**CNSS Instruction No. 4012**
**June 2004**


# National Information Assurance Training Standard For Senior System Managers

*Awareness, Training and Education (AT&E) are cost-effective methods of improving organizational Information Assurance (IA). In times of ever-contracting budgets, it is difficult to persuade management to spend money on security and training activities that have no direct impact on the organizational bottom line. This paper describes the process used to aid in the systematic development of training to serve as the first line of defense in Information Assurance (IA). In addition it describes how these materials are applicable to your organizational long-range plans.*

This document provides minimum standards for senior managers of national security systems. It also may offer guidelines for senior managers of unclassified systems. Your department or agency may require a more stringent implementation.

**COMMITTEE ON NATIONAL SECURITY SYSTEMS**

**NATIONAL MANAGER**

## FOREWORD

1. Since the September 11th terrorist attacks against the sovereignty of the United States and its people, both the President and the Congress have redoubled their efforts to underpin the nation's security. The following guidance, reflecting their support, is intended to assist all federal agencies and private sector concerns in protecting their information systems. Only through diligence and a well-trained workforce will we be able to adequately defend the nation's vital information resources.

2. CNSSI No. 4012 is effective upon receipt. It replaces the National Training Standard for Designated Approving Authority (DAA), dated August 1997, which should be destroyed.

3. This instruction establishes the minimum course content or standard for the development and implementation of Information Assurance (IA) training for Senior Systems Managers (SSMs) of national security systems. Please check with your agency for applicable implementing documents.

4. Additional copies of this instruction can be obtained on the CNSS Website www.cnss.gov or by contacting the office at the address below:

NATIONAL SECURITY AGENCY
CNSS SECRETARIAT
ATTN: I01C STE 6716
FORT GEORGE G. MEADE, MD 20755-6716

/s/

MICHAEL V. HAYDEN
Lieutenant General, USAF

# SENIOR SYSTEMS MANAGERS

NATIONAL IA TRAINING STANDARD FOR SENIOR SYSTEMS MANAGERS (SSMs)



## SECTION I – PURPOSE

1. This instruction establishes the minimum standard for the development and implementation of Information Assurance (IA) training for Senior Systems Managers (SSM), *viz*., Chief Information Officer (CIO), Designated Approving Authority (DAA), Chief Technology Officer (CTO), etc.

## SECTION II – APPLICABILITY

2. The President's National Strategy to Secure Cyberspace, Feb 03; National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501, 16 Nov 92, and Federal Information Security Management Act (FISMA), 17 Dec 02, establish the requirements for federal departments and agencies to implement training programs for IA professionals. As defined in NSTISSD 501, an IA professional is an individual responsible for the security oversight or management of national security systems throughout all life-cycle phases. Those directives and others are being implemented in a synergistic environment among departments and agencies, which are committed to satisfying vigorously these IA education and training requirements. The following document is a continuation in a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (CNSSI "old NSTISSI" Nos. 4011, 4013, 4014, 4015, and 4016). Implementing the training outlined in this document concomitantly will fulfill IA training requirements articulated in NIST Special Publication (SP) 800-16, and 5 Code of Federal Regulations (CFR) Part 930. The definitions for words used in this instruction are derived from the National Information Assurance (IA) Glossary, CNSSI No. 4009. Many references pertinent to this instruction may be found in ANNEX B.

3. The body of knowledge listed in this instruction was obtained from a variety of sources; *i.e.*, industry, government, and academia. ANNEX A lists the minimal IA performance standard for a SSM.

4. This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the development and implementation of IA training for SSMs.

## SECTION III – RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure that SSMs, *viz*., CIOs, DAAs, CTOs, etc., are trained to the level of proficiency outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

6. The National Manager shall:

a. maintain and provide an IA training standard for SSMs to U.S. Government departments and agencies;

b. ensure that appropriate IA training courses for SSMs are developed;

c. assist other U.S. Government departments and agencies in developing and/or conducting IA training activities for SSMs as requested; and

d. maintain a national clearinghouse for training and education materials.

