medium
- Basic

Information Sensitivity Matrices

The level of concern (basic, medium, and high) for each information assurance attribute (confidentiality, integrity and availability) is uniquely defined in the NISPOM Information Sensitivity Matrices.

Note: For confidentiality, the levels of concern translate to classification levels of Confidential (Basic), Secret (Medium) and Top Secret (High).

Level of Concern Considerations

When using the information sensitivity matrices to determine a level of concern, the following should be considered:

- The level of concern does not have to be the same for all system attributes.
- When multiple applications on a system result in different levels of concern for each attribute, the highest level of concern for each category shall be used.

Topic 2: Introduction to Protection Levels

In the previous topic, you learned about the three attributes of information assurance (confidentiality, integrity, and availability) and their associated levels of concern.

In this topic, you will learn about how the levels of concern are used with other factors to determine the NISPOM required protection level for confidentiality in a specific information system.

Reference: NISPOM paragraph 8-402

Protection Level

For the Confidentiality information assurance attribute, the NISPOM specifies that an information system must operate in one of four Protection Levels (PL): PL-1, PL-2, PL-3, or PL-4. The appropriate IS protection level is determined by the relationship between two parameters:

1. The clearance levels, formal access approvals, and need-to-know of users, and
2. Level of concern[13] based on the classification of the data on a particular system

Protection Level 1

Systems are operating at Protection Level 1 when all users must have:

1. Personnel Clearance for ALL information on the IS

2. Formal access approvals[14] for all information on IS (if applicable)

3. Need-to-know for all information on the IS

Protection Level 2

Systems are operating at Protection Level 2 when all users have:

1. Personnel Clearance for ALL information on the IS,

2. All required formal access approvals if applicable, but

3. At least one user lacks the need-to-know for some of the information on the system

Protection Level 3

Systems are operating at Protection Level 3 when all users have:

1. Personnel Clearance to the highest level of information on the IS, but

2. At least one user lacks formal access approval for some of the information on the system

Protection Level 4

Systems are operating at Protection Level 4 when all users have:

1. A Personnel Clearance, but

2. At least one user lacks the personnel clearance for all levels of classified information on the IS. In a PL 4, the lowest clearance allowable is Confidential and the varying clearance levels must be adjacent e.g., Secret and Top Secret or Confidential and Secret. In other words, an individual cleared only to the Confidential level cannot become a user on a PL 4 IS that processes up to Top Secret information.

Determining Protection Requirements

Once the required IS Protection Level is determined, NISPOM translates the PL into a set of requirements that must be implemented in the resulting system. NISPOM outlines the IS requirements in a Protection Profile[15] table.

The specific NISPOM requirements for the listed protection measures are identified in parenthesis for Protection Level 1, identified as Audit 1 are found in NISPOM paragraph 8-602.

Note: Protection profile requirements for Confidentiality are mandated by the NISPOM. The protection profile requirements for operational Integrity and Availability are implemented by the contractor only if they are contractually mandated. Be sure to review the contract documents, to include the DD 254, to see if these additional requirements are included.

Lesson Summary

In this lesson you learned:

- The attributes of information assurance

  The three attributes of information assurance are: confidentiality, integrity, and availability. Each attribute is assigned a level of concern (basic, medium, or high). The level of concern for each attribute is defined in the NISPOM Information Sensitivity Matrices.

- The factors that determine Protection Levels

  An information system must operate at one of four Protection Levels (PL 1 – 4). The protection level is determined by the relationship between two parameters:

  1. The clearance levels, formal access approvals, and need-to-know of users, and
  2. Classification of the data on a particular system

Lesson 2: Introduction to Information System Security Documentation

Before the formal certification and accreditation process can begin, you must prepare all required system security documentation. This is to ensure that the IS to be accredited is appropriately documented and that all required security measures and procedures have been identified.

You will learn about the documentation requirements for IS certification and accreditation as well as the protection requirements common to all accredited IS.

Reference: NISPOM paragraphs 8-101b, 8-202b, Chapter 8, Section 3, and 8-610

Lesson Objectives

After completing this lesson, you will be able to:

- Identify required information system (IS) security documentation
- Identify protection requirements common to all accredited IS

Topic 1: Introduction to Information System Security Documentation

Before classified processing can begin, you must prepare all required system security documentation. This documentation, which describes all aspects of the IS as well as the protection measures and processes required to protect it, is submitted to DSS and maintained on site once accreditation has been received.

In this topic, Information System Security Documentation, you will learn about the security documentation requirements for IS certification and accreditation.

Reference: NISPOM paragraphs 8-101b, 8-311 and 8-610

IS Security Documentation

When requesting accreditation, the Information System Security Manager (ISSM) must prepare and submit all required documentation. Chapter 8 of the NISPOM identifies required security documentation

as follows:

- IS Security Policy
- Configuration Management (CM) Plan
- System Security Plan (SSP)
- Certification and Accreditation Documentation

The following screens provide additional information about the security documents listed above.

IS Security Policy

One of the first documents required for certification and accreditation is an IS security policy. Chapter 8 of the NISPOM requires that contractor management publish and promulgate a security policy.

What is a security policy?

A security policy is a formal statement of the rules that users who are given access to an organization's technology and information assets must follow. The policy communicates the organization's security goals to all of the users, administrators, and managers.

What is its purpose?

The purpose of a security policy is to address the contractor's security procedures for holding and processing classified materials. It also serves to inform users, administrators and managers of their obligation to protect technology and information assets and demonstrates management's support of all identified procedures. To be effective, the policy needs to have the acceptance and support of all levels of employees within the organization.

A good security policy must:

- Be able to be implemented through system administration procedure, publishing of acceptable use guidelines, or other appropriate methods
- Be able to be enforced with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible
- Clearly define the areas of responsibility for the users, the administrators and the managers
- Be communicated to all once it is established
- Be flexible to the changing environment of a computer network since it is a living document

The IS Security Policy can be included in the SSP if the contractor so chooses.

Configuration Management Plan

The Chapter 8 of the NISPOM requires that the ISSM develop and implement a Configuration Management (CM) Plan. The CM plan documents procedures for identifying, controlling, accounting for and auditing system hardware, software, communication interfaces, operating procedures and installation instructions. The CM document must contain the following information:

- Type, model and brand of IS hardware that has the capability to retain information (e.g., CPUs, printer, memory keyboards, external drives, scanners, copiers, reproduction equipment, test equipment, communications devices, digital cameras and any other new technology not previously mentioned that are part of the accredited system). A unique hardware identifier may be needed to distinguish between two systems of the same manufacturer and model number (i.e., serial numbers or property numbers).

- Physical location

The SSP must have a CM section describing how the accredited IS protection features are implemented and maintained.

Other information that a CM document must contain includes:

- Security-relevant software product names and versions/release numbers. Avoid installing software which will not be utilized for classified processing on the system (e.g., infrared device drivers).

- System connectivity (including any software used for communication, including wireless communication).

- Connection sensitivity. The classification level of each connection or port controlled by the Security Support Structure (SSS) shall be documented. The SSS is the hardware, software and firmware required to adjudicate security policy and implementation differences among IS components and networks.

Additionally, the CM program will indicate that DSS must be notified before any security-relevant changes are implemented so that a reaccreditation decision can be made.

The Configuration Management Plan must also include the following:

- Formal change control procedures

  Formal change control procedures ensure that any security-relevant hardware or software is reviewed and approved before installation or removal from the accredited system.

- Procedures for management of all documentation

  Procedures for management of all documentation include documentation such as the SSP and security test plans. These processes and procedures must be periodically tested and verified to ensure the CM program is working effectively. Changes outside the approved process are technically or procedurally NOT allowed.

- Procedures for testing and verification of the CM Plan

  Certification testing involves verification of the correct operation of protection measures. It is performed and documented by the ISSM or ISSO. The plan outlines the inspection and test procedures and is conducted as part of the certification/validation process.

CM procedures need to be designed so that the identity of the IS can be recognized and recreated at any time.

System Security Plan

The System Security Plan (SSP) is an important part of the required security documentation. It is the basic system protection document and provides evidence that the proposed system (or update to an existing system) meets the protection profile requirements. It provides users with instructions on how to process classified information. It also serves as the basis for certification and inspection of the system. On the DSS web site, the Office of Designated Approving Authority has a suggested SSP format, which will ensure all aspects are covered.

The SSP:

- Indicates how you as the ISSM will implement your security policy
- Serves as a user's Instruction Guide
- Serves as an Inspection Guide

An SSP Checklist is available as a tool to help prepare an SSP by ensuring all applicable items are addressed.

The SSP Addresses

The SSP must address:

- System Identification
- System Requirements
- Protection Measures

System Identification

System Identification must include the following:

- Security Personnel: Names, locations, and phone numbers of the ISSM and (if applicable) the Information System Security Officer (ISSO)
- System Description: A brief narrative of the mission or purpose of the system and the architecture of the IS, including sub-networks, communications devices and protocols

A block diagram of the components that shows the interconnections between the components (as well as to other systems) and an information flow diagram should be included.

System Requirements

System requirements must include:

- Classification level(s) (Confidential, Secret, and Top Secret), personnel security clearance levels, need-to know and formal access approval requirements of Users
- Protection Level (1-4)

Protection Measures

The SSP includes information about the specific protection measures you as the ISSM plan to implement. The SSP must address:

- The protection measures that are identified for the Protection Level of the IS.

Protection measures for PL-1 as identified by Table 5, include:

Table 5 - Protection Profile Table for Confidentiality			
Requirements (NISPOM Paragraph)	Confidentiality Protection Level		
	PL1	PL2	PL3
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3 & 4
Data Transmission (8-605)	Trans 1	Trans 1	Trans 1
Access Controls (8-606)	Access 1	Access 2	Access 3
Identification & Authentication (8-607)	I&A 1	I&A 2, 3, 4	I&A 2, 4, 5
Resource Control (8-608)	–	ResrcCtrl 1	ResrcCtrl 1
Session Controls (8-609)	SessCtrl 1	SessCtrl 2	SessCtrl 2
Security Documentation (8-610)	Doc 1	Doc 1	Doc 1
Separation of Functions (8-611)	–	–	Separation
System Recovery (8-612)	SR 1	SR 1	SR 1
System Assurance (8-613)	SysAssur 1	SysAssur 1	SysAssur 2
Security Testing (8-614)	Test 1	Test 2	Test 3

Variances and Vulnerabilities

Variance

A variance is required if a protection measure requirement can be met, but in a different way. If a variance exists, the SSP must provide a description of the approved variance and the approval documentation must be attached to the SSP.

Unique Threat or Vulnerability

The SSP must address any unique threat[16] or vulnerability[17] to the system. If no threat or vulnerability exists, the SSP must state that fact.

Additional Items

The NISPOM requires the contractor to address additional procedures; however, 8-610a does not require they be included in the SSP. Since the DAA must ensure these procedures are adequate as part of the certification and accreditation process, it is recommended they be included in the SSP. If not, they must either be forwarded with the SSP. These additional procedures include:

- Trusted Downloading,[18] if applicable
- Common Requirements (addressed further in 4.3)
- Self-Inspections procedures
- Education and training of users

SSP Might Also Include

An SSP might also include a Memorandum of Understanding (MOU). An MOU is required when the system is connected to an IS accredited by a DAA other than DSS (e.g., Army, Navy, DOE, etc.). An MOU between DSS and another Government DAA is required for all government to contractor connections.

C&A Documentation

Certification and Accreditation (C&A) documentation includes:

- Security test plans, procedures and reports.
- A Certification statement - prepared by the ISSM certifying that the system performs as documented in the SSP. This statement must be submitted to DSS.
- An Accreditation Request - written by the contractor, requesting accreditation of the IS. This request must be submitted to DSS.

Depending on the Protection Level, the requirements for C&A documentation range from a simple statement that the system complies with the stated requirements at PL-1 to detailed security test plans, procedures and reports.

Accreditation Documentation

When a system is accredited, the contractor receives an accreditation letter issued by the RDAA/DAA. This Accreditation letter, along with a copy of all other documentation, must be maintained by the ISSM.

Topic 2: Introduction to Common Requirements

In the previous topic, you learned about IS security documentation requirements for IS certification and accreditation.

In this topic, Common Requirements, you will learn about the requirements that are common to all accredited IS.

Reference: NISPOM Chapter 8, Section 3

Common Requirements

No two information systems are completely identical. The specific security documentation required for an IS must reflect the unique environment of that particular IS. However, there are certain general requirements that all certifications must address. The NISPOM provides guidance about the type of information to include in the SSP or other IS security documentation.

As a minimum, the following elements must be addressed:

Common Requirements				
Personnel Security	Malicious Code	Physical Security	Identification and Authentication	Review of Printed Output
Maintenance	Examination of HW & SW	Clearing and Sanitizing	Marking Hardware, Output and Media	Protection and Review of Media

Personnel Security

Personnel who access the IS play an integral role in protecting classified information.

- Specify in writing the duties, responsibilities, privileges and specific limitation of IS users, both general and privileged .

Malicious Code

Malicious code and viruses are a concern to all IS.

The SSP must:

- Identify security features implemented to detect malicious code, viruses and intruders (hackers), as appropriate. Prior to introduction all software must be checked for viruses and other malicious code as possible. Incidents of malicious code, viruses or intruders are to be reported to DSS.

Physical Security

Access Controls (included in Table 5) require denial of physical access by unauthorized individuals; therefore, classified information must be physically secured at all times.

IS Documentation must:

- Establish what safeguards will be used to prevent or detect unauthorized modification of the IS; hardware and software;

- Maintain at all times the hardware integrity of the IS, including remote equipment, even when all classified information has been removed from the IS;

• Describe the area where classified processing will occur. (The designated area must meet NISP requirements for secure processing of classified information)

Table 5 - Protection Profile Table for Confidentiality			
Requirements (NISPOM Paragraph)	Confidentiality Protection Level		
	PL1	PL2	PL3
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3 & 4
Data Transmission (8-605)	Trans 1	Trans 1	Trans 1
Access Controls (8-606)	Access 1	Access 2	Access 3
Identification & Authentication (8-607)	I&A 1	I&A 2, 3, 4	I&A 2, 4, 5
Resource Control (8-608)	–	ResrcCtrl 1	ResrcCtrl 1
Session Controls (8-609)	SessCtrl 1	SessCtrl 2	SessCtrl 2
Security Documentation (8-610)	Doc 1	Doc 1	Doc 1
Separation of Functions (8-611)	–	–	Separation
System Recovery (8-612)	SR 1	SR 1	SR 1
System Assurance (8-613)	SysAssur 1	SysAssur 1	SysAssur 2
Security Testing (8-614)	Test 1	Test 2	Test 3

8-606. Access Controls (Access). The IS shall store and preserve the integrity of the sensitivity of all information internal to the IS.

a. Access 1 Requirements.

1. Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

b. Access 2 Requirements. In addition to Access 1:

1. Discretionary access controls shall be provided. A system has implemented discretionary access controls when the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The discretionary access control policy includes administrative procedures to support the policy and its mechanisms.

c. Access 3 Requirements. In addition to Access 2:

1. Some process or mechanism that allows users (or processes acting on their behalf) to determine the formal access approvals granted to another user.

2. Some process or mechanism that allows users (or processes acting on their behalf) to determine the sensitivity level of data.

IS documentation must also:

• Indicate how equipment that visually displays classified information will be positioned to prevent unauthorized disclosure;

• Indicate what procedures will be used to ensure that all personnel granted unescorted access to the area containing the IS have an appropriate security clearance and need-to-know, and that all uncleared personnel are escorted and appropriately supervised.

It is required that physical security safeguards are documented in the SSP.

Identification and Authentication Management

Identification and authentication controls (included in Table 5), are required to ensure that users have the appropriate clearances and need-to-know for the classified information they will access.

The SSP must:

• Identify I & A procedures and indicate how they will be managed

Note: Technical I & A, such as passwords and user IDs, are not always required. In certain circumstances manual procedures are acceptable.

Table 5 - Protection Profile Table for Confidentiality			
Requirements (NISPOM Paragraph)	Confidentiality Protection Level		
	PL1	PL2	PL3
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3 & 4
Data Transmission (8-605)	Trans 1	Trans 1	Trans 1
Access Controls (8-606)	Access 1	Access 2	Access 3
Identification & Authentication (8-607)	I&A 1	I&A 2, 3, 4	I&A 2, 4, 5
Resource Control (8-608)	–	ResrcCtrl 1	ResrcCtrl 1
Session Controls (8-609)	SessCtrl 1	SessCtrl 2	SessCtrl 2
Security Documentation (8-610)	Doc 1	Doc 1	Doc 1
Separation of Functions (8-611)	–	–	Separation
System Recovery (8-612)	SR 1	SR 1	SR 1
System Assurance (8-613)	SysAssur 1	SysAssur 1	SysAssur 2
Security Testing (8-614)	Test 1	Test 2	Test 3

Review of Printed Output

Appropriate classification reviews on human-readable output (e.g., paper, fiche, film) can be performed without the aid of an approved procedure and/or method. The material must be protected at the level of

the IS until it has been reviewed. The individual responsible for the review must be trained by the ISSM/ISSO on applying accurate classification markings after the review.

Maintenance

ISs are particularly vulnerable to security threats during maintenance activities. The level of risk is dependent on the nature of the maintenance person's duties, the security awareness of the employees and the maintenance person's access to classified information and facilities.

