CNSS Instruction 4014
April 2004

NATIONAL INFORMATION

ASSURANCE TRAINING STANDARD

FOR

INFORMATION SYSTEMS SECURITY

OFFICERS

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 Information Systems Security Officers responsible for national security systems. It also may offer guidelines for Systems Security Officers responsible for 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 the private sector concerned with 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. 4014 is effective upon receipt. It replaces the National Training Standard for Information Systems Security Officers (ISSO), 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 Information Systems Security Officers (ISSOs). Please check with your agency for applicable implementing documents.

4. Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this instruction from:

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

/s/

MICHAEL V. HAYDEN
Lieutenant General, USAF

CNSS Secretariat (I01C) * National Security Agency * 9800 Savage Road STE 6716 * Ft Meade MD 20755-6716
(410) 854-6805 * UFAX: (410) 854-6814
cnss@radium.ncsc.mil

NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

SECTION I – PURPOSE

1) This instruction establishes the minimum training standard for the development and implementation of training for an Information Systems Security Officer (ISSO) in Information Assurance (IA).

SECTION II – APPLICABILITY

2) The National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501 establishes the requirement 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 during phases of the life cycle of a given information system. That directive is being implemented in a synergistic environment among departments and agencies that are committed to satisfying these IA education and training requirements in the most effective and efficient manner possible. This instruction is the continuation of a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (NSTISSI Nos. 4011, 4012, 4013, and 4015). The definitions for words used in this instruction are derived from the National Information Assurance (IA) Glossary, NSTISSI No. 4009. The references pertinent to this instruction are listed 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 an ISSO.

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 training for ISSOs in the IA discipline.

SECTION III – RESPONSIBILITIES

5) Heads of U.S. Government departments and agencies shall ensure that ISSOs are made aware of the body of knowledge outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

6) The National Manager shall:
   - maintain and provide an IA training standard for ISSOs to U.S. Government departments and agencies;
   - ensure that appropriate IA training courses for ISSOs are developed; and
   - assist other U.S. Government departments and agencies in developing and/or conducting IA training activities for ISSOs as requested.

Enclosures:

Annex A

Annex B

ANNEX A

INFORMATION ASSURANCE (IA) PERFORMANCE STANDARD FOR THE ISSO (ENTRY, INTERMEDIATE, & ADVANCED LEVELS)

Job functions using competencies identified in:

DoDD 8500.2, Information Assurance Implementation

Common Criteria for Information Technology Security Evaluation

DCID 6/3, Protecting Sensitive Compartmented Information Within Information Systems

The IA functions of an ISSO are:

1) maintaining a plan for site security improvements and progress towards meeting accreditation;
2) ensuring the information system (IS) is operated, used, maintained, and disposed of in accordance with security policies and practices;
3) ensuring the IS is certified and accredited;
4) ensuring users and system support personnel have required security clearances, authorization and need-to-know, are indoctrinated, and are familiar with internal security practices before access to the IS is granted;
5) enforcing security policies and safeguards on personnel having access to an IS for which the ISSO is responsible;
6) ensuring audit trails are reviewed periodically (e.g., weekly, daily), and audit records are archived for future reference, if required;
7) initiating protective or corrective measures;
8) reporting security incidents in accordance with agency-specific policy, such as DoDD 8500.2, to the Senior System Manager (SSM), viz., Chief Information Officer (CIO), Designated Approving Authority (DAA), Chief Technology Officer (CTO), etc., when the IS is compromised;
9) reporting security status of the IS, as required by the DAA; and
10) evaluating known vulnerabilities to ascertain if additional safeguards are needed.

Terminal Objective:

- ENTRY LEVEL: Given a series of system security breaches, the ISSO will identify system vulnerabilities and recommend security solutions required to return systems to an operational level of assurance.

- INTERMEDIATE LEVEL: Given a proposed new system architecture requirement, the ISSO will investigate and document system security technology, policy, and training requirements to assure system operation at a specified level of assurance.

- ADVANCED LEVEL: Given a proposed IS accreditation action, the ISSO will analyze and evaluate system security technology, policy, and training requirements in support of the Senior System Manager (SSM), viz., Chief Information Officer (CIO), Designated Approving Authority (DAA), Chief Technology Officer (CTO), etc., approval to operate the system at a specified level of assurance. This analysis will include a description of the management/technology team required to successfully complete the accreditation process.

List of performance items under job functions

E = entry level
I = intermediate level
A = advanced level

In each of the competency areas listed below by job function, the ISSO shall perform the following functions at the levels indicated:

I. DEVELOP CERTIFICATION AND ACCREDITATION POSTURE

A. PLANNING FOR CERTIFICATION AND ACCREDITATION

(1) *Planning*

E – Define certification and accreditation
E – Explain Common Criteria (CC)
E – Discuss National Information Assurance Program (NIAP) Validated Products List
E – Explain Information Technology Security Evaluation Criteria (ITSEC)
E – Explain International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17799
E – Explain the Model for Information Assurance: An Integrated Approach (2nd Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2002)
E – Discuss goals, mission, and objectives of the organization(s)
E – Discuss Information Technology Security Evaluation Criteria (ITSEC)
E – Discuss the concepts of availability, integrity, confidentiality, authentication, and non-repudiation
E – Discuss the theoretical concepts of security models – confidentiality models (e.g., Bell & LaPadula)
E – Discuss the theoretical concepts of security models – commercial systems models
E – Discuss the theoretical concepts of security models – integrity models (e.g., Biba, Clark and Wilson)
E – Discuss the theoretical concepts of security models – information flow models
E – Discuss the components of information systems evaluation models
I – Analyze the constituent components of the certification and accreditation process
E – Discuss the constituent components of the certification and accreditation process
I – Develop policy for completing and maintaining certification and accreditation
I – Explain certification and accreditation policy planning
A – Develop site security policy
A – Summarize planning for certification and accreditation posture
A – Write plan for certification and accreditation policy

(2) *Defense in Depth*

E – Give examples of defense in depth methods
I – Discuss defense in depth
I – Explain defense in depth
I – Explain the Model for Information Assurance: An Integrated Approach (2nd Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2002)
I – Summarize defense in depth