Enclosures:
ANNEX A
ANNEX B

# ANNEX A

MINIMAL INFORMATION ASSURANCE (IA) PERFORMANCE STANDARD FOR SENIOR SYSTEMS MANAGERS (SSMs)

Job functions using competencies identified in:

- NSTISSI 1000, National Information Assurance Certification and Accreditation Process (NIACAP)
- NCSC-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities For Automated Information Systems
- NCSC-TG-029, Version 1, Introduction to Certification and Accreditation
- FIPS Publication 102, Guideline for Computer Security Certification and Accreditation
- DODD 8000.1, Management of DoD Information Resources and Information Technology
- DODD 8500.1, Information Assurance
- DODI 8500.2, Information Assurance Implementation

## TERMINAL OBJECTIVE:

Given a final report requesting approval to operate an information system at a specified level of trust, the SSM will analyze and judge the information for validity and reliability to ensure the system will operate at the proposed level of trust. This judgment will be predicated on an understanding of system architecture, system security measures, system operations policy, system security management plan, legal and ethical considerations, and provisions for system operator and end user training.

## GENERAL BACKGROUND

The following items constitute a basic literacy necessary for Senior Systems Managers to proceed through the course material.

| Definitions for SSMs | |
|---|---|
| Access authorization | Key management infrastructure |
| Access control policies | Law enforcement interfaces |
| Access controls | Law enforcement policies |
| Access controls – discretionary | Legal and liability issues as they apply to mission |
| Access controls – mandatory | Legal issues and Information Assurance (IA) |
| Access privileges | Legal issues which can affect Information Assurance (IA) |
| Accountability for sensitive data | Legal responsibilities of the SSM |
| Accreditation | Liabilities associated with disclosure of sensitive information |
| Accreditation procedure | Licensing |
| Accreditation types | Life cycle management |
| Administrative security policies | Life cycle security planning |
| Administrative security procedures | Life cycle system security planning |
| Aggregation | Logging policies |
| Approval to Operate (ATO) purpose and contents | Marking classified/sensitive information |
| Assignment of individuals to perform information assurance functions | Memorandum of Understanding/Agreement |
| Attacks | Methods of implementing risk mitigation strategies necessary to obtain ATO |
| Audit trail policy | Millennium Copyright Act |
| Auditable events | National Archives and Records Act |
| Automated countermeasures/deterrents | Need-to-know controls |
| Automated security tools | Non-repudiation |
| Availability (McCumber) | Operations Security |
| Background investigations | Organizational – threats |
| Backups | Organizational/agency information assurance emergency response teams |
| Biometric policies | Organizational/agency information assurance emergency response team role |
| Biometrics | Paperwork Reduction Act as codified in 44 U.S.C.A. Section 3501 |
| Budget | Personnel security |
| Business recovery | Personnel security guidance |
| Certification | Personnel security policies |
| Certification and Accreditation effort leading to Systems Security Authorization Agreement | PKI |
| Certification and Accreditation process policy | Principles of aggregation |
| Certification procedure | Principles of information ownership |
| Certification roles | Principles of risk |
| Certification tools | Principles of system reconstitution |
| Certifiers understanding of mission | Privacy Act |
| Change control | Problems associated with disclosure of sensitive information |

| | |
|---|---|
| Clinger-Cohen Act | Procedural/administrative countermeasures |
| Commercial proprietary information | Protection profiles |
| Commercial proprietary information protection | Purpose of Systems Security Authorization Agreement (SSAA) |
| Common Criteria (Product Assurance) role in acquiring systems | Recertification |
| Communications Security (COMSEC) materials | Recertification effort |
| Computer crime and the various methods | Recertification of systems characteristics that need review |
| Computer Fraud and Abuse Act as codified in 18 U.S.C.A. Section 1030 | Recertification process |
| Confidentiality (McCumber) | Recertification purpose |
| Configuration management | Reconstitution |
| Connected organizations | Recovery plan |
| Connectivity involved in communications | Remanence |
| Concept of Operations (CONOPS) | Residual risk |
| Contingency planning | Resources |
| Continuity of operations | Responsibilities associated with accreditation |
| Contracting for security services | Restoration |
| Copyright Act of 1976 and Copyright Amendment Act of 1992 as codified in 17 U.S.C.A | Restoration and continuity of operation |
| Copyright protection and license | Restoration process |
| Countermeasures | Results of certification tools |
| Countermeasures/deterrents – automated | Risk |
| Countermeasures/deterrents – technical | Risk acceptance |
| Criminal prosecution | Risk acceptance process |
| Declassification of media | Risk analysis |
| Delegation of authority | Role of risk analyst |
| Disaster recovery | Risk assessment |
| Disposition of classified material | Risk assessment as it supports granting waiver |
| Documentation | Risk assessment supporting granting an IATO |
| Documentation policies | Risk in certification and accreditation |
| Documentation role in reducing risk | Risk management |
| Downgrade of media | Risk mitigation |
| Due diligence | Risk mitigation strategies |
| Education, training, and awareness as a countermeasure | Risk mitigation strategies necessary to obtain IATO |
| Electronic emanations | Risk reports |
| Electronic records management | Risks associated with portable wireless systems, *viz*., PDAs *etc*. |
| Electronic-mail security | Risks from connectivity |
| Emergency destruction | Security Test, and Evaluation (ST&E) as part of acquisition process |
| Emergency destruction procedures | Separation of duties |
| Emissions Security (EMSEC) | Service Provider Exemption to the Federal Wiretap Statute [18 U.S.C.A. Section 2511(2)(a)(i)-(ii)] |
| Ethics | Storage (McCumber) |
| Evidence collection | System accreditors role |
| Evidence collection policies | System architecture |
| Evidence preservation | System certifiers role |