Procedures to identify the following must be established:

- How the clearances and need-to-know of maintenance personnel will be monitored
- How the use of cleared and/or uncleared/lower cleared maintenance personnel is managed

Examination of Hardware and Software

Hardware and software need to be examined to ensure they are in good working order and that they do not have any elements that could have an adverse effect on the secure operations of the system.

Procedures must indicate that all IS hardware and software will be examined when received from the vendor and before being placed into classified use. Hardware that leaves the protected area must be reexamined prior to reentry.

Clearing and Sanitization

Instructions on clearing, sanitization and release of IS media are published by DSS. A complete and current Clearing and Sanitization Matrix can be found on the DSS web site. The Matrix provides the procedures to be followed and documented in the SSP (as applicable).

Procedures in the IS documentation must indicate how the requirements of the Matrix will be applied.

Marking Hardware, Output and Media

Markings on hardware, output and media must conform to the NISPOM, Chapter 4. If the required marking is impractical or interferes with the operation of the media, DSS may approve alternate marking procedures.

Procedures must indicate that all hardware, output and media will be marked in accordance with the guidance provided in the NISPOM, Chapter 4.

Protection and Review of Media

Media refers to all materials that hold data in any form or that allow data to pass through them including:

- Hard, floppy and optical disks
- Magnetic tape , USB memory, memory cards

Procedures for protecting and reviewing media must include the following information:

- A description of how removable media is protected and that it will be marked with visible, human-readable, external markings to the accreditation level of the IS unless an approved classification review has been conducted.
- An indication that classification reviews are in accordance with DSS approved standards and will be conducted before the media is released outside the security perimeter.
- An indication that all media will be accurately marked with the appropriate classification and applicable associated security markings.

Lesson Summary

In this lesson, you learned about the following:

- IS Security Documentation

  In this topic, you learned about four types of security documentation that are required when requesting certification and accreditation:

  IS Security Policy

  Configuration Management Plan

  System Security Plan

  Certification and Accreditation Documentation

- Common Requirements

  In this topic, you learned about the requirements that are common to all accredited IS. You learned about the specific elements that must be addressed in the System Security Plan. You also learned about the procedures that must be followed and documented in the SSP for each of the elements.

Lesson 3: Introduction to Certification and Accreditation

Certification and Accreditation (C&A) is a team effort between Government and industry. Defense Security Service (DSS) works together with you to ensure that you and your company understand and adhere to the requirements established by the National Industrial Security Policy (NISP).

You will learn about the Certification and Accreditation process.

Reference: NISPOM Chapter 8 Section 2, 8-504, 8-614a

Lesson Objectives

After completing this lesson, you will be able to:

- Identify the Certification process

- Identify the Accreditation process
- Identify the Master System Security Plan (SSP) process

Topic 1: Identify the System Security Plan (SSP) process

The Certification process establishes the extent to which a particular Information System (IS) meets the security requirements of the NISPOM. During the process all factors relating to the security of your information system must be identified, documented, tested, and reviewed. Factors such as the IS's unique environment, proposed protection level, user's clearance level and access authority, data classification and sensitivity, configuration, facility location and outside connectivity must be considered.

In this topic, The Certification Process, you will learn to recognize the IS Certification process.

Reference: NISPOM 8-201

Certification Process

After all required security documentation has been prepared, the Information System Security Manager (ISSM) is ready to begin the Certification process. This process requires the ISSM/contractor personnel to develop and implement an IS certification test plan.

Plan and Implement Certification Testing

The SSP (and other IS security documentation as necessary) serve to document the IS and the protection measures designed to protect classified information. The first step in the C&A process requires the ISSM to conduct certification testing to ensure that the protection measures have been tested and found to operate as identified in the SSP, prior to submitting it to DSS.

Certification Testing

Certification testing:

- Involves verification that protection measures operate correctly
- Is performed and documented by the ISSM/Information System Security Officer (ISSO)

The extent of the testing and testing documentation required will depend upon the size and complexity of the system to be accredited, and the protection level under which the system will operate.

PL-1 Test Requirements

The following Test 1 requirements must be met for certification at PL-1.

Operational assurance must be documented in the SSP for:

- Security features
- Access controls
- Configuration management

A statement from the ISSM certifying that the IS identified in the SSP has the appropriate protection measures in place and provides the intended protection, is sufficient for PL-1 systems. This statement must be submitted to DSS.

Topic 2: Introduction to the Accreditation Process

In the previous topic, you learned about the IS Certification process.

In this topic, you will learn about the IS Accreditation process.

Reference: NISPOM 8-202 a-f, 8-504, 8-614a

What Requires Accreditation?

An IS processing classified must be accredited if it has storage media or programmable or writeable non-volatile memory. This includes all personal computers, as they utilize media, and test equipment with non-volatile memory.

The Accreditation Process

The formal Accreditation process is a five-step process that involves the following actions:

The ISSM:

- Step 1: Prepare a certification statement
- Step 2: Submit required IS documentation

The DSS:

- Step 3: Reviews the SSP (and other IS security documentation as necessary)
- Step 4: Certifies the SSP (and other IS security documentation as necessary)
- Step 5: Accredits the IS

Step 1: Prepare a Certification Statement

Once the required security documentation has been prepared and certification testing has been completed, the ISSM is ready to begin the formal C&A process.

This process begins when the ISSM certifies in writing that the system, as identified in the System Security Plan (and other IS security documentation as necessary) has the specified security controls in place, properly tested and is functioning as described.

Step 2: Submit Required IS Documentation

The next step is to prepare and submit to DSS a formal request for accreditation. The contractor must submit a written request to the ODAA and all required IS security documentation. This includes the following:

- The IS Policy (recommend included in the SSP)
- The Configuration Management Plan (included in the SSP)
- The System Security Plan (and other IS security documentation as necessary)
- Certification and Accreditation Documentation
  - A Certification Statement (can be included in the SSP)
  - A formal Accreditation Request

Step 3: DSS Reviews the IS Documentation

The next step of the process is for DSS to review and evaluate the documentation. The ODAA or their representative will conduct a thorough review of the SSP (and other IS security documentation as necessary). This may include an on-site review to validate the ISSM's certification.

If there are any questions or concerns, the contractor must address them and make corrections/changes as requested.

Step 4: DSS Certifies the IS Documentation

Once all questions and concerns have been addressed, the IS Rep and/or the ISSP certifies the system to the Designated Approving/Accrediting Authority (DAA).

Step 5: DSS Accredits the IS

Accreditation is an administrative action and is the formal approval for a system to process classified information.

Once DSS receives the formal request and related documentation, all technical and non-technical security features, safeguards and procedures are evaluated against the NISPOM requirements. Obviously, the more complete and accurate the SSP, the quicker the accreditation can occur.

If the request for accreditation is approved, the RDAA/DAA (DSS for most contractor systems) will issue an Accreditation letter. Once that letter is received, classified processing can begin. All approvals must be in writing; there are no verbal approvals authorized.

The DAA will retain a copy of the letter and all certification documentation for the duration of the accreditation.

Interim Approval to Operate (IATO)

The ODAA may grant the contractor interim approval to operate for as many as 180 days. Interim approvals must be in writing, specify the interim period and, if necessary, identify what minimum protection measures are required. At the end of the specified period, the ODAA may extend the interim approval for up to an additional 180 day period. Interim approvals that last up to 360 days should be rare.

Reaccreditation

The SSP must be reaccredited whenever security relevant changes are made to the accredited IS. Proposed modifications to an IS must be reviewed by the ISSM to determine if the proposed modifications will impact the security protections on the system.

During the reaccreditation cycle, DSS may grant an interim approval to operate the system.

The Reaccreditation Process

The reaccreditation process is similar to the accreditation process. The ISSM must send in the revised SSP with the proposed changes, and then DSS reviews the documentation. The ISSM may not make any changes to an accredited system until DSS has issued an Interim Approval to Operate (IATO). Once the ISSM has the IATO, he or she will make the changes, then notify the IS Rep that changes are complete. At this point, the written certification statement indicating the security controls are in place, tested and functioning is submitted to DSS, for reaccreditation.

An updated SSP is only required if there were changes to the one submitted at the beginning of the reaccreditation process.

Examples of Security Relevant Changes

Examples of security relevant changes that require reaccreditation include:

- The addition or replacement of any system to the accredited IS (however, a contractor may replace a system of the same make and model as a maintenance action)
- The addition of any equipment having a type of non-volatile memory, not previously accredited
- Change or addition of a sanitization software package not previously accredited for the system
- The addition of a secure telephone device (e.g., STU-III, STE) Secure Data Device (SDD) or network connection to another contractor or government site, or wireless devices
- A change in the operating system software (e.g., changing from Windows to Unix or Linux)
- Addition of Protected Distribution Systems
- Changes that warrant a higher Protection Level

Examples of security-relevant changes that may require reaccreditation include:

- A change in automated audit trails or identification and authentication
- A change in virus protection software (adding periodic updates or changing commonly utilized software, e.g. Norton to McAfee, does not require reaccreditation)
- Change in NSA Type 1 Encryption Device[19]
- Relocating a system, particularly if physical security is changed (Closed Area to Restricted)
- Installation or removal of third party security software

Re-Evaluation

Each IS must be evaluated for reaccreditation every 3 years. The ISSM must certify that all security features, etc. remain the same as when originally accredited. If not, the SSP must be updated and reaccredited. If there are no changes, the ISSM must notify the ODAA by email, with a copy to the ISR, Field Office Chief and ISSP. It is the ISSM's responsibility to maintain records as to when the re-evaluations are due. Upon receipt of the ISSM's certification that no changes occurred, the ODAA will analyze the current threat and any new policy changes against those of the original accreditation. If valid, the ODAA will annotate original accreditation letter (or send new letter) with date of re-evaluation.

Withdrawal of Accreditation

The DAA will evaluate the risks and consider withdrawal of accreditation if the system is no longer needed, if protection measures approved for the system are ineffective, or if changes to the IS or security configuration have been made.

Examples of such changes may include: the ISSM's technical knowledge or ability is no longer equal to the complexity of the information system and no technically knowledgeable ISSO is available, changes in protection levels, changes in technical or non-technical protection measures, new or increased vulnerabilities, change in operational environment, or interconnections.

Interim Approval May Be Granted

If there is no potential threat to the classified information, the IS Rep or ISSP may recommend to the DAA that the company be allowed to continue to process on an interim basis with no disruption to the processing, even though a withdrawal has been issued. The resubmission of the SSP will be processed as a reaccreditation.

The DAA may withdraw accreditation if the system is no longer required to process classified, or if the operational need for the system no longer outweighs the risk of operating the system (i.e., the IS has not been used to process classified information in the past 180 days). If the accreditation is withdrawn, the IS Rep or ISSP, will ensure proper sanitization of memory and media occurred.

Invalidation of Accreditation

Invalidation occurs when there is a potential compromise to classified information (e.g., when a classified system is connected to an unclassified system) or when a compromise has occurred. Invalidation requires immediate termination of classified processing. Should this occur, the IS Rep/ISSP will notify the contractor to terminate the classified processing immediately and conduct an administrative inquiry (see NISPOM paragraph 1-303, and Module 6 for more information on conducting administrative inquiries).

The DAA will determine on a case-by-case basis how long the system must be invalidated and what corrective action must be taken before allowing the contractor to begin processing. The DAA will send a letter reflecting the invalidation and the circumstances that led to the invalidation to the contractor.

Special Purpose Type Systems

Tactical, embedded, data-acquisition and special purpose systems encompass an array of information systems. These information systems can range from relatively compact subsystems (such as missile guidance sets) that have no users and perform a very limited set of predetermined functions, to much larger and complex systems such as a submarine, ship or aircraft. NISPOM 8-504 requires these types of systems be accredited; however, they are not required to meet the security requirements specified for

more general-purpose systems.

Security requirements for information systems that are embedded as an integral element of a larger system that is used to perform or control a function, such as control systems or weapons systems, should be established by the Government Contracting Activity (GCA) concurrently with the design and development of the system. If the GCA has not provided those requirements, the contractor shall request them from the GCA. Regardless of the existence of guidance from the GCA, these systems will not require CSA accreditation. However, if the GCA security requirements are not provided, the contractor will be required to submit classified processing procedures to the DSS that describe the security requirements and procedures implemented that protect the embedded system and classified information against unauthorized disclosure or loss.

Tactical, embedded, data acquisition and special purpose systems
These types of systems are essentially government systems, specifically designed for delivery and use in government controlled or tactical environments. Examples of these types of systems range from components such as guidance sets for command and control systems, to entire weapon platforms such as missile systems, tanks and submarines. These would also include prototypes of the systems that would remain under custody of the contractor.

Topic 3: Introduction to Master System Security Plan

In the previous topic, you learned about the Accreditation process for a single IS.

In this topic, Master System Security Plan (SSP), you will learn about the Master SSP, the process that is used when a contractor wants to self-certify[20] additional systems.

Reference: NISPOM 8-202g

Master System Security Plan

The NISPOM permits contractors who desire self-certification and have multiple PL-1 or PL-2 systems to be identified and accredited under the Master SSP approach. Additionally, the IS configurations must be essentially the same and the physical security protection for all IS must be similar. Separate Profiles will be created for various configurations as part of the Master SSP.

A Master SSP can address only <u>similar</u> ISs that operate in equivalent operational environments (e.g, the levels of concern and protection level are the same, the users have at least the required clearances and access approvals for all information on the IS, and the IS configurations are essentially the same).

Similar
Similar is defined as the same operating system(s). Similar is also defined as hardware that contains no components that require additional clearing, sanitization or disconnect procedures other than those described in the Master SSP.

If the contractor desires to self-certify additional operating systems other than one(s) listed in the accreditation letter, or if the system requires reaccreditation for any other reason, an interim approval to make the change to the IS is required from DSS. The contractor must submit a request for a change along with an updated Master SSP reflecting the new operating system and any additional changes. If approved, DSS will issue an interim approval to operate (IATO). Once the IATO is received, the ISSM can implement the changes.

A Master SSP can be written to allow the contractor to add additional standalone workstations under a

Master Plan for single-user standalone systems. Under a Master Plan for multi-user systems, the contractor can add workstations to an accredited network, create additional networks within the facility and/or add multi-user standalone workstations. The added hardware must be similar and operate in an equivalent operational environment.

Replacing workstations of the same make and model is permitted without self-certification and is considered a maintenance action.

Each contractor's facility is responsible for producing its own Master SSP. A Multiple Facility Organization (MFO) may not develop one Master SSP covering all locations. Self-certification is only authorized for systems that will process classified information within the local facility.

A Master SSP may be submitted for a Local Area Network (LAN) connected to a Wide Area Network (WAN) to allow the ISSM to self-certify additional workstations. However, the Master SSP must state that self-certification is limited to systems processing classified within the local site (CAGE Code) only. Under no circumstances will remote site connections be self-certified.

Equivalent Operational Environments

The NISPOM, paragraph 8-202g also discusses equivalent operational environments. This includes the entire environment in which the system operates, e.g., the operating system(s) used, access controls and physical security controls.

Separate MSSP’s will be required for similar systems operating in a closed area environment as opposed to a restricted area environment. One MSSP cannot be written to include systems in both restricted and closed area environments.

Self-Certification

Self-Certification is granted to an individual (ISSM), rather than a facility. The ISSM who will have self-certification authority will be identified by name in the Master SSP. DSS will determine if the ISSM is trained to a level commensurate with the complexity of the facility's IS and is qualified to perform self-certification. The ISSM must be deemed competent and reliable by DSS. Competency includes knowledge of both NISPOM requirements and IS technical features of the facility's accredited systems or appointment of a knowledgeable ISSO if those features exceed the capability of the ISSM. An ISSM would be considered reliable if he or she has established credibility with DSS in fulfilling requirements of the NISPOM.

During the certification process, DSS will ensure the ISSM named for self-certification understands the duties and responsibilities of the position. An alternate ISSM may also be appointed. This individual must also meet ISSM training, competency and reliability criteria and must be named in the Master SSP.

If the ISSM terminates the position, a letter advising of the change is acceptable if there are no other changes to the Master SSP. Otherwise, a new Master SSP with his or her name included is required. The new ISSM must meet criteria as previously outlined. In the interim period between outgoing and incoming ISSM's, if an alternate ISSM was not appointed, the contractor no longer has self-certification. However, the ISSM may continue to replace systems of the same make and model under maintenance actions.

Required Information

The SSP must contain detailed certification procedures as follows:

In addition to a description of the system, the Master SSP will discuss the extent of the contractor's self-certification authority. This authority would include adding workstations to an existing network, self-certifying similar networks within the local facility or self-certifying additional standalone workstations, for example.

The Master SSP must also include a requirement that DSS will be notified when a system has been self-certified. The ISSM or ISSO will perform certification testing of the similar system to ensure that systems have all automated auditing, identification and authentication and other technical features enabled. In addition, the contractor must have a written test procedure to ensure consistency in certifying additional systems.

The ISSM must submit an IS Certification Report to the IS Rep for each IS that he or she certifies. That report will contain, as a minimum, the system identification and location, and certification that the IS implements the requirements in the Master SSP. The ISSM must retain a copy of the report with the approved copy of the Master SSP.