A – Verify implementation of defense in depth

(3) *Assets*

E – Define assets
E – Define contracts, agreements, and other obligation policy
E – Define policy for user roles
E – Define system owner
E – Define data owner
E – Discuss user roles
E – Identify assets
E – Identify contracts, agreements, and other obligations
E – Identify database structure
E – Identify system owner
E – Identify data owner
E – Identify systems interconnection
I – Explain asset inventory
I– Explain contracts, agreements, and other obligation policy
I – Explain database security feature use policy
I – Explain systems interconnection policy
I– Explain user roles
I – Monitor systems interconnection
I – Summarize asset inventory
I – Summarize database security feature use policy
I – Summarize systems interconnection policy
A – Integrate database security feature use policy
A –Verify asset inventory process
A – Write asset inventory policy
A – Write contracts, agreements, and other obligation policy
A – Write database security feature use policy
A – Write systems interconnection policy
A – Interpret asset inventory report

(4) *Threats*

E – Define adversarial threat
E – Define aggregation
E – Define technological threats
E – Define threats from careless/disgruntled employees
E – Define social engineering threats
E – Describe how espionage (industrial/international) can impact security of information systems
E – Describe adversarial threat
E – Describe how people can threaten system's security, i.e., intentional and unintentional
E – Describe how security reviews can be used to identify threats to information systems
E – Describe threat from electronic emanations
E – Describe threat from natural sources (fire, flood, earthquake, etc)

E – Describe types of environmental control (air conditioning, filtered power, etc.) threats
E – Describe types of intentional human threats to system
E – Describe types of unintentional human threats to system
E – Discuss aggregation
E – Discuss boundary
E – Discuss application and system vulnerabilities and threats - web-based (e.g., XML, SAML)
E – Discuss security implications posed by portable devices and components
E – Discuss application and system vulnerabilities and threats - client-based (e.g., applets, Active-X)
E – Discuss natural disaster impacts on system
E – Discuss application and system vulnerabilities and threats - server-based
E – Discuss application and system vulnerabilities and threats - mainframe
E – Discuss application and system vulnerabilities and threats - malicious code (e.g., Trojan Horses, trap doors, viruses, worms)
E – Discuss data mining
E – Discuss databases and data warehousing vulnerabilities, threats and protections
E – Discuss inference
E – Discuss object reuse
E – Discuss polyinstantiation
E – Discuss perimeter and building grounds protection issues/systems
E – Discuss access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
E – Discuss how the security architecture is affected by assurance and confidence
E – Discuss how the security architecture is affected by covert channels
E – Discuss how the security architecture is affected by countermeasures
E – Discuss how the security architecture is affected by emanations
E – Discuss how the security architecture is affected by maintenance hooks and privileged programs
E – Discuss how the security architecture is affected by resource misuse prevention
E – Discuss how the security architecture is affected by states attacks (e.g., time of check/time of use)
E – Discuss how the security architecture is affected by timing attacks
E – Identify access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
E – Identify appropriate EMSEC/TEMPEST authorities
E – Identify process for evaluating threat
E – Identify related disciplines that should contribute to risk analysis
I – Discuss computer network attack threat
I – Discuss data aggregation policy
I – Explain careless employee policy
I – Explain disgruntled employee policy
I – Explain security review policy
I – Explain social engineering policy
I – Explain EMSEC/TEMPEST policy

I – Identify computer network attack threats
I – Identify sources of technological threats: hardware, software (operating systems, applications, malicious code), firmware, networks (local area networks, wide area networks, metropolitan area networks, and direct connect)
I – Identify threat from aggregation
I – Identify threats from related disciplines
I – Present computer network attack policy
I – Present computer network attack threat policy
I – Present data aggregation policy
I – Present facility management policy
I – Present human threat policy
I – Present security review policy
I – Present social engineering policy
I – Present EMSEC/TEMPEST policy
I – Present threat assessment policy
I – Summarize computer network attack policy
I – Summarize computer network attack threat policy
I – Summarize data aggregation policy
I – Summarize facility management policy
I – Summarize human threat policy
I – Summarize security review policy
I – Summarize social engineering policy
I – Summarize EMSEC/TEMPEST policy
I – Summarize threat assessment policy
I – Use knowledge of threats from related disciplines
A – Analyze threats
A – Evaluate computer network attack threats
A – Evaluate data aggregation policy
A – Evaluate threat assessment
A – Evaluate threat from aggregation
A – Integrate data in to threat assessment
A – Interpret security review
A – Write careless/disgruntled employee monitoring policy
A – Write computer network attack policy
A – Write data aggregation policy
A – Write disgruntled employee monitoring policy
A – Write facility management policy
A – Write human threat policy
A – Write security review policy
A – Write social engineering monitoring policy
A – Write EMSEC/TEMPEST policy
A – Write threat assessment plan
A – Write threat assessment policy

(5) *Vulnerabilities*

E – Assist in performance of vulnerability analysis
E – Define National Information Assurance Program (NIAP) Validated Products List

E – Define Protection Profiles
E – Define vulnerabilities
E – Describe agency/vendor cooperation/coordination
E – Describe agency policy for access by uncleared individuals and vendors
E – Describe agency policy for redeploying classified systems
E – Describe technical surveillance vulnerabilities
E – Describe vulnerability analysis
E – Identify technical surveillance vulnerabilities
I– Demonstrate how to use NIAP Validated Products
I – Conduct/perform vulnerability analysis
I – Discuss technical surveillance vulnerabilities
I – Discuss technical surveillance vulnerabilities policy
I – Evaluate vulnerability
I – Explain agency/vendor cooperation/coordination policy
I – Explain agency policy for access by uncleared individuals and vendors
I – Explain agency policy for redeploying classified systems
I – Explain Validated Products policy
I – Explain Validated Products
I – Explain Protection Profile policy
I – Identify vulnerabilities with acquisitions
I – Present security requirements
I – Select vulnerabilities identified by agencies/vendors with existing cooperation/coordination
I – Select vulnerabilities in agency policy for access by uncleared individuals and vendors
I – Select vulnerabilities in agency policy for redeploying classified systems
I – Summarize technical surveillance vulnerabilities policy
I – Use Protection Profiles for input into vulnerability analysis
A – Analyze results of vulnerability analysis
A – Analyze vulnerabilities
A – Compile recommended fixes for deficiencies identified by vulnerability analysis
A – Recommend Evaluated Products for use in a system
A – Write agency/vendor cooperation/coordination policy
A – Write agency policy for access by uncleared individuals and vendors
A – Write agency policy for redeploying classified systems
A – Write Validated Product policy
A – Write Protection Profile policy
A – Write technical surveillance vulnerabilities policy
A – Write vulnerability analysis policy