| | |
|---|---|
| Evidence preservation policies | System disposition |
| Execution of memoranda of understanding | System reutilization |
| Facilities planning | System security architecture |
| Federal Information Security Management Act (FISMA) | System security architecture support of continuity of operations (CONOPS) |
| Federal Property and Administration Service Act | Systems Security Authorization Agreement (SSAA) |
| Federal Records Act | TEMPEST failures |
| Fraud waste and abuse | TEMPEST requirements |
| Freedom of Information Act (FOIA) and Electronic Freedom of Information Act (EFOIA) | Test and evaluation |
| Government Information Security Reform Act (GISRA) | Threat |
| Government Paperwork Elimination Act (GPEA) | Threat analysis |
| Importance and role of non-repudiation | Threats – assessment |
| Importance and role of PKI | Threats – environmental |
| Importance of Security Test and Evaluation (ST&E) as part of acquisition process | Threats – human |
| Incident response | Threats – natural |
| Incident response policy | Threats from contracting for security services |
| Information Assurance (IA) | Threats to systems |
| Information assurance – SSM role | Transmission (McCumber) |
| Information assurance budget | Types of contracts for security services |
| Information assurance business aspects | Vulnerability |
| Information assurance cost benefit analysis | Vulnerability – aggregation |
| Information classification | Vulnerability – connected systems |
| Information ownership | Vulnerability – improper disposition |
| Information security policy | Vulnerability – improper reutilization |
| Interim approval to operate (IATO) | Vulnerability – network |
| Investigative authorities | Vulnerability – technical |
| Justification for waiver | Vulnerability – wireless technology |

In each of the areas listed below, the SSM shall perform the following functions:

## FUNCTION ONE - GRANT FINAL ATO

Granting final approval to operate an IS or network in a specified security mode

### A. RESPONSIBILITIES

1. Aspects of Security
   - Explain the importance of SSM role in Information Assurance (IA)
2. Accreditation
   - Discuss accreditation
   - Discuss the certification process leading to successful accreditation
   - Explain the importance of accreditation
   - Explain types of accreditation
   - Facilitate the certification process leading to successful accreditation
   - Discuss the significance of NSTISSP No. 6

### B. APPROVALS

1. Approval to Operate (ATO)
   - Explain ATO
   - Discuss purpose and contents of ATO
   - Explain the importance of risk assessment to support granting an ATO
2. Interim Approval to Operate (IATO)
   - Describe IATO
   - Explain the purpose and contents of IATO
   - Explain the importance of risk assessment to support granting an IATO
   - Facilitate implementation of risk mitigation strategies necessary to obtain IATO
3. Recertification
   - Describe recertification
   - Direct the recertification effort
   - Explain the importance of the recertification process
   - Identify characteristics of information systems that need re-certification
   - Initiate the recertification effort
4. Systems Security Authorization Agreement (SSAA)
   - Discuss the Systems Security Authorization Agreement (SSAA)
   - Explain the importance of the SSAA
5. Waive Policy to Continue Operation
   - Discuss justification for waiver
   - Discuss risk mitigation strategies necessary to obtain waiver
   - Ensure risk assessment supports granting waiver

## FUNCTION TWO - REVIEW ACCREDITATION

Reviewing the accreditation documentation to confirm that the residual risk is within acceptable limits for each network and/or IS.