Report Format

The format the contractor utilizes for the report and how often the IS Rep is notified will depend upon the situation and the preferences of the IS Rep and ISSM. For large companies, the ISSM and the IS Rep must concur whether the ISSM will submit a report on a weekly, biweekly or not less than monthly basis. The schedule for submission of reports must be in the Master SSP.

As in all SSPs, the ISSM must certify in writing that the IS(s) identified in the Master SSP, has appropriate protection measures in place and that all ISs provide the intended protection. If the ISSO is actually performing the testing, the ISSM will ensure that all work has been performed.

DSS must accredit the first of each Profile under the Master SSP. All other IS to be operated under the Master SSP shall be certified by the ISSM as meeting the conditions of the approved Master SSP Profile. This certification allows for the individual IS to operate under the Master SSP.

Recertification

IS certified under a Master SSP remain certified until the Master SSP is changed or three years have elapsed since the IS was certified and accredited. If the protection level described in the Master SSP change or any other changes requiring reaccreditation occur, the Master SSP must be reaccredited by DSS and all IS certified under the Master SSP must be recertified by the ISSM in coordination with DSS.

Lesson Summary

In this lesson, you learned about the following:

- The Certification Process

  In this topic, you learned how to recognize the Information System (IS) Certification process. You learned that the first step in the Certification and Accreditation (C&A) process requires the Information System Security Manager (ISSM) to conduct certification testing to ensure that the protection measures have been tested and found to operate as identified in the Systems Security Plan (SSP). The certification process requires the Information System Security Manager (ISSM)/contractor personnel to develop and implement an IS certification test plan. You also learned that the certification testing involves verification that protection measures operate correctly and the testing is performed and documented by the ISSM or the Information System

Security Officer (ISSO).

- The Accreditation Process

  In this topic, you learned about the IS Accreditation process. An IS processing classified must be accredited if it has storage media or programmable or writeable non-volatile memory including, personal computers and peripheral devices with media or non-volatile memory. You learned that the accreditation process is a five-step process. You learned about the reaccreditation process and that it is similar to the accreditation process. You also learned that there are specific security-relevant changes that may require reaccreditation.

- Master System Security Plan

  In this topic, you learned about the Master System Security Plan (SSP) and the process that is used when a contractor wants to self-certify additional systems. You learned that the NISPOM permits contractors who desire self-certification and have multiple PL-1 or PL-2 systems to be identified and accredited under the Master SSP approach. You learned that self-certification is granted to an individual, the ISSM and alternate ISSM, if applicable, rather than a facility. You also learned that the information systems certified under a Master SSP remain certified until the Master SSP is changed or three years have elapsed since the IS was certified and accredited.

Module 4: Non-Technical Requirements

Lesson 1: Introduction to Physical Security and Maintenance

The information on an Information System (IS) is typically in one of three states or conditions: transmission, storage or processing. First, information exists while being passed from one entity to another. Second, information exists while being kept for the possibility of future need. And last, information exists while being processed, such as when a spreadsheet is calculating figures. Information needs protection in all three states and physical security is part of that protection.

The Information System Security Manager (ISSM) for an accredited IS must ensure that the system is physically protected against unauthorized access to the IS and unauthorized modification of the IS hardware and software.

You will learn about the requirements for physical security and maintenance operations, hardware and software when in use, when not being use, and during maintenance operations.

References: NISPOM, paragraph 8-304, 8-308, and 8-605, and NSTISSI 7003

Lesson Objectives

After completing this lesson, you will be able to:

- Identify appropriate physical controls required to protect classified IS processing
- Identify physical security requirements for an IS during attended and unattended processing sessions
- Identify procedures to preclude vulnerabilities during maintenance actions

Topic 1: Introduction to Physical Security Controls

Ensuring that adequate physical security controls are in place is an important part of the system security process. The number and types of physical security controls implemented will depend on the complexity of your IS and facility.

In this topic, Physical Security Controls, you will learn about the controls required to maintain physical security for an accredited system.

Reference: NISPOM, paragraph 8-308

Physical Protection

Physical protection ranges from simple seals to complex Closed Areas. The IS Rep will look at the depth or layers of physical security already in place when deciding what physical security controls are appropriate for the system being accredited.

During the Certification Process, the IS Rep will ensure that the contractor has implemented sufficient physical safeguards to prevent or detect unauthorized access or modification to the accredited IS hardware or software.

Physical Safeguards

Physical safeguards are required at all times, even when all classified information has been removed from the IS. The IS Rep can approve various physical security safeguards; however, these safeguards can never vary to the point that the users, ISSM, or Information System Security Officers (ISSOs) cannot detect tampering.

The approved physical safeguards are based on the assumption that the information system will remain within and under the protection of the physical safeguards of the facility. The only exceptions are for maintenance or if the accredited IS is approved to be used at another location or facility for contract-related processing. In those cases, procedures must be established which will address how the equipment, software and all classified information is transported and safeguarded.

Hardware Integrity

Continuous physical protection is required even when the IS is not in use. This includes times when all classified information is removed and secured, and all remaining memory or media has been cleared (for Confidential or Secret) or sanitized (for Top Secret). One or more of the following methods can be used to maintain the hardware integrity:

- Continuous supervision by authorized personnel
- Use of area controls that prevent or detect tampering or theft
- Use of approved cabinets, enclosures, seals, locks or Closed Areas

These physical security controls will vary depending on the depth of security at the contractor's facility and in the immediate area of the IS. Depth of Security is a determination that your company's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility.

When the IS is of an appropriate size, it can be safeguarded in a substandard container or an approved General Services Administration (GSA) security container. Supplemental protection to the substandard or GSA container may be required, depending on the classification level of the accredited IS.

Seal Requirements

One of the more popular options for safeguarding the IS, once classified information has been removed, is the use of authorized security seals. Security seals are inexpensive, easily used and can be adapted to work on most equipment.

Security seals are not locks. They are intended to detect tampering or unauthorized entry. However, security seals are vulnerable and should never be the only form of protection afforded the IS.

Security Seal Use

The IS Rep and the ISSM must evaluate each area where security seals will be used. It is conceivable that security seals could provide adequate protection in one area of the facility, but not in another. The IS Rep will periodically evaluate the depth of the facility's security in areas where accredited systems are protected by minimum measures.

If a security seal is found broken, the system must be examined for loose wires, foreign objects, and signs of tampering prior to continuing classified processing. If necessary, an administrative inquiry must be conducted to determine if classified information has been compromised (See NISPOM 1-303).

Note: You will learn more about administrative inquiries in the Administrative Inquiries lesson.

The DSS web site contains information about seal vendors and guidelines for the use of seals.

Other Options

Although seals are the most popular choice for meeting hardware integrity, there are other options. One of those options is the use of area controls. These controls will vary depending on the depth of security at your facility and in the immediate areas of the IS.

Depth of Security

Determining depth of security involves evaluating existing layers of security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include:

- Perimeter fences
- Visitor controls
- Intrusion detection systems
- Guard patrols
- Automated access controls systems
- Closed circuit TV

Topic 2: Introduction to Physical Security Requirements

In the previous topic, you learned about the controls required to maintain physical security of accredited IS equipment.

In this topic, you will learn about the physical security requirements for an IS during attended and unattended classified processing sessions.

Reference: NISPOM, paragraph 8-308

In Use Controls

When processing classified information on an accredited IS, users must prevent unauthorized disclosure by exercising constant surveillance and maintaining control of all equipment and components. This is accomplished through the use of supervision and area controls.

Therefore, classified processing must take place in an area where authorized contractor personnel can exercise constant surveillance and maintain control of the IS. The area must have an identifiable perimeter (e.g., walls, signs, tape on the floor, ropes, chains, etc.) to make it obvious that the area is restricted to authorized personnel only. A defined perimeter control area is also referred to as a "restricted area".

Attended Classified Processing Requirements

All personnel granted unescorted access to the defined perimeter area must have the appropriate clearance and need-to-know; otherwise, they must be escorted. The ISSM must brief escorts on their responsibilities and ensure that they have sufficient knowledge of the established security policies and procedures in the System Security Plan (SSP).

Visual Access

Visual access issues must also be considered. The ISSM must position devices that display or output information in human readable form to prevent unauthorized individuals from reading the information. Also, the ISSM should look around to see if other computers or devices in the area are equipped with cameras or microphones that could record classified information.

During both the certification and security review process, expect the IS Rep to evaluate whether visual access to the IS will make classified information obtainable by unauthorized individuals. The IS Rep will also review placement of the IS in relation to portable partitions, hallways, passageways and windows.

Unattended Classified Processing Requirements

The ISSM must also be aware of the following requirements for unattended processing:

A Closed Area is required when the IS processing classified information is unattended or when classified information remains on an unattended IS (e.g., on an internal, fixed hard drive).

Closed Areas protecting Secret and Top Secret information require supplemental protection.

Classified documents, which include media, printed materials, etc., are to be stored in approved security containers within the Closed Area unless the area has been approved by DSS for open shelf or bin storage. As an exception, large items essential to the operation of an IS do not need to be further secured

within the Closed Area.

Large Items

For example, this would include large removable hard drives, in-use magnetic tapes, technical manuals, etc. Following this guidance, limited classified materials (e.g. electronic media, printouts, etc) associated with unattended IS processing sessions need not be stored in security containers.

NISPOM 5-306. Closed Areas

Due to the size and nature of the classified material, or operational necessity, it may be necessary to construct Closed Areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed Areas must be approved by the Cognizant Security Agency and be constructed in accordance with Section 8 of this Chapter. Access to Closed Areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared employee or by a supplanting access control device or system. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persons without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. The Closed Area shall be accorded supplemental protection during non-working hours. During such hours, admittance to the area shall be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSA, will not require additional locking devices.

a. Open shelf or bin storage of classified documents in Closed Areas requires CSA approval. Only areas protected by an approved intrusion detection system will qualify for such approval.

b. The CSA and the contractor shall agree on the need to establish, and the extent of, Closed Areas prior to the award of the contract, when possible, or at such subsequent time as the need for such areas becomes apparent during performance on the contract.

Mobile Systems

Accredited systems that will occasionally relocate to other sites must be identified in the SSP along with written procedures. These procedures must address the date and place the mobile system will travel. The ISSM must notify DSS of the destination and departure and arrival times. DSS accreditation of mobile systems is valid only at those locations under DSS cognizance. The IS Rep will provide specific requirements. The requirements will vary depending on whether the system will be used at another contractor site or at a government site.

If the system is relocating to a government site, a copy of the DSS Accreditation letter and a letter prepared by the ISSM acknowledging relocation of the IS to the government site must be sent by the ISSM.

Remote Terminal Devices

A remote terminal or device is defined as equipment located outside the defined perimeter (or closed area) within the contractor facility, that is connected to the IS.

If remote terminal/devices are part of the accredited system, they must be under the same physical control as any other component of the system. This includes the transmission lines connecting the devices. These

lines must be inspected as well as properly protected. The protection of these unencrypted lines can be accomplished through a Protected Distribution System (PDS), or approved encryption.

If the remote terminal/devices are not used for classified processing, they must be disconnected from within the protected area of the central computer system.

Final Reminders

Review the DD 254

The ISSM should review the DD 254 for any additional physical security requirements imposed by the contract.

Report all compromises

If tampering is suspected or actually detected, a thorough investigation of the area and equipment must be conducted immediately. It is important to investigate all instances, regardless of how minor they may appear. The ISSM should report all compromises or suspected compromises to the IS Rep through the Facility Security Officer (FSO).

Topic 3: Introduction to Protected Distribution Systems (PDS)

In the previous topic, you learned about the physical security requirements for an IS during attended and unattended classified processing sessions.

In this topic, Protected Distribution Systems, you will learn about Protected Distribution Systems (PDSs) and the ways in which they are used within a facility.

Reference: NISPOM, paragraph 8-605, NSTISSI 7003

Protected Distribution Systems

A Protected Distribution System (PDS) involves the protection of wire or fiber optic lines that transmit unencrypted, classified information through areas of lesser classification or control.

PDS Guidelines

The guidelines for establishing a PDS are found in the National Security Telecommunications and Information Systems Security Instruction (NSTISSI 7003). This document can be accessed from the Committee on National Security Systems website at http://www.nstissc.gov.

The NSTISSI 7003 contains the baseline security requirements for PDSs. The requirements emphasize detection of penetration rather than prevention. The guidelines apply to all U.S. government departments, agencies, and their contractors. Approval to use a PDS must be obtained before installation occurs.

The document provides requirements for Low and Medium threat environments. The threat environment in the US is considered Low. Medium requirements apply to facilities located outside the US.

Terminology

Controlled Access Area (CAA) - an area that is controlled such that unauthorized persons are escorted or under some type of physical or electronic surveillance

- A Closed Area would always meet the requirements and, depending on the construction and controls in place, a Restricted Area could meet the CAA requirements.

Limited Control Area (LCA) - a space that is controlled by the facility and where anyone or anything that represents a threat can be removed

- For example, the space the contractor leases or owns and can control

Uncontrolled Access Area (UAA) - an area over which the facility has no way of controlling access by unauthorized persons

- For example, a facility that has offices on either side of a hallway in a multi tenant office building where the PDS needs to go from one side to the other

Installation and Maintenance Requirements

Requirements for the installation and maintenance of PDSs are as follows:

- Terminal equipment must be protected and should be installed in a Controlled Access Area.
- PDS lines should not be concealed (in walls or above ceilings) to allow for visual inspections or continuous surveillance.

  If the PDS is alarmed and does not require inspection or surveillance, this does not apply.
- Employees must be made aware of the PDS and report suspicious activity.
- Records should be kept of inspections, patrol results, alarms or employee reports.
- Uncleared persons who need occasional temporary access to the PDS must be escorted and monitored by cleared, technically briefed, and knowledgeable persons.

Additional installation and maintenance requirements are:

- Persons responsible for inspecting PDSs must be technically knowledgeable and able to recognize unauthorized, or even authorized, changes or alterations which could compromise the PDSs' integrity

  Taps, additions, breaks, etc.
- Tampering or penetration must be reported to DSS and use should cease until an investigation has determined the security impact

  Technical inspections, as discussed in Annex B paragraph 1.a.(6) and table B-3 in NSTISSI 7003, are not currently required by DSS

  Tempest/Red/Black requirements need not be imposed unless contractually required

Decision Matrix

The Decision Matrix for Carrier Inspection outlined in Table B-2 of NSTISSI 7003 states how often random inspections of the PDS are needed depending on the classification and type of area involved (LCA or UAA).

Types of PDS

There are two types of Protected Distribution Systems:

- Simple Distribution Systems
- Hardened Distribution Systems

Hardened Distribution Systems

A Hardened Distribution System may use one of three types of carriers:

- Hardened Carrier
- Alarmed Carrier
- Continually Viewed Carrier

Hardened Carrier

When a Hardened Carrier is used the following conditions must be met:

- The carrier must be made of metallic materials.
- All connections must be permanently sealed (welded, epoxied, etc.). Boxes not sealed must be secured with a GSA approved padlock. Boxes with pre-punched knockouts may not be used.
- If buried, the carrier must be 1 meter (approximately 39 inches) below the surface, and remain on the contractor's property. If manholes are used, they should be secured using a GSA approved padlock or alarmed.

Other conditions that must be met when using a hardened carrier are:

- Suspended systems between buildings should be elevated a minimum of 5 meters (approximately 17 feet) and used only if the property traversed is owned or leased by the contractor controlling the PDS.

  The entire length must be able to be inspected, even at night

  The system should be clear of any obstruction or device which encroaches upon the system to facilitate tampering(e.g., part of a building)

  The system needs to be illuminated

Alarmed Carrier

When an Alarmed Carrier is used, the following conditions must be met:

- Verify functionality of the alarm daily for TS or Special Category, weekly for Secret, and monthly for Confidential

  The type of alarm is not specified. UL 2050 is not designed for PDS. The alarm should be of good quality and tamper resistant.

  Verifying function should be done under realistic conditions, not just a test to verify that the circuit is intact. Testing should provide assurance that it will work when a real attack is under way.

  There must be a 15 minute response to any alarm

- The cause must be determined
- A decision must be made whether or not to terminate transmission
- Any actual intrusion attempt must be investigated

Continuously Viewed Carrier

When a Continuously Viewed Carrier is used, the following conditions must be met:

- Should be under continuous observation, 24 hours per day
- Should not be mixed in with other things under surveillance (e.g., should not be just one of a number of other locations viewed sequentially on a monitor, like entrance doors, parking lots etc.)

Simple Distribution Systems

When Simple Distribution Systems are used:

- The carrier can be constructed of any kind of material
- Joints must be secured and the access points controlled to the highest level of data handled by the carrier
- Carrier must be inspected in accordance with Table B-2 in NSTISSI 7003
- Table B-1, Decision Matrix for Carrier Types is used to determine what type of carrier is appropriate for type of area and classification level involved. There is always a hardened carrier required in a UAA no matter what type of classified is being transmitted.

Circuit Separation

Circuits of different classification levels may use the same distribution system (however, this doesn’t mean wires for unclassified networks may use the carrier).

If Tempest or Red/Black requirements are imposed, this may not be possible.

DSS policy states that you can’t run unclassified fiber optic with classified metal wire cable or vice versa.

Circuit Access

Persons having access to any access points of the distribution system must be cleared to the highest level of information available at that point.

Persons servicing multi-level systems may be cleared at a lower level, as long as persons cleared to the highest level of the information escort them.