(6) *Criticality*

E – Define asset criticality
E – Define attack analysis
E – Define criticality
I – Develop asset criticality measures
I – Identify asset criticality
A – Assess criticality

A – Write attack analysis plan
A – Write attack analysis policy
A – Write attack analysis report

(7) *Risk*

E – Define risk (threat and vulnerability pairs together with significance)
E – Discuss risk management concepts
I – Develop risk policy
I – Present risk policy
A – Write risk policy

(8) *Conduct Risk Assessment*

E – Define information valuation
E – Define risk assessment
E – Describe risk assessment process
E – Describe three states of information
I – Coordinate risk assessment process
I – Develop policy and procedures for conducting a risk assessment
I – Summarize risk profile
I – Write risk assessment reports
A – Coordinate resources to perform a risk assessment
A – Interpret results of a risk assessment
A – Interpret risk assessment report
A –Perform security assessment
A – Write risk assessment plan
A – Write risk assessment policy

(9) *Countermeasures*

E – Define countermeasures
E – Describe how countermeasures can mitigate risk
E – Discuss application environment and security controls
E – Discuss audit trails/access logs & intrusion detection applications
E – Discuss firewalls
E – Discuss badging, and smart/dumb cards
E – Discuss biometric access controls to facility
E – Discuss CCTV requirements/capabilities
E – Define National Information Assurance Program (NIAP) Validated Products List
E – Discuss escort requirements/visitor control issues
E – Discuss fire detection and suppression issues/systems
E – Discuss intrusion detection system (e.g., firewalls, motion detectors, sensors, alarms) requirements/capabilities
E – Discuss keys and locks requirements/capabilities
E – Discuss power and HVAC considerations
E – Discuss restricted areas/work areas security requirements
E – Discuss risk management concepts
E – Discuss security guard requirements
E – Discuss site selection and facility design configuration considerations
E – Discuss turnstiles and mantraps requirements

E – Discuss water, leakage, flooding impact to system
E – Identify countermeasures to deter/mitigate attack threats (e.g.; malicious code, flooding, spamming)
I – Develop security plan
I – Develop a security policy
I – Explain ITSEC/Common Criteria
I – Summarize countermeasure
I – Summarize ITSEC/Common Criteria policy
A – Ensure training for SA/staff with specific IT security roles is provided
A – Evaluate information system security strategies
A – Recommend accreditation of a system to the SSM, viz., CIO, DAA, CTO, etc. based on risk assessment
A – Recommend actions to management based on risk acceptance
A – Recommend ITSEC/Common Criteria policy

(10) *Organizational/Agency Systems Emergency/Incident Response Team*

E – Define organizational/agency systems emergency/incident response team
E – Identify organizational/agency systems emergency/incident response team

(11) *Education, Training, & Awareness (ETA)*

E – List topics for inclusion into education, training, and awareness (ETA) policy
E – Discuss ETA as a countermeasure
I – Develop ETA policy
I – Recommend input to organizational ETA activities

(12) *Residual Risk*

E – Define residual risk
I – Explain residual risk
I – Summarize residual risk
A – Write residual risk standard and policy

(13) *Cost/Benefit Analysis*

E – Define cost/benefit analysis
E – Define risk acceptance
I – Conduct business impact analysis
I – Conduct cost/benefit analysis procedures
I – Describe cost of the system life cycle and security
I – Describe risk acceptance process
I – Summarize cost/benefit analysis
A – Interpret cost/benefit analysis results to formulate recommend changes
A – Recommend cost/benefit analysis
A – Write cost/benefit analysis

B. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA) POLICY

(1) *Contingency Plans*

E – Define contingency plans
E – Identify items for which plans must be developed
E – Prepare input to contingency plan

E – Write contingency plan
I – Present contingency plan
I – Specify method to exercise contingency plan
I – Specify method to test contingency plan
I – Exercise contingency plan
I – Assess effectiveness of contingency plan

(2) *Concept of Operations (CONOP)*

E – Define Concept Of Operations (CONOP)
I – Develop CONOP policy
I – Discuss information covered by CONOP
I – Present CONOP plan
I – Propose methods and policies to include in CONOP
A – Integrate standard operating procedures into CONOP
A – Write CONOP policy
A – Write CONOP plan
A – Develop/write roles and responsibilities for continuity participants

(3) *Continuity Plans*

E – Define continuity plan
E – Discuss business continuity planning (BCP)
E – Discuss business organization analysis
E – Discuss disaster recovery planning (DRP) (recovery planning and strategy)
E – Discuss project scope development and planning
E – Discuss resource requirements
E – Identify items for which plans must be developed
E – Outline security policy for backup procedures
E – Prepare input to continuity plan
E – Write continuity plan
I – Develop alternatives - cold, warm, hot and mobile sites, electronic vaulting, etc
I – Develop backups and off-site storage plan
I – Develop business resumption plan
I – Develop communications plan
I – Develop documentation plan
I – Develop emergency response plan
I – Develop fire and water protection plan
I – Develop logistics and supplies plan
I – Develop personnel notification plan
I – Develop processing agreements - reciprocal, mutual, etc
I – Develop recovery strategy
I – Develop unit priorities
I – Develop utilities plan
I – Explain business organization analysis
I – Explain project scope development and planning
I – Explain resource requirements
I – Modify contingency plan reflecting changes
I – Plan backups and off-site storage