### A. THREATS

1. Attacks
   - Discuss threats/attacks to systems
   - Explain the importance of threats/attacks on systems
2. Environmental/Natural Threats
   - Discuss environmental/natural threats
3. Human Threats
   - Explain the importance of intentional and unintentional human threats
4. Theft
   - Explain the importance of theft
5. Threat
   - Explain threat
   - Explain the importance of organizational threats
6. Threat Analysis
   - Explain the importance of threat analysis
7. Threat Assessment
   - Explain the importance of threat assessment

### B. COUNTERMEASURES

1. Education, Training, and Awareness as Countermeasures
   - Explain the importance of educational training, and awareness as countermeasures
   - Ensure educational training, and awareness countermeasures are implemented
2. Procedural Countermeasures
   - Explain the importance of procedural/administrative countermeasures
   - Ensure procedural/administrative countermeasures are implemented
3. Technical Countermeasures
   - Explain the importance of automated countermeasures/deterrents
   - Explain the importance of technical countermeasures/deterrents
   - Ensure technical/automated countermeasures/deterrents are implemented

### C. VULNERABILITY

1. Vulnerability
   - Explain vulnerability
2. Vulnerability Analysis
   - Explain the importance of vulnerability analysis

3. Network Vulnerabilities
   - Explain the importance of network vulnerabilities
4. Technical Vulnerabilities
   - Explain the importance of technical vulnerabilities

### D. RISK MANAGEMENT

1. Cost/Benefit Analysis of Information Assurance
   - Explain the importance of cost/benefit analysis of information assurance
2. Documentation
   - Explain the importance of documentation role in reducing risk
3. Risk
   - Explain risk
   - Discuss principles of risk
4. Risk Assessment
   - Explain the importance of risk assessment
5. Risk Management
   - Explain the importance of risk management
6. Residual Risk
   - Explain residual risk
7. Risk Acceptance Process
   - Explain the importance of the risk acceptance process
8. Systems Security Authorization Agreement (SSAA)
   - Explain the importance of the certification and accreditation (C&A) effort leading to accreditation
   - Discuss the contents of SSAA
   - Discuss the purpose of SSAA
   - Ensure the certifier understands the mission and it is reflected in SSAA the C&A effort leading to SSAA
   - Facilitate effort leading to SSAA

## FUNCTION THREE - VERIFY COMPLIANCE

Verifying that each information system complies with the information assurance (IA) requirements

### A. LAWS RELATED TO INFORMATION ASSURANCE (IA) AND SECURITY

1. Copyright Protection and Licensing
   - Explain the importance of copyright protection
   - Explain the importance of licensing
2. Criminal Prosecution
   - Explain the importance of criminal prosecution
3. Due Diligence
   - Explain the importance of due diligence

4. Evidence Collection and Preservation
   - Explain the importance of evidence collection
   - Explain the importance of evidence preservation
5. Fraud, Waste, and Abuse
   - Explain fraud, waste, and abuse
6. Laws Related To Information Assurance and Security
   - Explain the importance of implications of Electronic Records Management and Federal Records Act
   - Explain the importance of implications of Federal Managers Financial Integrity Act of 1982
   - Explain the importance of implications of Federal Property and Administration Service Act
   - Explain the importance of implications of USA Patriot Act, GPEA, and Paperwork Reduction Acts
   - Explain the importance of implications of legal issues which can affect Information Assurance (IA)
   - Explain the importance of implications of National Archives and Records Act
   - Explain the importance of implications of the Computer Fraud and Abuse Act, P.L. 99- 474, 18 U.S. Code 1030
   - Explain the importance of implications of the Freedom of Information Act and Electronic Freedom of Information Act
   - Explain the importance of Public Law 107-347, E-Government Act 0f 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 02
   - Explain the importance of implications of the legal responsibilities of senior systems managers.
   - Explain the importance of implications of the Privacy Act
   - Discuss implications of Public Law 107-347 regarding certification and accreditation
7. Legal and Liability Issues
   - Explain the importance of legal and liability issues as they apply to system and mission
8. Ethics
   - Discuss ethics