Topic 4: Introduction to Maintenance

In the previous topic, you learned about types of Protected Distribution Systems (PDSs) and the ways in which they are used within a facility.

Additional security concerns can arise when an accredited system requires maintenance. Hardware can be tampered with, software can be changed or malicious logic inserted, or removal of classified information by unauthorized personnel can occur.

In this topic, Physical Security and Maintenance, you will learn about the security requirements that must be met during maintenance operations.

Reference: NISPOM 8-304

Security During Maintenance Operations

Information systems are particularly vulnerable to security threats during maintenance activities. Therefore, the following need to be taken into consideration as the ISSM prepares the SSP:

- Personnel clearance and need-to-know of maintenance personnel
- Type of maintenance (HW/SW)
- Technical knowledge of the escort (if required)
- State of the system (classified, cleared, sanitized)
- Location of maintenance

Maintenance Verification

During the accreditation process, the IS Rep will verify that maintenance procedures contain sufficient instructions on sanitizing IS equipment/media. Instructions should address procedures for sanitizing the equipment/media before it leaves the facility and, if applicable for reexamining it upon return (to ensure there are no added features that will impact security). During the security review, the IS Rep will verify these actions by reviewing the contractor's maintenance records.

Maintenance Performed

Maintenance on IS systems can be performed:

- Outside the facility at a vendor's or third party's maintenance depot
- Via remote communications
- Inside the contractor's facility where the maintenance is performed by either an employee or a third-party individual.

Maintenance Outside the Facility

When practical, all maintenance actions should be performed by appropriately cleared personnel. However, sometimes there is no choice but to use outside vendors for maintenance on accredited systems. In some cases, the contractor must use a vendor for maintenance or the warranty will be voided. In other cases, there may be a requirement to contract out a certain portion or type of work. Also, a contractor may not have the expertise in house or may find that it is less expensive to contract maintenance to an outside vendor than to have a service engineer on staff. Finally, preventive maintenance checks and service may be required.

When maintenance is done outside a facility, the equipment must be sanitized and all labels and markings removed to ensure all indications it had been used for classified processing is no longer evident. Upon return the hardware must be inspected in the same manner as new hardware.

Cleared Maintenance Personnel

Cleared maintenance personnel do not have an inherent need-to-know for any classified information residing on the system; therefore procedures to enforce need-to-know must be addressed in the SSP. This procedure could be as simple as clearing, sanitizing or isolating the IS or equipment on which maintenance is being performed or using discretionary access controls to deny the maintenance person access to classified information. Being cleared permits the maintenance individual to have unescorted access to the unclassified protected maintenance or diagnostics software.

Escorts are not required if the maintenance personnel are cleared to the highest classification level of information on the system and have a need to know for all information processed on that system.

Uncleared Maintenance Personnel

If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower cleared person may be used.

Uncleared maintenance personnel must:

- Be US citizens - The contract between the maintenance service company and the contractor must specify that the maintenance personnel be US citizens. (The ISSM may spot check the citizenship of the maintenance personnel by contacting the company if there is doubt as to the citizenship of a specific maintenance person.)

- Use a separate, unclassified copy of the Operating System (OS), including any micro-coded, floppy disks, CD-ROM, or cassettes that are integral to the OS. The copies must be labeled "Unclassified-For Maintenance Only" and protected to the level of the IS. Any media used during classified processing and remaining on the system should be cleared. After maintenance any media not disconnected, and to be used during classified processing, should be cleared and necessary software reloaded from protected copies.

Escort Requirements

All uncleared (or lower cleared) maintenance personnel must be escorted. Escorts must be appropriately cleared and technically qualified. They need to understand what the maintenance technician is doing to ensure that the uncleared maintenance person neither gains access to any classified information nor has access to the "protected" IS operating system or diagnostic software. Escorts need to understand the

implications of the maintenance actions. They must have sufficient knowledge to suspect any maintenance activity outside the scope of work.

Escort Responsibilities

Escort responsibilities include the following:

- Maintaining constant control over the maintenance technician
- Maintaining shoulder-to-shoulder observation
- Performing system initiation and termination
- Monitoring keystrokes
- Completing the maintenance log.

If system parts are being replaced, the escort must retrieve the old part; the escort must also examine replacement parts prior to installation.

Maintenance Logs

The escort must record the date, time and name of the person responsible for maintenance, repair, installation or removal of hardware components into a maintenance log. The log must also contain information about the component involved, the action taken, and the name of the escort if an uncleared individual performed the maintenance.

Maintenance Tools

The tools used to perform maintenance may also present security concerns. The ISSM must develop procedures by which all maintenance diagnostic equipment is reviewed before usage by the maintenance engineer to ensure the equipment has no memory or storage capability. All components such as diagnostic tools, laptops, oscilloscopes, analyzers and PDA's, must be looked at by the ISSM and evaluated for their ability to retain information. The contractor may need to consult the vendor documentation or contact the vendor direct, to determine the type of memory involved.

The ISSM must review the components for the following capabilities:

- Non-volatile memory
- Fixed or Removable storage
- Volatile memory

If the diagnostic equipment does have memory or storage capability, the diagnostic equipment meets the IS definition and must be accredited before use. The contractor may need to consult the vendor documentation or contact the vendor direct, to determine the type of memory involved. In addition, all vendor-supplied software must reside on write-protected[21] media or be read only. If tools can't be accredited, any media connected to the system during maintenance must be cleared/sanitized prior to connection. After maintenance is completed the media must be cleared to ensure no malicious logic remains, and necessary software reloaded from protected copies.

System Components

Components of an accredited system must remain in the secure environment. If system components are released for maintenance or any other reason, they must be properly sanitized prior to release.

Remote Diagnostics

Remote diagnostics are strongly discouraged. However, if they must be used, the system must be sanitized and disconnected from other secure systems. In addition, the contractor must install a separate copy of the OS and any maintenance software. Even if the vendor is cleared, the IS must still be sanitized if the maintenance is performed using non-secured communication. If the maintenance is performed using secured communication (NSA Type I encryption), and the individuals performing the maintenance do not have a need-to-know for the data, the IS will only have to be "cleared" with access to the protected diagnostic software authorized.

Lesson Summary

In this lesson, you learned about the physical security and maintenance of information systems:

- Physical Security Controls

  In this topic, you learned how to identify appropriate physical controls required to protect classified IS processing. You learned that physical safeguards are required at all times, even when all classified information has been removed from the IS.

- Physical Security Requirements

  In this topic, you learned about the physical security requirements for an IS during attended and unattended classified processing sessions. You learned that all personnel granted unescorted access to the defined perimeter area must have the appropriate clearance and need-to-know, otherwise, they must be escorted. You also learned for unattended processing a closed area is required and closed areas protecting Secret and Top Secret information require supplemental protection.

- Protected Distribution Systems (PDS)

  In this topic, you learned about protected distribution systems and the ways in which they are used within a facility. You learned about the installation and maintenance requirements of PDSs. You also learned about the two types of PDSs including, hardened distribution systems and simple distribution systems.

- Maintenance

  In this topic, you learned about the security requirements that must be met during the maintenance operations. You learned about the maintenance verification process and where maintenance is performed. You also learned about cleared and uncleared maintenance personnel and escort requirements.

Lesson 2: Introduction to Hardware and Software Controls

The NISPOM requires that all hardware and software (HW & SW) be examined when received from the

vendor and before being placed into use. This is to ensure that it contains no obvious features that might endanger the security of the Information System (IS). In addition, appropriate HW & SW controls must be implemented and regularly tested to ensure that IS security is maintained.

You will learn about the security requirements for hardware and software controls.

Reference: NISPOM paragraphs 8-302, 8-306, 8-309, and 8-310.

Lesson Objectives

After completing this lesson, you will be able to:

- Identify software security procedures
- Identify examination requirements for hardware and for test equipment
- Identify marking requirements for hardware and software

Topic 1: Introduction to Software Security Procedures

Before software is introduced into an accredited system, it must be examined. If the software is not immediately loaded once examined, it is a good security practice to protect it from unauthorized modification or replacement. It needs to be protected at the level of the system; otherwise it will need to be examined again prior to loading. It is also a good security practice to maintain a dedicated, protected copy of the operating system in the event of a system crash or failure.

If additional security features, such as write protection mechanisms, are used, they must also be tested prior to use and verified during each classified session.

In this topic, Software Security Procedures, you will learn about the security procedures required to safeguard software.

Reference: NISPOM paragraph 8-302a

Security-Relevant/Related Objects

To ensure IS security, security-relevant/related objects and directories must also be protected. Examples of security-relevant/related objects and directories include:

- Operating system executables and configuration
- System management and maintenance executables
- Audit data
- Security related software
    - Virus protection software
    - Clearing/Sanitization
    - Auditing and Audit reduction software
    - Password generators
    - Trusted downloading process software (hexadecimal editors)

Maintenance/diagnostic software (software that is capable of verifying system performance and/or configuration)

Software disconnect routines (Secret and Confidential only)

Examination of Software

IS software must be examined as soon as it is received from the vendor and before it is used on an accredited system. This is to ensure that the software functions the way it is intended or expected to work. The software must be either reviewed or tested. A review consists of a line-by-line source code review. Testing involves a review of all functionality for security relevant issues, as well as resolving those issues. For example, if the software writes to a file, the file must then be reviewed utilizing a hexadecimal editor to ensure that only the intended information was written. The review and/or testing is to provide reasonable assurance that security vulnerabilities do not exist.

Testing of Software

All commercial off the shelf (COTS) software must be tested to ensure that it contains no obvious features that might be detrimental to the security of the IS. Security-related software must be tested to verify that the security features function as specified. All modifications to security-relevant software must also be reviewed or tested and approved prior to implementation.

Software must be validated before use, and reviewed or tested and revalidated when changed. Since most COTS software, including security-related software, is not available in source code version, testing of the software must be done. The testing must concentrate on the software's functionality. All known security-related functions or features must be tested and validated during the certification process. This is especially true for:

- Access controls
- Auditing
- Sanitization

The contractor must have procedures for testing, or reviewing, approving, installing and maintaining all software resident on the IS. These procedures must also include testing for malicious code and viruses.

Access Controls

Security-relevant/related software is normally protected through the use of access controls. These access controls, known as discretionary access controls are implemented via permission settings within the operating system. Access controls must be implemented for software that:

- performs system functions (such as OS functions, e.g., system log)
- performs security functions (such as auditing)

Access must be limited to personnel with appropriate personnel clearances and need-to-know.

Clearance Requirements

Unclassified software to be used specifically during classified processing periods (e.g. unclassified weapons systems software) can be developed or modified by personnel without a clearance; however, must be reviewed or tested and installed by cleared knowledgeable personnel before use on an approved system.

The contractor personnel, who design, develop, test, install, or make modification to systems or to commercially procured or security-related software are privileged users and require a security clearance to the level of the accredited IS.

Malicious Logic

The ISSM is responsible for implementing security features for the detection of malicious code, viruses, and intruders (hackers) as appropriate. All files must be checked for viruses before being introduced on an IS. The contractor's procedures must include installation of updated virus detection software.

The ISSM is also responsible for reporting incidents involving malicious code to DSS in accordance with NISPOM 8-103f(3).

Public Domain/Personal Software

The use of personal or public domain software is strongly discouraged. Even with the most current software testing, malicious code and viruses can still be present. Public domain software is often of uncertain origin and therefore you can't be certain as to whether or not it may contain malicious logic. For an IS that processes classified information, the vulnerability is significant. However, if the contractor proceeds with using personal or public domain software, the ISSM must approve each installation of such software. It is recommended that these procedures be included in the SSP.

Topic 2: Introduction to Hardware Examination Requirements

In the previous topic, you learned about software security requirements and procedures. In addition to examining and protecting the software used on your IS, you must also ensure that appropriate hardware controls are implemented.

In this topic, you will learn about the examination requirements for hardware.

Reference: NISPOM paragraph 8-302b.

Examination of Hardware

Hardware must be examined to determine that it appears to be in good working order and has no elements that might be detrimental to the secure operation of the IS when placed under control and cognizance. Subsequent changes and developments that affect security may require additional examination.

What to Look For

The ISSM must be cognizant of the following vulnerabilities when examining hardware before classified use, after a physical breach or after maintenance: programmable keyboards; IR/RF ports, other wireless technologies, imaging technology, printers with hard drives; keystroke recording devices (such as KeyGhost or KeyLogger); USB flash memory drives; fixed internal disks in fax machines and

reproduction machines, microphones and cameras, and non-volatile memory.

Evaluate Test Equipment

The ISSM must also ensure that all test equipment be evaluated. All equipment or media with non-volatile memory used to process or retain classified information must be accredited. This means that the ISSM must:

- Evaluate ALL memory
- Determine the type of memory being used
  - Volatile
  - Non-volatile

If the memory is non-volatile, the ISSM must identify which memory captures what type of information. If test equipment has non-volatile memory or secondary storage (floppy or hard drive) that is going to process or retain classified information, it must be accredited as an IS.

All hardware that will retain classified information must be identified in the IS security documentation, preferably the SSP.

Topic 3: Introduction to Marking Requirements

In the previous topic, you learned about the examination requirements for hardware and for test equipment.

In this topic, you will learn about the requirements for safeguarding and marking hardware, software and media output.

Reference: NISPOM paragraph 8-306, 8-309, and 8-310.

Review of Electronic Media

Media used on a classified system must be protected to the level of accreditation until an appropriate classification review has been conducted unless it was properly write protected prior to use. Electronic output, such as media released outside the security perimeter, must be verified by a comprehensive review (in human readable form) of all data on the media including embedded text (e.g., headers and footers). Information not in human readable form (e.g., embedded graphs, sounds, video, etc.) must be examined for content using the appropriate software application and approved procedures. These approved procedures are known as trusted downloading. Trusted downloading procedures must be followed before media is released at a lower classification level than the system. DSS has developed a standard for the trusted download process, which can be found on the DSS website.

Review of Printed Output

An appropriate classification review must be performed on printed output before it is released outside the security perimeter. The review is to determine whether the output is accurately marked with the appropriate classification and applicable security markings.

DSS will approve random or representative sampling techniques when verifying large volumes of output, (in excess of 100 pages), for proper markings. When the output is in printed form, a random sampling of

up to 20% of the output is required.

Marking

The purpose of externally marking media is to clearly identify the classification level of the media. Markings on hardware, output and media must conform to Chapter 4 of the NISPOM, "Classification and Marking." Components must bear a conspicuous, external label. For additional information on marking, DSSA offers a web based course entitled: Marking Classified Documents, IF105.06.

Marking of Internal fixed disks

Markings for internal fixed disks may be placed on the outside of the equipment housing the disks.

Marking Requirements

Labels and Signs

All hardware components of an IS, including input/output devices that have the potential for retaining information must bear a conspicuous, external label or sign that states the highest classification level and most restrictive classification category of the information accessible to the component of the IS.

Labels or signs must remain on the equipment used for classified information until the equipment is powered down or sanitized, as applicable.

The labeling can be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the IS and displayed on the screen.

External Markings

Hard copy output and removable media must be marked as follows:

- Hard copy output[22] must be marked with visible, legible, external markings to the accreditation level of the IS (unless an appropriate classification review has been conducted).
- Removable media must be marked with visible, legible, external markings to the accreditation level of the IS unless the information has been generated by a (DSS approved) tested program verified to produce consistent results (i.e., a trusted downloading process).

Marking Unclassified Media

In approved areas where classified and unclassified information are processed on collocated IS, classified as well as unclassified media must be marked. The purpose is to clearly convey/distinguish the classification level of the media.

The ISSM/ISSO must establish well-defined perimeters for the classified IS. These perimeters distinguish the classified area, and also help distinguish which media require marking.

Writeable media within the classified IS perimeter that is unmarked and not in factory sealed packages must be considered classified and must be marked accordingly.

Writeable media not in the classified area that is unmarked is considered unclassified.

Lesson Summary

In this lesson, you learned about the following:

- Software Security Procedures

  In this topic, you learned about security procedures required to safeguard software. You learned that security-relevant/related software includes virus protection software, sanitization software, audit reduction software, maintenance and diagnostic software. You also learned that IS software must be examined and tested as soon as it is received from the vendor and before it is used on an accredited system.

- Hardware Examination Requirements

  In this topic, you learned about the examination requirements for hardware. You learned that the ISSM must be cognizant of wireless technologies, printers with hard drives, programmable keyboards, and microphones and cameras when examining hardware before classified use, after a physical breach or after maintenance. You also learned that hardware that will retain classified information must be identified in the IS security documentation, preferably the SSP.

- Marking Requirements

  In this topic, you learned about the requirements for safeguarding and marking hardware, software, and media output. You learned that an appropriate classification review must be performed on all output before it is released outside the security perimeter. This review determines whether the output is accurately marked with the appropriate classification and applicable security markings. You also learned that all hardware components of an IS, hard copy output, and removable media must be marked according to the guidelines of the NISPOM, Chapter 4.

Lesson 3: Introduction to Information Systems Operation

As explained in the Information System Security Basics course, there are two states of memory: volatile and non-volatile. There is little security risk associated with volatile memory since all the information in it is lost when the power is removed. Security concerns come into play when the memory is non-volatile.