I – Plan business resumption
I – Plan communications
I – Plan documentation
I – Plan emergency response
I – Plan fire and water protection
I – Plan logistics and supplies
I – Plan personnel notification
I – Plan primary/backup/reconstitution utilities
I – Present continuity plan
I – Review backup policy
I – Specify method to exercise backup plan
I – Specify method to exercise continuity plan
I – Specify method to exercise reconstitution plan
I – Specify method to test continuity plan
I – Specify method to test reconstitution plan
I – Test/exercise continuity plans
I – Test/exercise reconstitution plans
A – Develop/write backups and off-site storage plan
A – Develop/write business resumption plan
A – Develop/write communications plan
A – Develop/write documentation plan
A – Develop/write emergency response plan
A – Develop/write fire and water protection plan
A – Develop/write logistics and supplies plan
A – Develop/write personnel notification plan
A – Develop/write utilities plan
A – Evaluate backup policy
A – Integrate reconstitution plans into local policy

(4) *Legal Plan*

(a) Criminal Activity Preparedness Planning

E – Discuss evidence collection and handling
E – Discuss incident handling and response
E – Discuss the parameters of investigations
I – Explain NSTISSP 11
I – Develop/write policy for criminal activity
I – Explain criminal activity preparedness planning policy
I – Explain evidence collection and handling
I – Explain incident handling and response
I – Explain the parameters of investigations
I – Explain containment/management of evidence
A – Evaluate criminal activity preparedness plan
A – Integrate criminal activity preparedness into local policy
A – Summarizes criminal activity preparedness plan
A – Write policy for criminal activity

(b) Laws*

E – Discuss Clinger-Cohen Act

E – Discuss Computer Fraud and Abuse Act
E – Discuss Copyright Act of 1976
E – Discuss Copyright Protection and License
E – Discuss Electronic Freedom of Information Act
E – Discuss Electronic Records Management and Federal Records Act
E – Discuss Federal Information System Management Act
E – Discuss Federal Managers Financial Integrity Act
E – Discuss Federal Property and Administration Service Act
E – Discuss Freedom of Information Act
E – Discuss Government Paperwork Elimination Act
E – Discuss Government Information Security Reform Act
E – Discuss Millennium Copyright Act
E – Discuss National Archives and Records Act
E – Discuss Privacy Act issues
E – Discuss USA Patriot Act
E – Discuss computer crime and various methods used to commit computer crime
E – Discuss computer crime laws
E – Discuss implications of the Privacy Act
E – Discuss import/export laws
E – Discuss information systems security laws
E – Discuss intellectual properties laws
E – Discuss international legal issues which can affect information assurance
E – Discuss liability laws
E – Discuss licensing laws
E – Discuss legal responsibilities of the SSM, viz., CIO, DAA, CTO, etc.
E – Discuss requirements of Computer Security Act
E – Discuss trans-border data flow laws
A – Verify applicable laws and directives
* As amended

(5) *Disposition of Classified Material & Emergency Destruction Policy (EDP)*

E – Define disposition of classified material
E – Explain emergency destruction policy (EDP) to those who execute plans
I – Explain disposition policy
I – Present disposition plan
I – Specify method to exercise deposition plan
I – Specify method to test deposition plan
I – Summarize disposition policy
A – Integrate EDP into overall plans
A – Recommend disposition policy
A – Write disposition policy
A – Test disposition/EDP plan

(6) *Identification and Authentication (I&A) Policy*

E – Discuss authentication
E – Discuss non-repudiation
E – Define account management

E – Define authentication
E – Define biometrics
E – Define identification and authentication (I&A)
E – Define non-repudiation
E – Define peer-to-peer security
E – Define unauthorized access
E – Describe how to choose appropriate passwords, and how/why to protect them
E – Explain need for account management
E – List underlying account management principles
E – List underlying authentication principles
E – List underlying security concerns with password sharing
E – Discuss good passwords/password conventions
I – Explain password management/password conventions
I – Develop authentication schema
I – Develop local policies and procedures governing password sharing
I – Develop non-repudiation schema
I – Develop organizational policies and procedures for password use/selection
I – Develop security policy for account administration
I – Discuss account management
I – Discuss authentication principles
I – Explain authentication policy
I – Explain I&A
I – Explain I&A policy
I – Explain need for authentication
I – Explain peer-to-peer security policy
I – Implement account management
I – Implement biometrics
I – Implement non-repudiation schema
I – Present authentication identification and authentication policy
I – Propose methods to share files without sharing passwords
I – Summarize biometrics
I – Summarize peer-to-peer security policy
A – Discuss good password systems
A – Implement authentication
A – Integrate authentication into local policy
A – Integrate biometrics into systems
A – Integrate I&A into overall plans
A – Integrate peer-to-peer security into local policy
A – Write authentication policy
A – Write biometrics policy
A – Write I&A policy
A – Write peer-to-peer security policy

(7) *Monitoring and Auditing Policy*

E – Define electronic monitoring
E – Define intrusion detections
E – Define keystroke monitoring

E – Define keystroke monitoring requirements for policy and procedures
E – Define monitoring
E – Define required audit features
E – Define requirements for error logs/system logs
E – Describe audit collection requirements
E – Describe policy for audit
E – Identify audit and log tools
E – Identify error and system tools
E – Outline known means of electronic monitoring
E – Outline known means of keystroke monitoring
I – Develop audit policy
I – Develop audit trails and logging policy and procedures in compliance with legal requirements
I – Develop electronic monitoring policy
I – Develop monitoring techniques and methods
I – Develop policy and procedures on use of audit trails and logging
I – Develop policy and procedures on use of error logs/system logs
I – Develop policy for monitoring and auditing information systems
I – Discuss audit collection requirements
I – Discuss audit policy and procedures
I – Discuss electronic monitoring
I – Discuss monitoring
I – Discuss policy and procedures
I – Implement audit trail and logging
I – Implement electronic monitoring policy
I – Implement logging
I – Implement monitoring policy
I – Propose implementation of intrusion detection
I – Use audit collection
I – Use results of electronic monitoring reports
A – Discuss audit collection requirements
A – Write audit trail error logs/system logs
A – Write audit trail logging policy
A – Write electronic monitoring policy
A – Write keystroke monitoring policy
A – Write monitoring policy
A – Write policies for intrusion detection in accordance with higher level policies

C. CONTROL SYSTEMS POLICIES

(1) ***Configuration Management Policy***

E – Define configuration management
E – Define Configuration Control Board (CCB)
I – Discuss change controls
I – Discuss configuration CCB
I – Integrate change control into operations
I – Plan change control