## B. POLICY DIRECTION

1. Access Control Policies
   - Explain the importance of access control policies
2. Administrative Security Policies And Procedures
   - Explain the importance of administrative security policies/procedures
3. Audit Trails and Logging Policies
   - Explain the importance of audit trail policy
   - Explain the importance of logging policies
4. Documentation Policies
   - Explain the importance of documentation policies
5. Evidence Collection and Preservation Policies
   - Explain the importance of evidence collection/preservation policies

6. Information Security Policy
   - Define information security policy
   - Explain the importance of information security policy
7. National Information Assurance (IA) Certification & Accreditation (C&A) Process Policy
   - Explain the importance of the National Information Assurance (IA) Certification & Accreditation (C&A) Policy
8. Personnel Security Policies & Guidance
   - Explain the importance of personnel security guidance

## C. SECURITY REQUIREMENTS

1. Access Authorization
   - Explain the importance of access authorization
2. Auditable Events
   - Explain auditable events
3. Authentication
   - Explain authentication
4. Background Investigations
   - Explain the importance of background investigations
5. Countermeasures
   - Explain the importance of countermeasures
6. Delegation of Authority
   - Discuss the importance of delegation of authority
   - Ensure that individuals are assigned to perform IA functions
7. Education, Training, and Awareness
   - Explain the importance of education, training, and awareness as countermeasures
   - Ensure educational, training, and awareness countermeasures are implemented
8. Electronic Records Management
   - Discuss electronic records management
   - Explain the importance of electronic records management
9. Electronic-Mail Security
   - Discuss electronic-mail security
   - Explain the importance of electronic-mail security
10. Information Classification
    - Discuss information classification
    - Explain the importance of information classification
11. Investigative Authorities
    - Discuss investigative authorities
    - Explain the importance of investigative authorities
12. Key Management Infrastructure
    - Discuss key management infrastructure
13. Information Marking
    - Discuss information marking

14. Non-repudiation
    - Discuss non-repudiation
    - Explain the importance and role of non-repudiation
15. Public Key Infrastructure (PKI)
    - Explain the importance and role of PKI

## FUNCTION FOUR - ENSURE ESTABLISHMENT OF SECURITY CONTROLS

Ensuring the establishment, administration, and coordination of security for systems that agency, service, or command personnel or contractors operate

### A. ADMINISTRATION

1. Accountability for Classified/Sensitive Data
    - Explain the importance of accountability for sensitive data
    - Discuss classification and declassification of information
2. Automated Security Tools
    - Explain the importance of automated security tools
3. Backups
    - Discuss backups
    - Explain the importance of backups
4. Change Control/Configuration Management
    - Discuss change control
    - Discuss configuration management
    - Explain the importance of configuration management
5. Declassification/Downgrade of Media
    - Explain the importance of downgrade of media
    - Discuss the importance of downgrade of information
6. Destruction/Purging/Sanitization of Classified/Sensitive Information
    - Explain the importance of destruction/purging/sanitization procedures for classified/sensitive information

### B. ACCESS

1. Access Controls
    - Define manual/automated access controls
    - Explain the importance of manual/automated access controls
2. Access Privileges
    - Explain the importance of access privileges
3. Discretionary Access Controls
    - Discuss discretionary access controls
    - Explain the importance of discretionary access controls
4. Mandatory Access Controls
    - Define mandatory access controls
    - Explain the importance of mandatory access controls

5. Biometrics/Biometric Policies
   - Explain biometric policies
6. Separation of Duties
   - Define the need to ensure separation of duties where necessary
   - Explain the importance of the need to ensure separation of duties where necessary
7. Need-To-Know Controls
   - Define need to know controls
   - Explain the importance of need to know controls

## C. INCIDENT HANDLING AND RESPONSE

1. Emergency Destruction Procedures
   - Explain the importance of emergency destruction procedures
2. Organizational/Agency Information Assurance Emergency Response Teams
   - Explain the role of organizational/agency information assurance emergency response teams

## D. CONTINUITY OF OPERATIONS PLANNING

1. Business Recovery
   - Define business recovery
   - Explain the importance of business recovery
2. Contingency/Continuity of Operations Planning
   - Explain the importance of contingency/continuity of operations planning
   - Ensure the establishment and testing of contingency/continuity of operations plans
3. Disaster Recovery
   - Explain the importance of disaster recovery
4. Disaster Recovery Plan
   - Explain the importance of recovery plan
   - Ensure the establishment and testing of recovery plans
5. Incident response policies
   - Explain the importance of incident response policy
6. Law enforcement interfaces/policies
   - Discuss law enforcement interfaces
   - Discuss law enforcement policies
   - Explain the importance of law enforcement interfaces
7. Reconstitution
   - Define principles of system reconstitution
   - Explain the importance of principles of system reconstitution
8. Restoration
   - Explain the importance of restoration to continuity of operation