Non-volatile memory is memory that is permanent or semi-permanent. Since it is desirable to retain some data in computers between various sessions (e.g., data describing the hardware configuration) most computers will have some type of non-volatile memory. Your job is to identify the type and size and include procedures to prevent unauthorized modification to it as well as sanitization of it in the event classified is written to it.

You will learn about the requirement for various Information System (IS) operations used to protect against the unauthorized release of information from storage media.

Reference: NISPOM 8-301, 8- 310b, 8-502, DSS Trusted Download Standard

Lesson Objectives

After completing this lesson, you will be able to:

- Identify clearing and sanitization requirements for various memory, media and equipment
- Identify requirements for trusted downloading

- Identify requirements for periods processing

Topic 1: Introduction to Clearing and Sanitizing Requirements

Any classified data that is contained in any type of memory presents a security risk. To mitigate this risk, you must ensure that all requirements for clearing, sanitizing, and destroying IS storage media are carefully followed.

In this topic, Clearing and Sanitization Requirements, you will learn about the clearing and sanitization requirements for various types of memory, media, and equipment.

Reference: NISPOM paragraph, 8-301

Clearing and Sanitizing Requirements

During the life cycle of an accredited IS, memory and storage media can be cleared or sanitized many times. The distinction of when to clear or when to sanitize depends on the classification level of the information and how the IS is used for classified processing.

If the Information System Security Manager (ISSM) or Information System Security Officer (ISSO) is unable to determine the type of memory or media in the IS to be accredited, the ISSM will need to first, review the documentation for the device or contact the vendor. If a determination still cannot be made, the ISSM may contact the Industrial Security Representative (IS Rep) who may need to contact their Information System Security Professional (ISSP).

Clearing

Clearing is the removal of data from an IS, its storage devices and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using normal system capabilities (i.e. keyboard strokes).

Clearing memory and media (Secret and Confidential only) is required before and after periods processing as a method of ensuring need-to-know protection, and before uncleared maintenance personnel are utilized.

Cleared equipment must continue to be safeguarded at all times, and must carry the highest, most restricted information category type, until sanitized. The cleared equipment can be used to process lower classified information provided it continues to be protected at its original classification level.

Sanitizing

Sanitization is the process of removing information from media or equipment such that data recovery using known techniques or analysis is prevented. Sanitization also includes the removal of all classification labels and markings.

All equipment accredited to handle Top Secret (TS) information must be sanitized during each security level upgrade/downgrade. Once systems that have processed Secret and Confidential information have been sanitized, that equipment can be released from the facility's safeguarding program and either returned to the vendor from which the equipment was obtained or released to an unclassified environment. Top Secret must be destroyed.

Clearing and Sanitization Matrix

A DSS Clearing and Sanitization Matrix, which is an accumulation of known DoD approved methods for clearing and/or sanitization of memory, media and equipment is posted on the DSS website.

If a contractor has memory, media or equipment not identified in the matrix or has a procedure that is more effective than the one identified, the IS Rep will contact the assigned ISSP to inquire whether DSS, NSA or an authorized DoD laboratory has performed or can perform an evaluation. If not, the contractor can send the memory or media to NSA for destruction or arrange with the government customer to return the memory or media for destruction.

Why Destroy Media?

Media and memory are destroyed to preclude the reconstruction or recognition of classified information. The destruction method used should be appropriate for the type of memory, media or equipment.

- National Security Agency (NSA) has approved various destruction devices to destroy CD-ROMs. Contact your IS Rep or ISSP for a listing of these approved devices.
- NSA also provides destruction services to contractor and government for destruction of classified non- Communications Security (COMSEC) related IS media, to include CDs and DVDs**. Normally only Government Furnished Equipment (GFE) See procedures below.**

For additional information, access the DSS Clearing and Sanitization Matrix at the DSS website.

NSA

NSA may accept classified media for destruction from government agencies and contractors. However, contractors must now submit a NSA Destruction Contractor Approval Form, signed by their Contracting Officer Representative (COR), validating that the media in question is associated with a classified contract**. Normally, NSA will destroy classified Government Furnished Equipment (GFE), COMSEC, & Special Access Program (SAP)**. If multiple contractors fall under the same COR then these can be listed on one form and signed by the one COR. The completed form can be submitted to NSA by FAX at 301-688-5468 or by mail to:

National Security Agency

Attn: CMC-Suite #6890

9800 Savage Rd

Fort. George G. Meade, MD 20755-6980

For additional information, refer to the NSA Destruction Facility Guidelines in ISL 2007-01 dated October 11, 2007.

Overwriting Rigid Media

Sanitization of rigid media by overwriting, is no longer authorized by the DSS Clearing and Sanitization Matrix. The overwriting of rigid media to remove classified contamination from an unclassified

Information System (IS), may be allowed, but you should check with your DSS ISSP on a case by case basis. Depending on the situation a clearing action, one time overwrite, may be allowed. In other situations more thorough purging techniques may be required.

Degaussing

Degaussing refers to the destruction of information contained in magnetic media by subjecting that media to high-intensity alternating magnetic fields, causing the magnetic fields to slowly decrease.

Magnetic Tape

Magnetic storage media can be classified according to the amount of magnetic force (measured in "oersteds") necessary to leave a permanent magnetic pattern in the material. To successfully remove magnetic patterns created by these increased magnetic forces, the ISSM must use degaussing equipment of higher oersteds ratings.

Degausser Ratings

Typically, magnetic media are rated according to the amount of magnetic force required to create the magnetic pattern, and degaussers are also rated accordingly, showing the amount of oersteds (Oe) necessary to remove that magnetic pattern causing the magnetic media to be destroyed. Degaussers are defined by the coercivity of the magnetic tape and hard disk media that can be erased, e.g., a 1000 Oe degausser can erase less than or equal to 1000 Oe magnetic media.

A list of NSA approved degaussers is available from your ISR/ISSP.

Other Considerations

Remanance

Remanance is defined as residual information remaining on storage media after clearing. Even when media is overwritten or degaussed, there remains a residue of the former information that can be read using scientific means. If the media is not adequately or properly overwritten or degaussed, it is possible to obtain classified information.

File Deletion or Erasure

File deletion or erasure removes the pointer in the File Allocation Table (FAT) and marks the directory entry as deleted. The computer then treats file space as unallocated and ready for use by another file. Therefore, the file or data may still be retrievable using a utility such as Norton Utilities, DOS Recover, undelete or other "unerase" functions. One hundred percent of the original file may be retrieved. File deletion or erasure is NOT an approved method of clearing or sanitization.

Records

A record of destruction, in accordance with NISPOM paragraph 5-707 is required when TS or Secret Foreign Government Information (FGI) (NISPOM paragraph 10-314) memory or media is destroyed. An audit log entry is required when any classification level of memory or media is cleared or sanitized. Destruction records for TS must be retained for two years and three years for FGI.

5-707. Destruction Records

Destruction records are required for TOP SECRET material. The records shall indicate the date of destruction, identify the material destroyed, and be signed by the individuals designated to destroy and witness the destruction. Destruction officials shall be required to know, through their personal knowledge, that such material was destroyed. At the contractor's discretion, the destruction information required may be combined with other required control records. Destruction records shall be maintained by the contractor for 2 years.

Topic 2: Introduction to Trusted Downloading

In the previous topic, you learned about the requirements and procedures for clearing, sanitizing, and destroying classified information on IS storage media and the security concerns involved with these procedures.

In this topic, Trusted Downloading, you will learn about the IS requirements for trusted downloading.

Reference: NISPOM 8-310b, DSS Trusted Downloading Standard

Trusted Downloading

Trusted downloading refers to a CSA approved procedure or series of procedures, for the secure transfer of classified information of different levels (e.g. Top Secret, Secret, Confidential) or sensitivities (e.g., NATO, Foreign Government Information/FSI, Restricted Data/CNWDI, COMSEC, etc.) to media that will be handled at a lower classification or sensitivity level, or unclassified level, than the IS from which the data was transferred. If not done properly, this downloading process can easily lead to compromise because of the hidden saving and storage capabilities of the software used.

Transferred

The transfer of data from IS accredited/operating at PL-1 to media that will remain under the same or higher level classified environment/controls (i.e. access controls, safeguarding, etc.) does not require the use of trusted downloading procedures. Rather, a review must be accomplished to ensure only designated files were transferred to the new media. This could include a review of hard copy output and/or a short visual review of the electronic file. In instances where information such as NATO, FGI, CNWDI, RD, etc, is stored on the IS and information is downloaded to electronic media, trusted downloading procedures do apply.

To ensure a trusted download has occurred, knowledgeable personnel[23] who are using approved software and techniques must review all information transferred to the new media. These trained and authorized individuals are required to verify no higher classified information is contained on the new media prior to release.

New Media

Use of new media would facilitate compliance with the guidance in NISPOM 8-302a, 8-305 and 8-309. New media would mitigate the possibility of classified system contamination or corruption, as used media could contain and inadvertently introduce unauthorized software into the classified system. Additionally, used media might contain sensitive/classified information for which the recipient is not authorized, causing a violation or compromise.

File Transfer Procedures

The DSS standard identifies approved file types and formats and file transfer procedures.

One of those procedures states that the Folder/directory/subdirectory/File names and/or path names must be unclassified. These names can show up in the information transferred[24]. If these items are classified, the information transferred will be classified. Path names are normally not visible.

These procedures must be documented in the SSP. There are provisions in the standard for alternative procedures that will require written acknowledgement of additional risk from the government customer/data owner.

All files must be reviewed after transfer. Hex Editor software[25] should be used for text. In addition, the ISSM should be sure to check all file names and sizes.

The ISSM must also maintain appropriate records. Records must:

- Specify the data released
- Specify the personnel involved
- Be retained with the audit records

DSS Authorized Formats

DSS has listed the authorized formats in which information can be saved in order to ensure extraneous information, which cannot be easily viewed, does not transfer. This extraneous information could contain classified information.

The following formats are authorized:

- For text files:

  ASCII (.txt, .dat, .c, .for, .fil, .asc, .bat)

  .htm/.html

- For spreadsheet and database files:

  ASCII

Additional authorized formats include:

- For graphic files: Graphic files, which normally can't be viewed with other utilities, can be saved as a 'flat file' in the following authorized formats:

  BMP

  JPG

  GIF

Review Required

Even though the file is saved in one of the authorized formats, the file on the new media must be reviewed in its entirety after the transfer. Utilities other than the application should be used to view the transferred file on the new media.

Preferred Review for Applications

- ASCII text - The preferred application for reviewing these files is NotePad. However, this application has file size limitations; therefore, Hex editing software may need to be used. When conducting the review, be sure to check file names and sizes.
- BMP and JPG files - These files may be reviewed with a graphics file viewer such as MS Photo Editor.
- GIF files - GIF files may be viewed with Internet Explorer or Netscape. Because GIF files may contain a 3D/animation/multi-page image, they must be viewed with a program that will show all the information stored in the GIF files. MS Photo Editor will not display all the frames (images).

Training and Acknowledgement

Users that are required to perform trusted downloading must be trained on each format used. A Trusted Download Authorization form, available on the DSS website must be executed and the ISSM must maintain the forms for each user. The record must be maintained with the audit records.

Non-DSS Procedures

If alternate[26] procedures are needed, the procedures must be tested and coordinated with DSS. The ISSM must submit the alternate procedures with a Risk Acknowledgement Letter to the GCA/data owner(s) for signature.

Once the Risk Acceptance Letter is received, signed by the Government Contracting Activity (GCA)/data owner, the ISSM must modify the SSP to include the approved alternative procedures, attach a copy of the signed letter and then submit the modified SSP to DSS.

Problems in Downloading

One of the most serious problems in downloading is that many applications have areas where classified information can reside, but not be immediately viewable. The user may or may not be aware of these areas to check.

This is why the standard limits the file formats authorized. Files need to be saved in an authorized format for DSS to approve trusted downloading. Otherwise, alternative procedures must be developed, tested, and approved and accepted by the data owner.

Areas to Check

Examples of areas to check include speaker notes in PowerPoint slides, information stored in 'undo' files attached to the original file, and track changes which do not show up on the screen. In addition there are software programs such as those used for Computer-Aided Design (CAD) systems and mapping software that may have many levels of information that can be "turned on or off".

Slack Space

A second problem concerns the use of slack space. All operating systems have slack space at the end of a file because the file normally does not fill the last allocation unit on the new media. Some older OS (DOS, Windows 3.1, Windows 95 and older versions of MAC OS) take whatever information is in memory next to the file (while it is being copied to the new media) and puts it on the new media.

If you use these types of operating systems as part of the trusted download process, you must do a complete review of the slack space and document the review procedures in your SSP.

Newer operating systems, such as Windows 98, NT, 2000 and XP, fill the slack space with 0's. Therefore, slack space in those cases is not an issue, and does not need to be addressed in your SSP. Some software that can be used to review slack space if necessary includes, S Copy, K Copy, WINREVW, Axe and Winhex. Your ISSP may have one or more of these tools they can make available to you.

Before You Download

Before downloading lower or unclassified information to a separate media source, the following should be considered:

- Is software available to view everything in the text files?
- How will graphics be handled?
- Will changing the format of the file help?
- Does the person reviewing the information know the security classification guide?
- Have the procedures been thoroughly tested?
- How does the operating system or copy utility deal with 'slack space'?

Remember: Security personnel must be able to read all material before they can ensure that it does not contain classified information.

Topic 3: Introduction to Periods Processing

In the previous topic, you learned about the requirements for trusted downloading and the security concerns related to this process.

Security concerns can also arise when users with different clearances, need-to-know, formal access authorizations, or combinations thereof share the same IS. When this occurs, a process known as periods processing may be used to avoid accreditation at higher protection levels.

In this topic, you will learn about the requirements for periods processing.

Reference: NISPOM 8-502

Periods Processing

Periods processing refers to a standalone IS that is shared by users with different clearance, or needs-to-

know, formal access approval requirements or combinations thereof. Periods processing also involves upgrading a system to a classified or higher classified level or downgrading it to an unclassified or lower classified level.

An IS employed in periods processing must:

- Be cleared/sanitized before and after use
- Be cleared/sanitized between Periods
- Have separate media for each period of processing (including copies of operating systems, utilities, and software applications)

Sanitization After Use

The NISPOM, paragraphs 8-301 and 8-502b, requires that IS resources and media be sanitized before and after periods of processing.

However, only clearing is required as a method of ensuring need-to-know protection and prior to maintenance. If the IS is being "released" (i.e., not physically protected at the higher level) to a user with a lower personnel security clearance, or, if the IS is accredited at the Top Secret level, then sanitization is required.

These procedures must be documented in the SSP.

Sanitization Between Periods

The NISPOM, paragraph 8-502c, requires the IS to be sanitized between different processing sessions (between different groups of users).

Only clearing is required if the IS is not being released to a user with a lower PCL or accredited Top Secret Level.

These procedures must be documented in the SSP.

Security Level Upgrading

The IS needs to be properly upgraded and or downgraded when transitioning from one periods processing session to another. Security level upgrading refers to increasing the classification level of processing on an IS. Such procedures include describing how to upgrade the system from a lower classified state or unclassified state to a higher level of classification. They include:

- Ensuring Closed Area controls are in place or
- Establishing the defined perimeter (restricted area) as described in the SSP
- Removing storage media not used for the classified processing session
- Loading separate media

IS being upgraded to process classified information can be booted from a floppy disk or CD-ROM provided they are protected to the level of the information system and are used in a read-only

configuration. DSS recommends, however, that classified information systems be configured to boot only from specific hard drives to minimize the possibility of security controls being circumvented by external media.

When upgrading the security level, the ISSM must be sure to:

- Practice In Use controls[27] while processing classified information
- Ensure that all media within the defined perimeter in a collocated environment is properly marked

Security Level Downgrading

Security level downgrading refers to lowering the classification level of processing on an IS. This involves taking the system from a classified state to an unclassified state or to a lower or less restrictive level of classification. Procedures for downgrading the security level include:

- Removing, marking and storing classified material and media
- Clearing of memory and media for Secret and Confidential before and after periods processing
- Sanitization of memory and media for Top Secret

Complete the Paperwork

Remember that nothing is finished until the paperwork is complete. Appropriate entries in the audit trails and/or logs are required for the upgrade and downgrade actions.

Lesson Summary

In this lesson, you learned about the following:

- Clearing and Sanitizing Requirements

  In this topic, you learned about clearing and sanitization requirements for various types of memory, media, and equipment. You learned that the distinction of when to clear or when to sanitize depends on the classification level of the information an how the IS is used for classified processing. You learned that maintaining the security of the overwrite utility is an important part of the IS security plan and the utility and procedures must be carefully developed and clearly identified. You also learned about several other types of clearing and sanitizing methods and issues such as degaussing, remanance, file deletion or erasure, and records.

- Trusted Downloading

  In this topic, you learned about the IS requirements for trusted downloading. You learned that when multiple files are transferred, a new folder/directory/subdirectory should be set up to retain files for review prior to transfer and that all files must be reviewed after transfer. You learned that DSS has a list of the authorized formats in which information can be saved in order to ensure extraneous information, which cannot be easily viewed, does not transfer. You also learned that files need to be saved in an authorized format for DSS to approve trusted downloading.

- Periods Processing

  In this topic, you learned about requirements for periods processing. You learned that periods processing refers to a standalone IS that is shared by users with different clearance, or needs-to-know, formal access approval requirements or combinations thereof. You learned that periods processing also involves upgrading a system to a classified or higher classified level or downgrading it to an unclassified or lower classified level. You also learned the requirements for security level upgrading and downgrading.