A – Evaluate change control plan
A – Integrate information system security requirements into configuration management program
A – Write configuration management policy

(2) *Protective Technology Policy*

E – Define protective technology
E – List protective technologies
I – Develop policy for integrating protective technology
A – Explain protective technologies policy
A – Predict requirements for protective technology policy
A – Write protective technology policy

(3) *Intrusion Detection Policy*

E – Define intrusion detection
I – Develop policy governing intrusion detection
I – Discuss intrusion detection policy
I – Explain intrusion detection policy
I – Identify requirements for intrusion detection
A – Write intrusion detection policy

(4) *Malicious Code Policy*

E – Define malicious code
E – Describe malicious code and outline various types of malicious code
E – Describe techniques for protection from malicious code to users, and provide examples (real and theoretical)
I – Propose methods and policies to combat introduction of malicious code into system
A – Explain consequences of introducing malicious code
A – Integrate protection techniques into policies
A – Write policy on malicious code

(5) *Access Controls*

E – Define need to understand policy
E – Define need-to-know
E – Define risk management policy
E – Explain user access policy
E – Explain user access requirements
I – Develop need to understand policy
I – Develop security policy for administration of access controls
I – Explain access control requirements
I – Explain risk management to access control policy
I – Summarize risk management policy
A – Integrate access controls into policy
A – Summarize risk management policy
A – Write access control policy
A – Write risk management policy
A – Write user access policy

D. CULTURE AND ETHICS

(1) *Policy*

E – Define culture and ethics policy
E – Define roles, responsibilities, and organization (e.g., separation of duties)
E – Identify basic management issues and their impact on information systems security program
I – Demonstrate professional ethics
I – Explain professional ethics
I – Develop policy governing use of information systems
I – Discuss importance of privacy
I – Discuss privacy policy
I – Explain organization's culture and its affect on security of information systems
I – Explain privacy policy
A – Implement privacy policy
A – Integrate privacy concerns and laws into organizational policy
A – Write policy governing appropriate use of information system
A – Write privacy policy

(2) *Organization Culture*

E – Describe organization culture
I – Explain organization culture
I – Explain organization culture policy

(3) *Basic/Generic Management Issues*

E – Describe basic/generic management issues
A – Integrate management issues into local policy

(4) *Agency-Specific Security Policies & Procedures*

E – Describe how effective security policies and procedures can reduce threats to information systems
E – Identify security policy-making bodies
I – Write local guidance
A – Interpret agency policy and procedures for guiding local policy and procedures

E. INCIDENT RESPONSE

(1) *Concept of Operations (CONOP)*

E – Define Concept of Operations (CONOP)
I – Develop CONOP
I – Develop CONOP policy
I – Discuss information covered by CONOP
I – Propose methods and policies to include in CONOP
A – Integrate standard operating procedures into CONOP
A – Write CONOP policy

(2) *Criminal Activity Preparedness Planning*

E – Explain criminal activity preparedness planning policy
I – Develop policy for criminal activity
A – Evaluate criminal activity preparedness plan
A – Integrate criminal activity preparedness into local policy
A – Summarize criminal activity preparedness plan
A – Write policy for criminal activity

(3) *Organizational/Agency Systems Emergency/Incident Response Team*

E – Define organizational/agency systems emergency/incident response team
E – Identify organizational/agency systems emergency/incident response team
E – Interact with organizational/agency systems emergency/incident response team to resolve incidents

(4) *Malicious Code*

E – Define malicious code
E – Describe malicious code and outline various types of malicious code
E – Describe techniques for protection from malicious code to users, and provide examples (real and theoretical)
I – Propose methods and policies to combat introduction of malicious code into system
A – Integrate protection techniques into policies
A – Write policy on malicious code

II. IMPLEMENT SITE SECURITY POLICY

A. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA)

(1) *Contingency Plans*

I – Develop contingency plan
I – Discuss current contingency plan with necessary parties
I – Explain contingency plan
I – Monitor contingency plan training
I – Propose contingency plan
I – Summarize contingency plan
A – Direct implementation of contingency plan
A – Direct operation of contingency plan
A – Influence management on importance of having properly trained SA/staff to perform contingency plan on mission critical systems
A – Test contingency plan
A – Verify current contingency plan is available and accurate
A – Verify that necessary parties understand contingency plan and where it is maintained
A – Write contingency plan

(2) *Emergency Destruction Procedures (EDP)*

E – Discuss current emergency destruction plan (EDP) with necessary parties
I – Develop EDP
I – Explain EDP
I – Monitor EDP training
I – Summarize EDP
I – Verify that necessary parties understand EDP and where it is maintained
A – Direct implementation of EDP
A – Direct operation of EDP
A – Influence management on importance of having properly trained SA/staff to perform EDP on mission critical systems
A – Propose EDP
A – Test EDP
A – Verify current EDP is available and accurate
A – Write EDP

(3) *Continuity Plans*

(a) Reconstitution

I – Discuss current reconstitution plan with necessary parties to ensure they understand their respective reconstitution roles and responsibilities.
I – Explain reconstitution plan
I – Explain restoration
I – Monitor reconstitution plan training
I – Monitor restoration/reconstitution
I – Summarize restoration/reconstitution plan

I – Verify that necessary parties understand restoration/reconstitution plans and where they are maintained
A – Develop restoration/reconstitution plan
A – Direct implementation of reconstitution plan
A – Direct operation of reconstitution plan
A – Implement and maintain recovery procedures
A – Implement recovery procedures
A – Implement testing and assessment
A – Implement training
A – Influence management on importance of having properly trained SA/staff to perform reconstitution plan on mission critical systems
A – Propose reconstitution plan
A – Test/exercise restoration/reconstitution plan
A – Verify current restoration/reconstitution plan is available and accurate
A – Write restoration/reconstitution plan
A – Evaluate test/execution of reconstitution plan