## FUNCTION FIVE - ENSURE PROGRAM MANAGERS DEFINE SECURITY IN ACQUISITIONS

Ensuring that the Program Manager/Official defines the system security requirements for acquisitions

### A. ACQUISITION

1. Certification Test & Evaluation (CT&E)
   - Define CT&E as part of acquisition process
   - Discuss the importance of CT&E as part of acquisition process
2. Certification Tools
   - Discuss significance/results of certification tools
3. Product Assurance
   - Explain the importance of product assurance role in acquiring systems, *i.e.*, NSTISSP No. 11, Jan 00
   - Explain the importance of protection profiles
   - Explain the importance of security targets
4. Contracting For Security Services
   - Discuss types of contracts for security services
   - Define where contracting for security services is appropriate
   - Explain threats from contracting for security services
5. Disposition of Classified Material
   - Discuss disposition of classified materials
   - Explain the importance of the correct disposition of classified material
   - Explain the importance of remanence
6. Facilities Planning
   - Discuss facilities planning
   - Explain the importance of facilities planning
7. System Disposition/Reutilization
   - Explain the importance of vulnerabilities from improper disposition/reutilization

### B. LIFE CYCLE MANAGEMENT

1. Life Cycle System Security Planning
   - Discuss life cycle security planning
   - Explain the importance of life cycle system security planning
2. System Security Architecture
   - Discuss system security architecture
   - Explain how system security architecture supports continuity of operations CONOPS

## FUNCTION SIX - ASSIGN RESPONSIBILITIES

Assigning Information Assurance (IA) responsibilities to the individuals reporting directly to the SSM

1. Certification and Accreditation (C&A)
   - Discuss responsibilities associated with accreditation
   - Discuss roles associated with certification
   - Explain importance of certification and accreditation (C&A)
   - Facilitate the C&A process
2. Information Ownership
   - Explain the importance of establishing information ownership
3. System Certifiers and Accreditors
   - Discuss risk as it applies to certification and accreditation
4. Risk Analysts
   - Discuss risk analyst's reports
   - Discuss systems certifiers and accreditors in risk mitigation
5. Information System Security Manager (ISSM)
   - Define the role of Information Assurance Manager (ISSM)
6. Information System Security Officer (ISSO)
   - Define the role of System Security Officer (ISSO)

## FUNCTION SEVEN - DEFINE CRITICALITY AND SENSITIVITY

Defining the criticality and classification/sensitivity levels of each IS and approving the classification level required for the applications implemented on them

1. Aggregation
   - Explain the importance of the vulnerabilities associated with aggregation
2. Disclosure of Classified/Sensitive Information
   - Explain the liabilities associated with disclosure of classified/sensitive information

## FUNCTION EIGHT - ALLOCATE RESOURCES

Allocate resources to achieve an acceptable level of security and to remedy security deficiencies

1. Resource Roles and Responsibilities
   - Discuss the respective roles and responsibilities of resource management staff
   - Assign/appoint key resource managers

2. Budget/Resource Allocation
   - Evaluate the information assurance budget
   - Explain the importance of the information assurance budget
   - Defend the budget for information assurance
3. Business Aspects of Information Security
   - Discuss business aspects of information security
   - Discuss protection of commercial proprietary information
   - Explain the importance of business aspects of information security
   - Explain the importance of protecting commercial proprietary information

## FUNCTION NINE - MULTIPLE AND JOINT ACCREDITATION

Resolve issues regarding those systems requiring multiple or joint accreditation. This may require documentation of conditions or agreements in Memoranda of Agreement (MOA); and

1. Memoranda of Understanding/Agreement (MOU/MOA)
   - Explain the importance of MOU/MOA
   - Facilitate development and execution of MOU/MOA

## FUNCTION TEN - ASSESS NETWORK SECURITY

Ensure that when classified/sensitive information is exchanged between IS or networks (internal or external), the content of this communication is protected from unauthorized observation, manipulation, or denial