Module 5: Technical Protection Measures

Lesson 1: Introduction to Identification and Authentication

As the complexity of a specific Information System (IS) and the associated risk for this system increases, the need for identification and authentication (I&A) of users and processes becomes more significant. I&A controls are required to ensure that users have the appropriate clearances and need-to-know (NTK) for the information on a particular system. I&A controls are also required to ensure that users are managed in accordance with procedures identified in the System Security Plan (SSP).

You will learn about I&A technologies and required I&A procedures.

References: NISPOM paragraphs 8-303, 8-505, and 8-607a

Lesson Objectives

At the end of this lesson, you will be able to:

- Identify types of Identification and Authentication technologies
- Identify requirements for user ID generation, protection, removal and revalidation
- Identify appropriate session controls

Topic 1: Introduction to Identification and Authentication Technologies

Identification and Authentication (I&A) can be established using a number of different methods. In this topic, you will learn about several types of I&A options or methods.

References: NISPOM paragraph 8-303

Identification and Authentication

When users logon to a computer system, they must both identify and authenticate themselves as authorized users of the system.

What do identification and authentication mean?

- Identification refers to the process that an IS uses to recognize an entity. It is the way you tell the system who you are. This usually consists of a name.
- Authentication is a security measure designed to establish the validity of a transmission, message or originator; or a means of verifying an individual's authorization to receive specific categories of information. It is how you prove you are who you claim to be.

Identification

Unique identification

No matter how small or large an IS is, each user must be uniquely identified or identifiable before access can be granted. Before first access is granted, every user must provide the ISSM with proof of identification. Once identification is verified, the ISSM must validate the user's clearance level and NTK against the Protection Level (PL) of the system.

Ways to Authenticate

There are three classic ways for users to authenticate themselves:

- Something you know
- Something you are
- Something you possess

Something You Know

The use of passwords is the most common form of authentication.

Something You Are

In place of passwords, physiological or behavioral traits can be used to authenticate IS users. This includes the use of fingerprints, hand prints, iris scans, voice, signature or keystroke patterns.

These biometric systems compare a particular user trait against one stored for the user and determine whether the user is who he/she claims to be.

Something You Possess

Instead of passwords or biometrics, the following can also be used to authenticate IS users:

- Challenge-Response systems

  Challenge-Response systems are based on the ancient concept of challenge/response. You are asked a question and you must provide the proper response. An example is a card that generates pseudo random numbers that you must enter when requested by the system.

- Smart Cards

Smart cards contain microchips with the information needed to access the system. They are used in conjunction with a pin number or other authenticator (e.g., fingerprint) much like an ATM card.

No matter what form of technical authentication is used, access to authentication data shall be restricted to only those privileged users whose job function requires access. User authenticators are for individual use only and shall not be shared. Passwords may be committed to memory, but if written down must be safeguarded to their level of access. Any authenticator in the form of a possession (i.e., smart card, token or key) shall be kept in the possession of the owner when in proximity of an accredited IS.

Standalone Work Stations and Small LANS

In some cases, I&A becomes a manual procedure. This is true, for example for standalone workstations or small local area networks (LANs). In this case, physical security controls and personnel security controls are used.

NISPOM, Paragraph 8-303c permits alternative authentication procedure that enables the ISSO to quickly and easily authenticate users.

Alternative authentication procedures include physical security controls and personnel security controls to augment the logon authentication requirement for standalone workstations or local area networks. What types of personnel security controls are acceptable?

• Answer: The ISSM/ISSO are responsible for verifying all users' clearance and need-to-know requirements. Once briefed, the users' names will be added to the area access list or the equipment authorization lists which authenticates that the user is authorized and briefed. The access lists shall be retained as an Audit 1 requirement.

Four Conditions

Four conditions must be met before the alternative, manual I&A procedures can be used in the case of small LANs.

1. The LAN must meet the requirement for "small"

   Small
   Small refers to the area, to include size, in which the workstations are located. All workstations need to be arranged such that each user is visually identified as authorized prior to and during classified processing.

   If the OS supports technical I & A, DSS recommends that contractors implement these features.

2. The workstation must not have a permanent (internal) hard drive

3. All users with access to the workstation and the security container/removable media must have the required clearance level and NTK for all the data processed on the system

4. The system must be located within an approved security area (i.e., a Closed Area or a "restricted area")

   Restricted area
   A perimeter control boundary area is also referred to as 'restricted area'.

The ISSM/ISSO verifies all users' clearances and need-to-know requirements. Once briefed, the users' names are added to the area access list or the equipment authorization lists which authenticate that the user is authorized and has been briefed. This type of authentication works well in conjunction with user identification (e.g., picture identification). These access lists must be revalidated annually and retained as an Audit 1 requirement (12 months). (Note: Audit 1 requirements will be discussed in the Audit Requirements lesson.)

Alternative I & A procedures include area access lists, picture ID and visual observation to ensure only authorized individuals are allowed access.

Topic 2: Introduction to I&A Requirements

In the previous topic, you learned about required I&A controls and the various ways in which user I&A can be implemented. You learned that these I&A controls help ensure that users have the appropriate clearances and need-to know for information on a particular IS.

In this topic, I&A Requirements, you will learn about requirements for user ID generation, protection, removal and revalidation.

References: NISPOM paragraphs 8-303 and 8-607a

User Identification

NISPOM requires that identification to the system occur when authenticating (i.e., at logon). The most common method used is the user identification (user ID). The ISSM will issue the user a unique user ID for ISs that require technical user ID. Usually, the user ID will consist of some portion of the user's name or initials, and identifies to the IS who the user is. (Note: Guest logins need to be disabled.)

Each user must be uniquely identified so that the user's identity can be associated with all auditable actions taken by that individual.

User ID Protection

There are several steps the ISSM can take to protect user IDs. The ISSM must ensure that:

- Only authorized users have access to the ID
- User IDs are not shared
- Active user IDs are revalidated regularly (at least annually)
- All access authorizations are removed from the system, prior to reusing a user ID

User ID Removal

When an employee terminates, loses access to the system for cause, or no longer has a reason to access the IS, the ISSM must ensure that that individual's user ID and its authentication are disabled or removed from the system. This procedure must be included in the SSP.

Requirements for Passwords

When using passwords to authenticate a user to the system, the ISSM must be aware of several requirements. When used as authenticators, passwords must:

- Be marked and protected at a level equal to the classification level of the information to which they allow access (Note: Even though passwords are hashed[28], a printed password file must be treated as though classified.)
- Contain a minimum of eight, non-blank characters
- Be valid for no longer than 12 months
- Be changed if compromised

Password Generation

The preferred method of password generation is to have the IS generate unique, random passwords. However, users may generate their own passwords. If passwords are generated by users, they must also contain a minimum of eight, alpha/numeric, upper/lower case characters and users must be briefed on not using dictionary-definable words.

The SSP must address password generation method, length and size of the password space. The length of the password and the possible characters in each position determine password space size. There is vulnerability associated with the size of the space. The larger the space, the longer it takes to brute force a password.

To satisfy the NISPOM requirement for the size of a password space, the SSP must contain the minimum password length and the number of characters that are possible in each position in the password.

Password Space

If the possible characters for your password were all of the uppercase letters, then you'd have 26 choices for each position in the password. If your password were one character long, then you would have 26 possible passwords. The password space is the number of possible passwords. If your password is two characters long, then a theorem in probability theory says that the number of possible combinations (size of the password space) is 26 x 26, or 26^2 (26 to the second power). If the password is eight characters long it is 26^8.

If the possible characters for each position in the password is all upper case, lower case, numbers, punctuation and special characters, there are 26 (upper case) + 26 (lower case) + 10 (numbers) + 33 (punctuation and special characters, including the "space " character) = 95 possible characters for each position. Then, for an 8-character minimum password length, the minimum size of the password space = 95^8 (the size of the password space would be exactly 95^8 if the password length was 8 characters).

However, the NISPOM requires a minimum of eight non-blank characters, so the space character cannot be used.

At PL 1, the NISPOM does not require a minimum password age, or password history. No minimum password age allows a user to change the password and then, immediately change the password back to the original password. Password history will, depending on the number set in this area, not allow the user to change their password to one previously used. While not a requirement, it is recommended as a good security practice to set the minimum password age and password history at other than zero for PL 1 systems. At PL-2 Password history must be implemented.

Also, the contractor must ensure that standard (default) passwords have been changed. Refer to vendor documentation for information on any default passwords. Some operating systems have standard authenticators such as SYSTEM, MASTER, TEST and other passwords already installed on the system. Those passwords must also be changed. It is also important to remember that passwords may need to be changed after a new software version is installed or after other action is taken that might result in the restoration of these standard passwords. When an IS cannot prevent a password from being echoed or visually displayed, an overprint mask must be printed before the password is entered to conceal the typed password.

'The following website lists many default passwords for various types of computer products. This is for informational purposes only. The best source is the vendor documentation.

http://www.phenoelit.de/dpl/dpl.html

Topic 3: Introduction to Session Controls

In the previous topic, you learned about the requirements for user ID generation, protection, removal and revalidation.

In this topic, Session Controls, you will learn about the requirements for PL-1 session controls.

References: NISPOM paragraphs 8-505 and 8-609a

Session Controls

Session controls provide additional protection to ensure only authorized personnel have access to the system.

Session Controls 1: PL-1

The NISPOM provides the following PL-1 session control requirements. Prior to gaining access to a system, all users must be notified that:

- System usage is monitored, recorded and subject to audit.
- By using the system, they consent to such monitoring and recording.
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties.

If the Operating System (OS) permits, this warning text (also known as a warning banner) appears on each initial screen (displayed before the user logon). Users are required to remove the notice before they can continue.

DSS has posted the DSS authorized warning banner text on the ODAA page of the DSS website.

If it is not possible to provide an initial screen warning notice, establish another method[29] of notification that is approved by the CSA. This would be documented as an approved variance in the SSP.

Logon Attempt Controls

The NISPOM also discusses Logon Attempt controls. If the OS provides the capability, successive logon

attempts shall be controlled as follows:

- Deny access after no more than five consecutive unsuccessful attempts on the same user ID
- Limit the number of access attempts in a specified time period
- Use a time delay control system[30]
- Or employ other methods approved by your ISR/ISSP

The controls used need to be described in your SSP.

System Entry

All users' accounts must indicate under what conditions the individual may gain access to any remote system.

If specific requirements are not indicated, users may not have remote access to the system, nor may they have remote anonymous file access to the system.

Group Authenticators

Some systems allow users to use a Group authenticator[31] to identify and authenticate themselves.

In general, group authenticators should not be used. When group authenticators are used, it is not possible to associate a particular act with the person who initiated it. This can create difficulties with audits and/or administrative inquiry investigations.

Group authenticators shall be used only for broader access after the use of a unique authenticator for initial identification and authentication. The procedures must be documented in the SSP.

Group authenticators may not be shared with anyone outside of the group.

Lesson Summary

In this lesson, you learned about the following:

- Identification and Authentication Technologies

  In this topic, you learned about the various types of Identification and Authentication options. When users logon to a computer system, they must both identify and authenticate themselves as authorized users of the system. You also learned that there are three classic ways for users to authenticate themselves, namely, by "something you know," "something you are," or "something you possess."

- Identification and Authentication Requirements

  In this topic, you learned about the requirements for user ID generation, protection, and removal and revalidation. Each user must be uniquely identified so that the user's identity can be associated with all auditable actions taken by that individual. You also learned that the preferred

method for password generation is to have the IS generate unique, random passwords. If this is not technically possible, users may generate their own passwords.

- Session Controls

  In this topic, you learned about the requirements for PL-1 session controls. You learned that for PL-1 session control requirements, all users must be notified of specific requirements prior to gaining access to a system. These specific requirements are the following: system usage is monitored, recorded and subject to audit; by using the system, users consent to such monitoring and recording; and unauthorized use of the system is prohibited and subject to criminal and civil penalties.

Lesson 2: Introduction to Audit Requirements

Security auditing involves recognizing, recording, storing and analyzing information related to security-relevant events. Maintaining comprehensive records and ensuring that these records are reviewed on a regular basis is an important part of the Information System (IS) security process.

You will learn about audit requirements for accredited systems.

References: NISPOM 8-501, 8-503, 8-602a

Lesson Objectives

After completing this lesson, you will be able to:

- Identify the purpose of audit records
- Identify standard auditable events
- Identify review intervals and record retention requirements

Topic 1: Introduction to Audit Trails, Records, and Logs

Audit trails[32], audit records[33], manual logs, and manual auditing play an important role in maintaining the security of an information system. Audit trails, logs and records enable you to more effectively monitor your system and protect it against potential and actual threats.

In this topic, Audit Trails, Records, and Logs, you will learn about the purpose and types of audit trails, records, and logs.

Reference: NISPOM 8-602a

Why is Auditing Important?

Auditing is important for two reasons. It enables the Information Systems Security Manager (ISSM) to:

1. Maintain a record of which activities occurred and which user or process was responsible
2. Reconstruct events before and after a security incident

Auditing also enables the ISSM to check for the initiation or termination of security-related events, and can be used as an investigative tool to determine the extent of loss or compromise of classified information.

Two Types of Auditing

There are two types of auditing: automated and manual.

Automated auditing occurs when an Operating System (OS) automatically creates and maintains an audit trail. This includes the use of third party software used to meet NISPOM audit requirements.

In certain circumstances an alternative method of accountability for user activities on the system is needed. This alternative auditing method is referred to as manual auditing.

Auditing Requirements

The NISPOM lists the following auditing requirements:

All multi-user systems must use automated auditing unless the OS cannot provide an automated audit capability. In that case, alternative manual auditing is required.

For single-user, standalone systems, audit trails are not required; however, manual logs are. A single-user, standalone system is an IS that is physically and electrically isolated from all other systems and is intended to be used by one person only, e.g., a laptop assigned to one person, a personal computer assigned to one individual. If each user of the standalone has his or her individually assigned removable hard drive and the system is sanitized between users, the system will be considered single-user, standalone. Information Technology (IT) personnel will not be considered users of single-user standalone systems.

OS cannot provide

The NISPOM requires automated auditing which may require the contractor to upgrade OSs that are not capable of meeting these requirements unless an exception is granted. Exceptions are intended for rare situations and require a government contracting activity to authorize in writing the continued use of an OS that is not capable of automated auditing.

Capability

Most OSs can be configured to meet NISPOM audit requirements; however, some OSs do not have this capability and will require the installation of third party software in order to be in compliance with NISPOM requirements.

Topic 2: Introduction to Auditable Events

In the previous topic, you discovered why auditing is important and that there are two types of auditing,

automated and manual.

To ensure that all necessary information is accurately recorded, the NISPOM indicates the specific types of events that must be audited when using manual or automated auditing.

In this topic, you will learn to identify:

- Automated auditing requirements
- Alternative manual auditing requirements
- Manual log requirements

References: NISPOM 8-501, 8-503 and 8-602a

Automated Auditing Requirements for PL-1 Systems (Audit 1)

The NISPOM specifies the type of information that must be gathered and the standard events that must be audited when using automated auditing on a PL-1 system (Audit 1). These automated audit trails must include enough information to determine the action, the date and time of the action, the system locale of the action, the system entity that initiated/completed the action, and the resources involved for:

- Successful and unsuccessful logons and logoffs
- Unsuccessful accesses to security-relevant objects and directories
- Changes in user authentication
- Blocking of a user ID, terminal or access port (and the reason)
- Denial of access for excessive logon attempts

The NISPOM also requires that the contents of audit trails must be protected against unauthorized access, modification or deletion.

Automated

Microsoft OS (i.e., Windows NT, 2000, XP & Vista) can be configured to meet NISPOM audit requirements. Microsoft Windows can be configured to audit individual success or failure to system accounts, directory service access, object access and system user activity.

Unix OS capabilities will vary. Some Unix type operating systems (e.g. Linux) require the addition and local configuration of third party software while others (e.g. IRIX, Solaris) can be configured to meet audit requirements using products delivered with the OS software.

Unsuccessful accesses

Unsuccessful accesses include unsuccessful attempts to create, open/close, or modify/delete security-relevant objects or directories.

Security-relevant objects and directories

Security-relevant objects and directories are part of all operating systems but are not identified the same or may not reside in the same folders/directories. Security-relevant objects include operating system executables; operating system configuration; system management and maintenance executables; audit data and security-relevant software. Security-relevant software includes:

- Virus protection software
- Clearing/Sanitization software
- Auditing/Audit reduction software
- Password generators
- Trusted downloading process software (Hex editors)
- Maintenance/diagnostic software (software that is capable of verifying system performance and/or configuration
- Software disconnect routines (Secret and Confidential only)

Alternative Manual Auditing Requirements

If the OS cannot provide automated auditing and an exception is granted, then manual auditing must be performed. The manual auditing must include:

- User name
- Time on the system
- Time off the system

Exception is granted

The NISPOM requires automated auditing which may require the contractor to upgrade OS that are not capable of meeting these requirements or obtain third party software unless an exception is granted. Exceptions apply only to those rare situations when a government contracting activity requires the use of an operating system that is not capable of meeting Chapter 8 audit requirements. In such instances, a NISPOM waiver is not required. Contract documentation from the GCA, such as the DD Form 254, formal classification guidance and/or a formal memorandum that clearly directs the use of these operating systems must be provided to DSS. A suggested format is a statement such as, “the contractor is required to use Windows 98”, followed by the rationale for its use. The statement must be signed by the Contracting Officer, the contracting Officer’s Representative (COR) or the Contracting Officer’s Technical Representative (COTR). A formal contract modification is not necessary.