(b) Recovery

E – Address recovery procedures with SA/staff
I – Develop recovery plan
I – Direct SA/staff to use recovery plan during recovery
I – Discuss current recovery plan with necessary parties
I – Explain recovery plan
I – Monitor recovery plan training
I – Summarize recovery plan
I – Verify that necessary parties understand recovery plan and where it is maintained
A – Direct implementation of recovery plan
A – Direct operation of recovery plan
A – Influence management on importance of having properly trained SA/staff to perform recovery plan on mission critical systems
A – Propose recovery plan
A – Test recovery plan
A – Verify current recovery plan is available and accurate
A – Verify SA understands rules for restoring files
A – Write recovery plan

(c) Accountability

E – Define who has responsibility for accountability
E – Describe accounting process for hardware, software, and information
E – Outline accountability process/program
A – Verify assigned responsibilities are commensurate with underlying information system security policies and are appropriately assigned

(4) *Disposition of Classified Material*

E – Address disposition procedures with system administrator SA/staff
E – Explain the maintenance of audit records
I – Develop disposition plan

I – Direct SA/staff to review relevant policy and procedures for disposition of classified material
I – Direct SA/staff to use disposition plan
I – Discuss current disposition plan with necessary parties
I – Explain disposition plan
I – Monitor disposition plan training
I – Summarize disposition plan
I – Verify that necessary parties understand disposition plan and where it is maintained
A – Direct implementation of disposition plan
A – Direct operation of disposition plan
A – Influence management of importance of having properly trained SA/staff to perform disposition plan on mission critical systems
A – Propose disposition plan
A – Test disposition plan
A – Verify current disposition plan is available and accurate
A – Verify disposition classified material plan is executed
A – Verify SA understands rules to disposition procedures
A – Write disposition plan
A – Evaluate disposition plan

(5) ***Monitoring and Auditing***

Alarms, Signals, & Reports

E – Address auditing and logging management with SA/staff
E – Address work force auditing and logging management procedures
E – Discuss alarms, signals, and reports requirements
E – Discuss auditing and logging management policies, laws, and penalties with personnel
E – Discuss current auditing and logging management with necessary parties
I – Develop auditing and logging management plan
I – Direct SA to follow proper auditing and logging management procedures
I – Direct SA to implement auditing and logging management procedures
I – Direct SA/staff to follow proper auditing and logging procedures
I – Direct SA/staff to follow proper monitoring and auditing procedures
I – Direct SA/staff to restrict access to auditing and logging functions and collected log files
I – Direct SA/staff to restrict access to auditing and logging system and collected information
I – Direct SA/staff to review policy and procedures for auditing and logging management
I – Direct SA/staff to review relevant policy and procedures for auditing and logging management
I – Direct SA/staff to use auditing and logging management
I – Explain alarms, signals, and reports requirements
I – Explain auditing and logging management plan
I – Monitor auditing and logging management plan training
I – Summarize auditing and logging management plan

I – Use analysis of intrusion indicators, when appropriate, and generate results
I – Verify that necessary parties understand auditing and logging management plan and where it is maintained
A – Direct implementation of auditing and logging management plan
A – Direct operation of auditing and logging management plan
A – Establish auditing and logging management policy for infractions
A – Implement auditing and logging management policy
A – Implement auditing and logging management reporting
A – Influence management on importance of having properly trained SA/staff to perform auditing and logging management plan on mission critical systems
A – Interpret legal aspects of logging and auditing systems
A – Prescribe changes that result from analysis
A – Prescribe oversight associated with alarms and signals
A – Propose auditing and logging management plan
A – Test alarms, signals, and reports
A – Test auditing and logging management plan
A – Verify adherence to auditing and logging procedures
A – Verify auditing and logging management plan is executed
A – Verify current auditing and logging management plan is available and accurate
A – Verify monitoring and auditing procedures and that they are being followed
A – Verify SA understands rules for auditing and logging management
A – Verify strategic items being audited and logged
A – Verify strategic placement of auditing and logging system
A – Write auditing and logging management plan

(6) *Audit Trail and Logging, Error/System Logs*

I – Prescribe changes resulting from evaluation alarms, signals, & reports

(7) *Intrusion Detection*

E – Address intrusion detection management with SA/staff
E – Address SA/staff about monitoring and auditing intrusion detection policies
E – Address work force about intrusion detection management procedures
I – Develop intrusion detection management plan
I – Direct implementation of intrusion detection management plan
I – Direct operation of intrusion detection management plan
I – Direct SA/staff to follow proper intrusion detection management procedures
I – Direct SA/staff to implement intrusion detection management procedures
I – Direct SA/staff to follow proper monitoring and auditing procedures
I – Direct SA/staff to restrict access to intrusion detection system and collected information
I – Direct SA/staff to review relevant policy and procedures for intrusion detection management
I – Direct SA/staff to review relevant policy and procedures for intrusion detection management
I – Direct SA/staff to use intrusion detection management
I – Discuss current intrusion detection management plans, policies, and procedures with necessary parties

I – Discuss intrusion detection management policies, laws, and penalties with personnel
I – Explain intrusion detection management plan
I – Monitor intrusion detection management plan training
I – Summarize intrusion detection management plan
I – Verify that necessary parties understand intrusion detection management plan and where it is maintained
A – Establish intrusion detection management policy for infractions
A – Implement intrusion detection management policy
A – Implement intrusion detection management reporting
A – Influence management on importance of having properly trained SA/staff to execute intrusion detection management plans, policies, and procedures on mission critical systems
A – Interpret legal aspects of intrusion detection systems
A – Propose intrusion detection management plan
A – Test intrusion detection management plan
A – Verify current intrusion detection management plan is available and accurate
A – Verify intrusion detection management plan is executed
A – Verify intrusion detection management policy is followed
A – Verify monitoring and auditing procedures and that they are being followed
A – Verify SA understands rules for intrusion detection management
A – Verify strategic placement of intrusion detection system
A – Write intrusion detection management plan

(8) *Investigation of Security Breaches*

E – Define security breaches
I – Discuss consequences of security breaches
I – Discuss security breaches
A – Evaluate results of security breaches
A – Evaluate significance of security breaches
A – Implement policy for addressing security breaches
A – Prescribe changes resulting from evaluation of security breaches
A – Prescribe oversight associated with investigations
A – Test security breach detection systems
A – Verify security breach policy is implemented