1. Connectivity
   - Discuss connected organizations
   - Discuss connectivity involved in communications
   - Explain the importance of connectivity involved in communications
2. Emissions Security (EMSEC) and TEMPEST
   - Define TEMPEST requirements
   - Discuss threats from Emissions Security (EMSEC)
   - Discuss threats from TEMPEST failures
   - Explain the importance of the threats from Emissions Security (EMSEC)
   - Explain the importance of the threats from TEMPEST failures.
3. Wireless Technology
   - Discuss electronic emanations
   - Discuss threats from electronic emanations
   - Explain the importance of wireless technology
   - Explain the risks associated with portable wireless systems, *viz*., PDAs, *etc*.
   - Explain the importance of vulnerabilities associated with connected systems wireless technology

## ANNEX B

## REFERENCES

The following references pertain to this instruction:


1. Common Criteria for Information Technology Security Evaluation, dtd Aug 99
2. DOD Directive 8000.1, Management of Information Resources and Information Technology, dtd 27 Feb 2002, *etc*.
3. DoD Directive 8500.1, Information Assurance, dtd 24 Oct 2002
4. DoD Directive 8500.1-M, Information Assurance Manual, (when effective)
5. DoD Instruction 8500.2, Information Assurance (IA) Implementation, dtd 6 Feb 2003
6. DOD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), dtd 30 Dec 1997
7. DoD 8510.1M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, dtd 31 Jul 2000
8. EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, dtd 3 Apr 1984
9. E O 13231, Critical Infrastructure Protection in the Information Age, dtd 16 Oct 2001 as amended by EO 13286, Transfer of Certain Functions to the Secretary of Homeland Security, dtd 28 Feb 2003
10. Federal Information Processing Standards Publication (FIPS) Publication 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, dtd Jun 1974
11. Federal Information Processing Standards Publication (FIPS) Publication 65, Guideline for Automatic Data Processing Risk Analysis, dtd 1 Aug 1993
12. Federal Information Processing Standards Publication (FIPS) 87, Guidelines for ADP Contingency Planning, dtd 27 Mar 1981
13. Federal Information Processing Standards Publication (FIPS) Publication 102, Guideline for Computer Security Certification and Accreditation, dtd 27 Sep 1983
14. National Computer Security Center (NCSC) TG-005, Trusted Network Interpretation (TNI), dtd 31 Jul 1987
15. National Computer Security Center (NCSC)-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities for Automated Information Systems, dtd May 1992
16. National Computer Security Center (NCSC)-TG-029, Version 1, Introduction to Certification and Accreditation, dtd Jan 1994
17. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, dtd Oct 1995
18. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, dtd Sep 1996
19. NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-based Model, dtd Apr 1998
20. NIST SP 800-18, Guide for Development of Security Plans for Information Technology Systems, dtd Dec 1998

21. NIST SP 800-64, Security Considerations in the Information Systems Development Life Cycle, dtd, Oct 2003
22. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, dtd 5 Jul 1990
23. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, dtd 16 Nov 1992
24. NSTISSI No.1000, National Information Assurance Certification and Accreditation Process (NIACAP), dtd Apr 2000
25. CNSSI No. 4009, National Information Assurance (IA) Glossary, dtd May 2003
26. NSTISSP No. 11, Revised Fact Sheet, National Assurance Information Acquisition Policy, dtd July 2003
27. OMB Circular No. A-130, Revised (Transmittal Memorandum No. 4), Management of Federal Information Resources, dtd 30 Nov 2000
28. OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, dtd 28 Feb 2000
29. OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, dtd 16 Jan 2001
30. OMB Memorandum M-01-24, Reporting Instructions for the Government Information Security Reform Act, dtd 22 Jun 2001
31. OMB Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, dtd 17 Oct 2001
32. Code of Federal Regulations, 5 C.F.R. §903 *et seq*., Employees Responsible for the Management or Use of Federal Computer Systems
33. PL 93-579, 5 U.S.C. §552a, the Privacy Act of 1974
34. PL 107-347, E-Government Act 0f 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 2002
35. PL 104-106, Division E, the Information Technology Management Reform Act (Clinger-Cohen Act) of 1996
36. PL 106-398, Title X, Subtitle G, the Government Information Security Reform Act (GISRA)
37. The President's National Strategy to Secure Cyberspace, dtd Feb 2003