Manual Log Requirements

In addition to the information gathered by automated auditing or manual auditing, ISL 01L-1, Question 53, specifies the information that must be gathered for all systems.

1. The Date, Time, and Person Responsible for:
2. Periods processing times
3. Installation, testing, and modification of OS and security related/relevant software (logs must

identify the software involved)

4. Application and reapplication of security seals (if applicable)

5. Sanitization of memory, media, and devices

Maintenance, repair, installation or removal of hardware components (logs must include the component involved, the action taken and the name of the escort, if the maintenance was performed by an individual without an appropriate clearance)

Reduced Technical Requirements for Special Categories

Using reduced technical requirements can adequately protect certain types of systems. This applies to the following special category type systems:

- Single-user, standalone systems
- Pure servers

Standalone Systems

A standalone system is a system that is not connected to any other system and has no outside connectivity. Standalone systems can be either single-user or multi-user systems.

The difference between single-user, standalone systems and multi-user, standalone systems is the number of users who are authorized to use the system.

- Single-user, standalone systems - intended to be used by one person only or if each user of the standalone system has his or her individually assigned removable hard drive and the system is sanitized between users, the system will be considered single-user (IT personnel will not be considered users of single-user, standalone systems).
- Multi-user, standalone systems - an IS that is physically and electrically isolated from all other systems, intended to be used by one person at a time with data belonging to other users remaining on the system.

Requirements for Single-User, Standalone Systems

For single-user, standalone systems, extensive technical protection measures are normally not appropriate. In these cases, administrative and physical protection measures may be substituted for technical ones (i.e., picture IDs and access lists).

Automated audit trails (as well as automated Identification and Authentication (I&A)) are not required; however, manual logs are.

Requirements for Pure Servers

Pure servers are special purpose servers that have the following characteristics:

- No user code is present on the system

- Only system administrators and maintainers can access the system
- The system provides non-interactive services to clients
- There is a low risk of attack

The category of specialized systems such as pure servers does not fit the protection level criteria as does the general-purpose or office automation system. The pure server does not have users in the traditional sense, but has clients. Examples of pure servers include: NSA (National Security Agency), Type 1 encryption devices, application servers, guards, and proxy servers. Each pure server is different, serves a specialized purpose and must be reviewed by DSS before a determination is made as to what, if any, technical security features are required. Generally, technical security requirements can only be reduced if other security requirements (e.g., the physical and communications security requirements determined by the information handled or protected by the system) for the system are adequately applied.

If the maintenance of pure servers is performed remotely, I&A, audit and access control mechanisms must be in place.

Topic 3: Introduction to Audit Analysis

In the previous topic, you learned to identify standard auditable events.

Creating and maintaining accurate audit trails and logs is an important part of the IS security process. It is equally important, however, to establish a regular schedule for reviewing the data collected in the audit records.

In this topic, Audit Analysis, you will learn about the requirements for reviewing and retaining your audit records.

Reference: NISPOM 8-602a

Why Review Audit Records?

In addition to requiring that audit records be maintained, the NISPOM also requires that audit records be analyzed on a regular basis. Doing so helps ensure that any unusual and potentially threatening events are noted and dealt with in a timely manner.

The Audit Review

When a review is conducted, any anomalies must be noted, reported to the ISSM/ISSO, and corrected.

A good rule of thumb is: Don't assume anything! If a potential compromise is found, stop processing and investigate.

In particular, the following should be monitored:

- Who uses the system?
- Who has privileges above the ordinary user (for example, super users)?
- Abnormal activity (for example, unusual hours of usage)

- Unauthorized access attempts
- Unscheduled maintenance

The audit review should also include a review of:

- Maintenance equipment brought in
- Unscheduled equipment changes
- Additions to IS (HW, SW, or Firmware)
- Disconnects not performed
- An unclassified system connected to a classified system

User Compliance

All users must comply with the IS security program requirements, know their responsibilities and be accountable for their actions on an IS. The ISSM must ensure that all users are aware of this requirement. During IS briefings, the importance of reporting anything unusual should be emphasized.

Audit Review Intervals

Audit reviews must be scheduled and performed at regular intervals. Information about audit review intervals must be included in the System Security Plan (SSP).

The ISSM must identify an IS audit review interval. The frequency of reviews must be at least weekly, but can be as often as daily (e.g., for large or networked ISs). When deciding on the appropriate review interval, consider the amount and type of classified information to be processed and, if necessary, discuss with your IS Rep.

Audit records must be retained for 12 months.

Lesson Summary

In this lesson, you learned about the following:

- Audit trails, records, and logs

  In this topic, you learned about the purpose and types of audit trails, records, and logs. You learned that there is automated and manual auditing and logs. You also learned that auditing is important because it enables the ISSM to maintain a record of which activities occurred, which user or process was responsible, and to reconstruct events before and after a security incident.

- Auditable events

  In this topic, you learned to identify automated auditing requirements, alternative manual auditing requirements, and manual log requirements. You learned that automated audit trails must include information to determine the action, the date and time of the action, successful and unsuccessful logons and logoffs, changes in user authentication, and denial of access for

excessive logon attempts. You learned that manual auditing must include user name, time on the system, and time off the system. You learned that manual log requirements include the date, time and person responsible for periods processing times, application and reapplication of security seals, sanitization of memory, media and devices, installation, testing, modification of OS and security related and relevant software, and maintenance, repair, installation, or removal of hardware components. You also learned that the contents of audit trails must be protected against unauthorized access, modification or deletion.

- Audit analysis

  In this topic, you learned about the requirements for reviewing and retaining audit records. You learned that the NISPOM requires audit records be analyzed on a regular basis. You learned what to look for when conducting an audit review such as who uses the system, unauthorized access attempts, unscheduled maintenance, disconnects not performed, and unscheduled equipment changes. Audit reviews must be scheduled and performed at regular intervals and information about the review must be included in the System Security Plan. You also learned audit records must be retained for the period covering the previous 12 months, or since the IS was accredited (whichever is less).

Lesson 3: Introduction to Interconnected Systems Management

When information systems (IS) are interconnected and implemented as networks, special security considerations are required. Even if the networks are accredited at the same protection level, the combination of data and/or the combination of users on a connected network may require a higher protection level and require that additional security measures be implemented.

You will learn about the security requirements for interconnected networks.

References: NISPOM paragraphs 8-605, 8-700 through 8-702

Lesson Objectives

After completing this lesson, you will be able to:

- Identify types of networks
- Identify methods for securing network interconnections
- Identify network requirements and accreditation procedures for Unified and Interconnected networks

Topic 1: Introduction to Types of Networks

Security requirements and Certification and Accreditation (C&A) procedures for IS vary depending upon the type of network being certified and accredited.

In this topic, you will learn about different types of computer networks and interconnection methods.

References: NISPOM paragraphs 8-700 and 8-702

What is a Network?

A network is comprised of an Information System implemented with a collection of interconnected nodes. The perimeter of a network encompasses all of its hardware, software, and attached devices. Its boundary extends to all of its users.

Two common types of communications networks are:

- Local Area Network (LAN)
- Wide Area Network (WAN)

Local Area Networks and Wide Area Networks

A LAN is defined as two or more computers connected together so they can share files and computer equipment. Local area networks are usually confined to a small geographic area, such as an office or building.

A WAN is also composed of two or more PCs connected together so they can share files and computer equipment. However, unlike a LAN, a WAN connects computers across a large geographic area, such as a city or country. (The Internet is an example of a WAN.)

The Information System Security Manager (ISSM) must ensure that there is some method to verify[34] that each remote user has a clearance, need-to-know (NTK), and formal access approvals for access to connecting sites. There cannot be an assumption that, since the ISSM for the remote site has verified the information for their own users, it is sufficient for the host.

Network Components

LANS and WANS can be made up of the same components. These components include:

- Multiple computers
- Network Interface Card (NIC)
- Controlled Interface
- Cable or wires
- Wireless connectivity
- Network Operating System (NOS)

Network Architectures

Networks can be configured in one of two ways:

- **Client/Server Network**
  A client/server network is an architecture in which the user's PC (the client) is the requesting machine and the server is the supplying machine.

- **Peer-to-Peer**

  A peer-to-peer network describes a system without defined client/server functionality. A peer-to-peer involves systems with no specialized functions. Each machine has equal responsibility and/or authority.

Types of Networks

For purposes of accreditation, the NISPOM identifies two types of Networks:

- Unified Network - A collection of information systems accredited as a single entity under a single security policy
- Interconnected Network - Two or more separately accredited information systems or unified networks

Unified Networks

As a general rule, LANs within the facility are considered Unified networks. In addition, two or more LANs connected within a facility (same CAGE Code) are generally accredited as Unified networks, although in some cases they can be accredited as Interconnected networks.

Only in rare instances should WANs be accredited as a Unified network.

Unified Network Characteristics

A unified network is always:

- Accredited as a single entity with one System Security Plan (SSP)
- Issued a single letter of Accreditation
- Accredited at a single security protection level
- Managed by a single ISSM/Information Systems Security Officer (ISSO)
- Directed by a single security policy

Interconnected Networks

An interconnected network is comprised of two or more separately accredited systems and/or networks. These can be intrafacility, contractor-to-contractor or contractor-to-government. Each separately accredited system or network maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation.

Interconnected networks can consist of LANs within a facility or WANs. This type of network requires a Network Security Plan (NSP).

Interconnected Network Characteristics

An Interconnected Network:

- Is managed by a Network ISSO
- Is composed of separately accredited ISs with their own SSPs
- Is also accredited at the network level through an Network Security Plan
- Maintains its own intra-IS services and controls
- Protects its own resources
- Retains individual accreditations

An interconnected network has a host site which functions as the network security management site. The ISSO for the host site becomes Network ISSO and prepares the Network Security Plan.

The Protection Level (PL) of the network will be based on clearance, need to know, and formal access authorization of the users relative to the material on the network. However, each node will operate at its assigned protection level.

Controlled Interface

When information systems are networked, whether Unified or Interconnected, and the transmission leaves the facility, a controlled interface (CI) may be required.

A Controlled Interface:

- Is required for interconnected networks if needed to adjudicate different security implementations, classification levels and need-to-know
- Includes firewalls, high assurance guards and communication equipment like routers and bridges

Controlled Interface Functions

The functions of a CI include:

- Providing a secure interconnection between
  - Networks
  - Peripheral devices
  - Remote terminals
  - Remote hosts
- Providing a reliable exchange of security-related information
- Filtering information based on associated security labels for data content

Controlled Interface Characteristics

A CI has the following characteristics:

- No general users
- No user code running
- Supports the protection requirements of the most restrictive of the attached networks or IS
- Ensures that communication policies and connections that are not explicitly permitted are prohibited

Topic 2: Introduction to Securing Network Interconnections

In the previous topic, you learned that a network can be accredited either as a Unified network or as an Interconnected network. You also learned how Unified and Interconnected networks are configured.

In this topic, you will learn about the network requirements and accreditation procedures for Interconnected networks.

Reference: NISPOM 8-700

Network Information Systems Security Officer

When working within an Interconnected network, it is important to ensure that appropriate personnel are in place to assume responsibility for the system. This means that a Network ISSO must be appointed at the Host site that is responsible for overseeing the security of the network. He or she may be the ISSM for the facility or an ISSO for the network. DSS would expect the following from a Network ISSO:

- Ensuring that security measures are appropriate and in compliance with the NISPOM
- Serving as a focal point for network and connecting node ISSOs/ISSMs to include collecting Network Security Profiles and copies of accreditation letters.
- Generating a Network Security Plan and, if applicable, maintaining the Memorandum of Understanding (MOU)
- Ensuring all systems on the network have an accredited SSP.

Network ISSO duties also include:

- Developing and implementing network security procedures
- Ensuring weekly reviews of the host are performed and that only connections that are accredited and exhibited on a topology diagram are connecting to the host system
- Evaluating the impact of system and network changes and submit reaccreditation documentation when appropriate
- Reporting security violations and anomalies to the DAA(s)
- Maintaining a list of network users

Accreditation Requirements

Accreditation requirements and responsibilities for an Interconnected network are somewhat different

than for other networks.

When the network is a contractor-to-contractor network:

- Each connecting node is accredited by its respective DSS DAA
- The connecting contractors will establish which system will act as the host
- Appoint a Network ISSO for the network

Documentation

The Network ISSO submits the following documents to the host DSS Representative:

- SSP and certification statement for host system
- A Network Security Plan
- Network Security Profile for host system
- Connecting node(s) Network Security Profiles, topology diagram(s) and copy of accreditation letter(s) if available

Network Security Plan

Every Interconnected system is required to have a Network Security Plan in place. The Network Security Plan is a document that reflects how the Interconnected network will be managed and administered. The Network Security Plan makes the Interconnected network a unit. With the addition of each connection, the Network Security Plan must be revised and reaccredited. The Network Security Plan will include the following:

- Name of the Network ISSO
- Details of connections, to include remote workstations
- Procedures on how privileged and general users' accesses will be controlled

The following must also be addressed in the Network Security Plan:

- Type 1 encryption utilized, including auditing, if required
- A network topology diagram
- A description of any network protocols in use
- A description of the baseline for configuration of the routers
- All connection requirements appropriate to the PL of the network
- A Network Security Profile for the network host system and each connecting node, to include government connections

Network Security Profile

A network security profile is required for the host and every node. This security profile contains information about:

- Facility name and address
- Name and contact information of the ISSM
- Highest classification of data transmitted

The connecting node must provide the Network Security Profile to the Network ISSO, along with a topology diagram and copy of the accreditation letter for the node.

A network security profile provides acknowledgement from each contractor of the participation in the network and that the system is accredited. It is important that each participant know what the other participants have in the way of equipment and protection level(s).

Remember: The risk accepted by one is shared by all.

Network Cognizance

Who has cognizance?

The NISPOM identifies three environments in which classified information can be exchanged.

Communication can take place:

- Within a contractor's facility
- From contractor-to-contractor
- Between the Government and a contractor

Within a Contractor’s Facility

When communication is within a NISP contractor facility, DSS has cognizance. DSS ensures that the following requirements are met:

- The IS must be accredited
- Data must be protected during transmission through the use of :
  - A closed area
  - Encryption
  - Protected distribution system

Contractor-to-Contractor

When communication is from contractor-to-contractor, DSS has cognizance. DSS ensures that the following requirements are met:

- Each contractor must have accredited information system(s)

- Data must be encrypted (NSA Type 1) prior to transmission
- There must be a Network Security Plan

  The plan must include Network Security Profile(s)

When communication is from contractor-to-contractor, DSS and DAA(s) have specific responsibilities. DSS representative for host:

- Reviews the Network Security Plan
- Reviews Network Security Profiles

  Determines overall network protection level

DSS representative for remote site:

- Certifies local node
- Notifies host

DAA for the remote location accredits the local node. Host DSS Representative certifies the host site and entire network Host. DAA accredits the host site as well as the entire network.

Government-to-Contractor

When communication is between the Government and a contractor, DSS and the DAA of the Government connecting site have cognizance and the following requirements must be met:

- All parties must have an accredited IS
- Data must be encrypted (NSA Type 1) prior to transmission
- All parties must adhere to DoD Long-Haul Telecommunication Policy (DoD Directive 4640.13)
- An MOU is required

DoD Long-Haul Telecommunication Policy (DoD Directive 4640.13.)

DoD requires that all government long haul (i.e. off federal base, post, camp, station or office) communication requirements be sent to Defense Information Systems Agency (DISA) for a Defense Information Systems Network (DISN) determination.

In a Government-to-contractor environment, host responsibilities apply as follows:

- Network ISSO notifies other nodes of Government connection
- Network ISSO submits Network Security Plan and system profiles to their DSS Rep
- Host DSS Representative reviews the Network Security Plan and
- reviews all profiles for PL determination
- reviews the technical aspects of the connection

- Host DSS Representative obtains MOU and solution from DISA regarding DoD Long-Haul Telecommunications Policy
- Host DSS Representative certifies the network
- Host DAA accredits the network

Memorandum of Understanding

An MOU between the government activity and DSS is required by the NISPOM for all government-to-contractor connections to include connections over STU III, STE and Secure Data Devices. An MOU is not required for contractor-to-contractor connections.

The purpose of the MOU is to adjudicate the differences in requirements of different DAAs. Many government Program Offices have standard MOU formats that are routinely utilized for all connections. DSS will allow the use of these formats but may require some additional information to meet NISPOM requirements.