(9) *Monitoring*

E – Address monitoring management with SA/staff
E – Address SA/staff about legal monitoring restrictions
E – Address work force about monitoring management procedures
I – Develop monitoring management plan
I – Direct SA/staff to follow proper monitoring management procedures
I – Direct SA/staff to help work force with monitoring management procedures
I – Direct SA/staff to follow appropriate laws and policies for monitoring
I – Direct SA/staff to follow proper monitoring procedures
I – Direct SA/staff to restrict access to monitoring functions and collected log files
I – Direct SA/staff to restrict access to monitoring system and collected information

I – Direct SA/staff to review relevant policy and procedures for monitoring
I – Direct SA/staff to use monitoring management procedures
I – Discuss current monitoring management with necessary parties
I – Discuss monitoring management policies, laws, and penalties with personnel
I – Explain monitoring management plan
I – Monitor monitoring management plan training
I – Summarize monitoring management plan
I – Verify that necessary parties understand monitoring management plan and where it is maintained
A – Direct implementation of monitoring management plan
A – Direct operation of monitoring management plan
A – Establish policy infractions for monitoring management
A – Implement monitoring management policy
A – Implement monitoring management reporting
A – Influence management on importance of having properly trained SA/staff to perform monitoring management plan on mission critical systems
A – Interpret legal aspects of monitoring systems
A – Propose monitoring management plan
A – Test monitoring management plan
A – Verify adherence to appropriate laws and policies for monitoring
A – Verify adherence to monitoring procedures
A – Verify current monitoring management plan is available and accurate
A – Verify monitoring and auditing procedures and that they are being followed
A – Verify monitoring management plan is executed
A – Verify monitoring management policy is followed
A – Verify SA understands rules for monitoring management
A – Verify strategic items being monitored
A – Verify strategic placement of monitoring systems
A – Verify that consent to monitoring banners are in place
A – Verify that process for maintaining signed consent to monitoring forms exists
A – Write monitoring management plan

(10) ***Configuration Management***

E – Address configuration management with SA/staff
E – Address SA/staff about legal configuration restrictions
E – Address work force about configuration management procedures
I – Direct SA to follow proper configuration management procedures
I – Direct SA to help work force with configuration management procedures
I – Direct SA/staff to follow appropriate laws and policies for configuration
I – Direct SA/staff to follow configuration control software procedures
I – Direct SA/staff to follow proper configuration procedures
I – Direct SA/staff to restrict access to configuration functions and collected log files
I – Direct SA/staff to restrict access to configuration system and collected information
I – Direct SA/staff to review relevant policy and procedures for configuration management
I – Direct SA/staff to use configuration management procedures
I – Discuss configuration management policies, laws and penalties with personnel

I – Discuss current configuration management with necessary parties
I – Explain configuration management plan
I – Monitor configuration management plan training
I – Summarize monitoring management plan
I – Verify that necessary parties understand configuration management plan and where it is maintained
A – Develop configuration management plan
A – Direct implementation of configuration management plan
A – Direct operation of configuration management plan
A – Establish configuration management policy
A – Implement configuration management policy
A – Implement configuration management reporting
A – Influence management on importance of having properly trained SA/staff to perform configuration management plan on mission critical systems
A – Interpret legal aspects of configuration systems
A – Propose configuration management plan
A – Test configuration management plan
A – Verify adherence to appropriate laws and policies for configuration procedures
A – Verify adherence to configuration procedures
A – Verify configuration and auditing procedures and ensure that they are being followed
A – Verify configuration management plan is executed
A – Verify configuration management policy is followed
A – Verify current configuration management plan is available and accurate
A – Verify SA understands rules for configuration management
A – Verify strategic items being under configuration management
A – Verify that software configuration is restricted
A – Write configuration management plan

(11) *Countermeasures*

(a) Intrusion Detection

E – Discuss intrusion detection problems
I – Direct intrusion detection be implemented
I – Explain intrusion detection problems
A – Evaluate results of intrusion detection process
A – Prescribe changes resulting from evaluation of intrusion detection process
A – Prescribe oversight associated with intrusion detection process
A – Test intrusion detection system
A – Verify intrusion detection is in accordance with policy

(b) Protective technologies

E – Define cryptanalytic techniques
E – Define cryptographic concepts
E – Define digital signatures/non-repudiation
E – Define key management
E – Define message digests (e.g., MD5, SHA, HMAC)
E – Define methods of encryption
E – Identify protective technologies

I – Discuss methods of encryption
I – Discuss protective technologies implementation
I – Explain alternatives (e.g., steganography, watermarking)
I – Explain cryptanalytic techniques
I – Explain cryptographic concepts
I – Explain digital signatures/non-repudiation
I – Explain email security (e.g., PGP, PEM)
I – Explain internet security (e.g., SSL)
I – Explain key management
I – Explain message digests (e.g., MD5, SHA, HMAC)
I – Explain public key infrastructure (PKI) (e.g., certification authorities, etc)
I – Present protective technologies implementation plan
I – Recommend alternatives (e.g., steganography, watermarking)
I – Recommend digital signatures/non-repudiation tools
I – Recommend email security (e.g., PGP, PEM)
I – Recommend internet security (e.g., SSL)
I – Recommend message digests (e.g., MD5, SHA, HMAC) tools
I – Recommend protective technologies
I – Recommend public key infrastructure (PKI) (e.g., certification authorities, etc.)
I – Summarize protective technologies implementation plan
A – Plan protective technologies implementation
A – Test alternatives (e.g., steganography, watermarking)
A – Test email security (e.g., PGP, PEM)
A – Test internet security (e.g., SSL)
A – Test protective technologies plan
A – Test public key infrastructure (PKI) (e.g., certification authorities, etc.)
A – Verify countermeasures exist and that countermeasure procedures are being followed
A – Verify protective technologies performs as expected

B. ENSURE FACILITY IS APPROVED

E – Define an approved facility
E – Define an approved service
I – Explain what constitutes approved facility
I – Explain what constitutes approved service
I – Monitor acquisition of approved facility
I – Monitor acquisition of approved service
I – Monitor operation of approved facility
I – Monitor operation of approved service
I – Present approved facility plan to SSM, viz., CIO, DAA, CTO, etc.
I – Present approved service plan to SSM, viz., CIO, DAA, CTO, etc.
I – Recommend approved facility configuration
I – Summarize major elements of an approved facility
I – Summarize major elements of an approved service
A – Direct Contracting Officer's Technical Representative (COTR) through facility acquisition process
A – Direct COTR through service acquisition process