MOU formats

Whatever the format used, as a minimum the MOU must contain all of the following:

- Date of MOU
- Names of DAA and Network ISSO
- High-level description and usage of overall network
- Contract or program name
- Name of Facility, the Security POC and telephone number
- IS Name and number
- Highest classification of data
- Network Protection Level; minimum clearance level of users, categories and formal access approvals, if applicable
- Network type (Interconnected or Unified)
- Any Defense Information Systems Network (DISN) established by DISA (Defense Information Systems Agency)
- Statement that there is no further connection to any DISN other than the one(s) involved in the connection as outlined in the MOU
- Brief explanation that the government activity will oversee the government system and operate under applicable regulations and DSS will oversee the contractor system which will operate under the NISPOM
- It is also helpful to have a statement that the MOU will not be re-signed unless there is a change to the overall security of the network

Interconnected Network Accreditation

ISSMs must carefully monitor the system and make note of any changes that may occur. If a node changes:

- The node ISSM notifies the Network ISSO of the changes to the network
- The Network ISSO determines if reaccreditation is required

Reaccreditation

Depending on the issue(s) involved, reaccreditation of a node may or may not require network reaccreditation. If the node reaccreditation is due to an issue that does not affect the network, reaccreditations of the network are not required. ISSMs with self-certification may never self-certify an additional remote node to the network. If a node reaccreditation will affect security of the network or if another node is added to the network, then DSS must reaccredit the network.

Topic 3: Introduction to Securing Network Interconnections

Several conditions must be met before ISs and networks are Interconnected to ensure that the ISs or networks are able to communicate without reducing their inherent security.

In the previous lesson you learned about the requirements involved with accrediting Interconnected networks and the differing documentation needed. In this topic, Securing Network Interconnections, you will learn about several methods that can be used to ensure safe interconnectivity between Interconnected networks.

Reference: NISPOM 8-605

Securing Network Interconnection

The NISPOM identifies three primary methods for securing network interconnections.

- Closed areas
- Encryption devices
- Protected distribution systems

Closed Areas

In a Closed Area, all of the equipment comprising the network is contained within an approved closed area (e.g., a LAN -Unified network).

Encryption Devices

When classified information must be transferred outside an approved area, security measures are required to protect the data being transmitted. An approved method is the use of encryption devices.

Encryption devices must be National Security Agency (NSA) approved Type 1 and procedures to use Type 1 approved encryption devices must be included in the SSP. The contractor must also have a copy

of the doctrine for that device on hand, particularly if auditing of the device is required by NSA. A copy of most Type 1 encryption doctrines is available from the DSS ISSP.

Types of Encryption Devices

NSA approved Type 1 encryption devices include:

- STU-III (1910)
- Taclane
- STE-(ISDN)
- Fastlane
- NES
- Sectera
- KG84
- KIV 21

Note: This is not intended to be a comprehensive list. (For additional information, check with your IS Rep.)

Protected Distribution Systems

A Protected Distribution System (PDS) involves the protection of wire or fiber-optic systems that transmit unencrypted classified information through areas of lesser classification or control (discussed in Lesson 5)

Lesson Summary

In this lesson, you learned about the following:

- Types of networks

  In this topic, you learned about the different types of computer networks and interconnection methods. You learned about the components and architectures of LANs and WANs. You learned about accredited networks including Unified and Interconnected. Unified networks are accredited as a single entity with one SSP, issued a single letter of accreditation, accredited in a single security protection level, and directed by a single security policy. Interconnected networks are managed by a Network ISSO, composed of separately accredited ISs with their own SSPs, accredited at the network level through a Network Security Plan, and retain individual accreditations.

- Interconnected network requirements

  In this topic, you learned about network requirements and accreditation procedures for Interconnected networks. You learned that when working within an Interconnected network, appropriate personnel such as a Network ISSO must be appointed at the Host site that is responsible for overseeing the security of the network. You learned that every Interconnected system is required to have a Network Security Plan in place to describe how the Interconnected

network will be managed. You learned that a network security profile is required for the host and every node. A network security profile provides acknowledgement from each contractor of the participation in the network and that the system is accredited. You also learned that there are three environments in which classified information can be exchanged including within a contractor's facility, from contractor-to- contractor, and between the government and a contractor.

- Securing network interconnections

  In this topic, you learned about several methods that can be used to ensure safe interconnectivity between Interconnected networks. You learned about the three primary methods for securing network interconnections including closed areas, encryption devices, and protected distribution systems. In a closed area, all of the equipment comprising the network is contained within an approved closed area. You learned when classified information must be transferred outside an approved area, encryption devices or PDS are used to protect the data being transmitted. You also learned that a PDS involves the protection of wire or fiber-optic systems that transmit unencrypted classified information through areas of lesser classification or control.

Module 6: IS Administrative Inquiries

Lesson 1: Introduction to Administrative Inquiries

Government guidelines require that all classified information be protected against unauthorized disclosure. If you suspect classified information may have been disclosed to unauthorized individuals, you must conduct an Administrative Inquiry (AI).

You will learn when and how to conduct an Administrative Inquiry.

Reference: NISPOM 8-103 f(3)

Lesson Objectives

At the end of this lesson, you will be able to:

- Identify the definitions for loss, compromise, and suspected compromise of classified information
- Identify the administrative inquiry process

Topic 1: Introduction to Administrative Inquiries Overview

Maintaining IS security requires that sensitive information be protected at all times. If, in spite of the best protective measures, classified information is disclosed or believed to have been disclosed to individuals who are not authorized access to it, you must ensure that appropriate measures be taken.

In this topic, The Administrative Inquiry, you will be introduced to key terminology used when conducting an administrative inquiry.

Reference: NISPOM paragraphs 1-303 and 8-103 f(3)

What is an Administrative Inquiry?

Government guidelines mandate that classified information not be disclosed to any individual who is not authorized to access that information. Any suspected occurrence must be investigated and promptly reported to the appropriate authorities. This investigation and reporting process is known as an administrative inquiry (AI).

When is an Administrative Inquiry Required?

The NISPOM requires that an appropriate report be filed whenever it is suspected that classified information, foreign or domestic, has been:

- Lost,
- Compromised, or
- Suspected to have been compromised.

NISPOM

- NISPOM 1-302.l requires reporting of unauthorized receipt of classified material
- NISPOM 1-303 requires reporting of loss, compromise, or suspected compromise of classified information
- NISPOM 8-103.f.(3) requires that the ISSM reports security incidents to the CSA

Key Terms

When conducting an administrative inquiry, you must understand the distinction between loss, compromise, and suspected compromise, and use the appropriate term to identify the type of incident that has occurred. These terms are defined as follows:

- Loss refers to material that cannot be located within a reasonable time, or if the material is out of the custodian's control.
- Compromise occurs when classified information is disclosed to an unauthorized person.
- Suspected compromise occurs when disclosure cannot be reasonably precluded.
- No compromise is reserved for inquiries in which classified information may have been vulnerable to compromise but circumstances of the situation led the FSO/ISSM/IS Rep to reasonably conclude that either no unauthorized individual had access to the classified information, or that based on the facts of the inquiry, the possibility of access was extremely remote.

How Does Compromise Happen?

Classified material can be compromised in many different ways. For example, it can occur when there is:

- A change in classification level

- An unsecure transmission
- Accidental use of non-accredited equipment
- Intentional use of non-accredited equipment

Change in classification level

A change in classification level can occur when a government customer upgrades the sensitivity of information. Sometimes a new classification guide goes into effect, but is not supplied with the contract or, if supplied, is not properly reviewed.

Unsecure transmission

The most common way for an unsecure transmission to occur is when classified information is sent out without being encrypted (e.g., in an email). However, it can also occur during unattended network processing or when encryption devices are improperly operated, causing transmission in the clear.

Use of non-accredited equipment

Accidental use of non-accredited equipment can occur when someone puts classified information on non-accredited equipment without realizing the information is classified. The accident may be discovered later, when a worker in the company with experience in that subject realizes something on the system is classified. When classified information is processed on a non-accredited system it is referred to as a contamination.

Additional Examples

Compromises can also occur when:

- A user has the "track changes" feature enabled, but does not have the changes highlighted on the screen. When the document is printed, classified information that was thought to have been deleted can show up on the printed output.
- An unclassified file is extracted from a classified hard drive without following approved, trusted download procedures. More sophisticated word processing programs with undo features append the new data onto the end of files. If approved, trusted download procedures are not followed carefully, classified information can inadvertently be transferred to the unclassified media.
- Information is compiled. In some instances, certain information that would otherwise be unclassified (or classified at a lower level) when standing alone may require classification (or higher level classification) when combined or associated with other unclassified (or lower classified) information. This is why it is very important to understand the classification guidance.

Topic 2: Introduction to the Administrative Inquiry Process

In the previous topic, you learned to define loss, compromise, and suspected compromise of classified information.

In this topic, The Administrative Inquiry Process, you will learn how to conduct an administrative inquiry.

Reference: NISPOM paragraph 1-303

Conducting an Administrative Inquiry

All loss, compromise, or suspected compromise of classified information must be investigated and reported to Defense Security Service (DSS).

This requires that the following four-step process be followed:

- Step 1: Conduct a Preliminary Inquiry
- Step 2: Make an Initial Response
- Step 3: Conduct a Thorough Investigation
- Step 4: Write a Final Report

Step 1: Conduct a Preliminary Inquiry

As soon as a loss, compromise, or suspected compromise of classified information is reported, the contractor must initiate a preliminary inquiry. The purpose of this inquiry is to:

- Identify the "Who, What, When, Where, Why, and How" of the incident
- Determine if a loss, compromise, or suspected compromise has indeed occurred
- Determine the extent of the loss, compromise, or suspected compromise
- If a no compromise determination is made , a record of that determination must be kept for an assessment by the IS Rep at the next review

Submit Initial Report

If the contractor's preliminary inquiry confirms a loss, compromise, or suspected compromise of any classified information, the contractor must promptly submit an initial report to the IS Rep.

Step 2: Make an Appropriate Initial Response

If it is established that a contamination has occurred resulting in the loss, compromise, or suspected compromise of classified information, security personnel must:

- Physically isolate and protect all contaminated equipment
- Remove all unauthorized individuals from the area
- Ensure that data is NOT deleted because it makes it harder to find it to overwrite and sanitize.
- Call the Facility Security Officer (FSO)
- Contact the ISR/ISSP for instructions on how to proceed with cleanup. DSS will help identify how to sanitize all infected systems and prevent other systems from being contaminated.

Step 3: Conduct a Thorough Investigation

After the information has been secured and the cleanup completed, a more thorough investigation should be conducted. This involves:

- Gathering and reviewing all audit trails. The audit trails reflect who has been on the system in the period under review. This will help identify who might have been involved in the incident.
- Interviewing all individuals known to have been involved. Don't limit the interviews to only the users on the system since there may have been others indirectly involved.

Step 4: Write a Final Report

After the investigation has been completed, the contractor must write and submit a final report. (See NISPOM 1-303 for specific guidance in preparing this report.)

Follow Available Guidance

All available guidance should be followed as the inquiry is completed. This includes:

- NISPOM AI report requirements (NISPOM 1-303 and 304)
- General Administrative Inquiry Guidance
- Guidelines for Conducting an AI Involving a Non-accredited System
- Clearing and Sanitization Matrix at the DSS IA webpage

What to Identify

The following must be identified:

- Each component of the system that potentially contains classified information
- Whether the data was encrypted and what commercial encryption algorithms were used
- The platforms and OSs involved
- The type of email system involved (if appropriate)
- Any other network connections

Additional Suggestions

The following should not be overlooked:

- Home based computers/remote dial-ins
- Backup tapes
- Connecting systems

- Remote storage locations
- Printers/print servers
- Reproduction equipment/services

Any or all of the equipment above could contain information that may be of use for the investigation; these system components may also need to be cleared or sanitized.

In the case of classified material being upgraded, the contractor's written notice[35] shall not be classified unless the notice contains additional information warranting classification. In the case of material which was inadvertently released as Unclassified, the contractor's written notice shall be classified Confidential, unless it contains additional information warranting a higher classification. The ISSM must use secure communications (e.g., STE) if their conversations reveal detailed specific information[36].

Lesson Summary

In this lesson, you learned about the following:

- Administrative Inquiries

  In this topic, you learned about administrative inquiries and how to determine when one is required. You also learned about key terminology used when conducting administrative inquiries and the different ways that classified material can be compromised.

- Administrative Inquiry Process

  In this topic, you learned how to conduct an administrative inquiry through a four-step process which includes:

  Conducting a preliminary inquiry,

  Making an initial response,

  Conducting a thorough investigation, and

  Writing a final report.

  You also learned what to identify during the investigation and the specific types of equipment that should not be overlooked.

1
Contractors

Contractor refers to a company that has been awarded a classified contract to work for the US Government.

2
Designated Approving Authority

Within the NISP, the Designated Approving Authority (DAA) is the government official with the authority to formally accredit operation of the contractor's complex information systems.

3
External

External threats come from individuals or groups of people who are outside the organization being threatened (for example, an unauthorized user who attempts to break into an organization's computer network).

4
Internal

Internal threats come from individuals who are a part of the organization (for example, a disgruntled employee who removes, deletes or changes sensitive information stored on an organization's information system).

5
Bombs

Logic bomb
A resident computer program that triggers an unauthorized act when particular states of an information system (IS) are realized.
Time bomb
A resident computer program that triggers an unauthorized act at a predefined time.

6
Well-known worms

Well-known worms include, for example, Blaster, Slammer, and Code Red worms.

7
New Products

Examples of new products include small, portable storage devices, recording and key stroke capturing devices, thumb drives, and wireless devices.

8
New Technologies

Examples of new technologies include mass storage devices, miniaturization, imaging technology and wireless technology advances.

9
Signs of malicious logic contamination

Malicious logic can spread quickly throughout an entire system, so it is important to recognize and respond quickly to signs of contamination. The user should be on the look-out for any of the following signs: The date or time stamp on files changes; Operations slow or cease; Files are damaged or become inaccessible; Frequent, unexpected messages appear on the screen; The computer reboots unexpectedly or crashes frequently; Hard drive space or memory decreases

10
Confidentiality

Confidentiality is assurance that information is not disclosed to unauthorized entities or processes.

11
Integrity

Integrity is protection against unauthorized modification or destruction of information.

12
Availability

Availability is timely, reliable access to data and information services for authorized users.

13
Level of Concern

Level of Concern for Confidentiality translates to classification levels Basic=Confidential, Medium=Secret, and High=Top Secret

14
Formal Access Approvals

Formal access approval refers to a type of classified information that requires formal signed briefings prior to access and formal signed debriefings when access is no longer required. Under NISPOM, this includes NATO, CNWDI, and CRYPTO (COMSEC keying material used to secure or authenticate telecommunications carrying classified US Government information.).

15
Protection Profile

A protection profile is a description of an implementation-independent set of security requirements for a family or category of protection levels.

16
Unique threat

Example: A number of researchers at a cleared university are granted personnel security clearances to work on DoD contracts. There is a large population of foreign students at the university who have free access to the rooms and hallways surrounding the cleared researcher's offices and labs.

17
Vulnerability

Example: It is discovered that the operating system does not record all instances of successful and unsuccessful user log offs as required by paragraph 8-602a.

18
Trusted Downloading

Trusted downloading involves the downloading of unclassified or lower classified information to lower or unclassified media. If this needs to occur, go to http://www.dss.mil/infoas/index.htm for DSS Trusted Downloading standards.

19
NSA Type 1 Encryption Device

Examples include STU-III, STE, NES, KG-84, Taclane, Fastlane, KIV-21. For a complete listing of currently approved devices contact your IS Rep.

20
Self-Certify

Self-certification refers to the ability of the ISSM, rather than DSS, to certify additional systems in accordance with the SSP for classified processing.

21
Write-protected

Write-protected media must be tested once per session, as long as the system is continuously up and "session" is clearly defined and appropriately reflected in the SSP as being for each user, per day.

22
Hard Copy Output

Hard copy output can include: Paper; Fiche; Film; and Other printed material

23
Knowledgeable Personnel

A knowledgeable person is someone who is familiar with the classification requirements and security classification guides as well as the vulnerabilities of different types of electronic formats.

24
Transferred

When multiple files are transferred, a new folder/directory/subdirectory should be set up to retain files for review prior to transfer. The files transferred to the new media must be reviewed to ensure that only the lower classified or unclassified information that was intended to be moved was moved. The knowledgeable reviewer must also ensure the compilation of all files transferred to the new media does not increase the classification level.

25
Hex Editor Software

A program that displays every character in a file in hexadecimal notation. Software that allows examination of every byte in a file (e.g., hex editor software) should be used on all files.

26
Alternate

Using formats other than the limited formats approved by DSS and/or using processes that differ from the DSS approved procedures.

27
In Use controls

Individuals shall be responsible for safeguarding classified information in their custody or under their control. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise.

28
Hashed

An algorithm that turns a variable sized amount of text into a fixed-sized output.

29
Another method

Another method might include posting a sign with the appropriate language near the IS or in the user audit log.

30
Time delay control system

Some operating systems provide a mechanism that will lock out a user for a specified time period (e.g., 30 minutes) after some number (maximum 5) of consecutive unsuccessful access attempts.

31
Group authenticator

A group authenticator allows a group of people to use the same ID and password to access an IS.

32
Audit Trails

Audit trails generally refer to automated auditing of system activities.

33
Audit Records

Audit records encompass manual logs, automated audit trails and manual auditing.

34
Verify

One method to verify this is by using JPAS (Joint Personnel Adjudication System). Another is through email with nonrepudiation.

35
Notice

The notice shall cite the applicable Contract Security Classification Specification or other classification guide on the “Derived From” line and be marked with an appropriate declassification instruction.

36
Specific information

Examples of specific information are file names, date/time, groups on message headers, etc., when the system is still contaminated.