A – Evaluate contracted security services
A – Integrate security services
A – Plan an approved facility
A – Plan an approved service
A – Plan for acquisition of an approved facility
A – Plan for acquisition of an approved service
A – Report on contracted security services
A – Verify facility is approved appropriate authority
A – Verify service is approved appropriate authority
A – Write plan for implementing an approved facility
A – Write plan for implementing an approved service contract

C. OPERATIONS

(1) *Security Policy*

I - Ensure Information System is installed, operated, used, maintained, and disposed of in accordance with security policy

(2) *Agency/Vendor Cooperation/Coordination*

E – Describe agency policy for redeploying classified systems to the SA and SSM viz., CIO, DAA, CTO, etc.
E – Explain agency policy for access by uncleared individuals and vendors to the SA and SSM viz., CIO, DAA, CTO, etc.
E – Explain cooperation concerns to vendors
E – Explain cooperation concerns with vendors to SSM, viz., CIO, DAA, CTO, etc.
E – Facilitate agency control of access by uncleared individuals and vendors
E – Facilitate correct agency redeployment of classified systems
E – Facilitate vendor cooperation
I – Present the agency policy for access by uncleared individuals and vendors
I – Present the agency policy for redeploying classified systems
I – Present vendor cooperation report
I – Summarize vendor cooperation
A – Evaluate agency policy for access by uncleared individuals and vendors
A – Evaluate agency policy for redeploying classified systems
A – Evaluate vendor cooperation
A – Report vendor cooperation
A – Verify corrective vendor actions when required

(3) *Certification Advocacy*

E – Define advocacy
E – Explain advocacy role
I – Demonstrate compliance with certification plan
I – Explain certification to SSM, viz., CIO, DAA, CTO, etc.
I – Explain certification to SA
A – Coordinate with certifier

(4) *Conduct Risk Assessment*

E – Define information valuation
E – Define risk assessment

E – Describe risk assessment process
E – Describe three states of information
I – Develop policy and procedures for conducting a risk assessment
I – Summarize risk profile
I – Write risk assessment reports
A – Coordinate resources to perform a risk assessment
A – Coordinate risk assessment process
A – Interpret results of a risk assessment
A – Interpret risk assessment report
A – Write risk assessment plan
A – Write risk assessment policy
A – Analyze threats to and vulnerabilities of an information system

(5) *Contracting for Security Services*

E – Define an approved service
E – Explain security services to contracting officers
I – Direct contracting officers to incorporate security services as required
I – Discuss Protection Profiles and Security Target
I – Explain what constitutes an approved service
I – Monitor acquisition of approved service
I – Monitor operation of approved service
I – Plan an approved service
I – Plan for acquisition of an approved service
I – Present approved service plan to SSM, viz., CIO, DAA, CTO, etc.
I – Summarize major elements of an approved service
A – Direct COTR through service acquisition process
A – Evaluate contracted security services
A – Integrate security services contracts
A – Report on contracted security services
A – Verify obligation for security services
A – Verify service is approved by appropriate authority
A – Write plan for implementing an approved service contract

(6) *Ensure information system is approved*

A – Verify system approval with SSM, viz., CIO, DAA, CTO, etc.

(7) *Life Cycle System Security Planning*

E – Define life cycle security
E – Describe agency policy for redeploying classified systems
E – Explain life cycle security planning
E – Explain life cycle system security planning
I – Explain agency policy for redeploying classified systems
I – Direct life cycle system security planning
I – Direct SA to incorporate life cycle security planning as required
I – Explain life cycle security plan
I – Monitor life cycle security acquisition process
I – Monitor life cycle security process
I – Plan life cycle security

I – Present life cycle security plan to SSM, viz., CIO, DAA, CTO, etc.
I – Summarize major elements of life cycle security
A – Evaluate life cycle security implementation
A – Implement Data Item Descriptions (DID) for life cycle security
A – Implement life cycle security process to support CONOPS
A – Integrate life cycle security
A – Report on life cycle security implementation
A – Validate use of appropriate life cycle security process
A – Verify life cycle security planning is approved
A – Verify life cycle system security planning is implemented

(8) *System Security Architecture Study*

E – Address system security architecture study
E – Define system security architecture
E – Explain system security architecture study
I – Direct SA to incorporate system security architecture study as required
I – Direct support of system security architecture
I – Direct system security architecture study
I – Explain system security architecture study
I – Monitor system security architecture acquisition process
I – Monitor system security architecture process
I – Present system security architecture study to SSM, viz., CIO, DAA, CTO, etc.
I – Summarize major elements of system security architecture
A – Evaluate system security architecture implementation
A – Implement DIDS for system security architecture
A – Integrate system security architecture
A – Report on system security architecture implementation
A – Study system security architecture
A – Validate appropriate system security architecture process
A – Verify results mapped to security CONOPS
A – Verify that security architecture study provides for defense in depth
A – Verify system security architecture is approved
A – Verify system security architecture study is implemented

D. GENERAL PRINCIPLES

(1) *Access Control Models*

E – Discuss access control models

(2) *Approval to Operate*

E – Explain approval to operate
A – Verify SSM, viz., CIO, DAA, CTO, etc. can discuss approval to operate

(3) *Attack*

E – Explain attack
E – Explain backdoor routines
E – Explain denial-of-service (DOS) attacks
E – Explain remote explorer attack

E – Explain attack root exploits
E – Explain session hijacking tools
E – Explain war dialer/THC-scan attacks
E – Explain war dialers

(4) *Business Aspects of Information Security*

E – Explain business aspects of information security

(5) *Common Criteria*

I – Discuss common criteria
I – Explain common criteria
I – Discuss Evaluation Assurance Levels (EALs)
I – Summarize common criteria
A – Verify security services as defined by common criteria are implemented

(6) *Computer Network Attack*

E – Explain computer network attack

(7) *Criminal Prosecution*

E – Explain criminal prosecution

(8) *Defense in Depth*

E – Give examples of defense in depth methods
I – Discuss defense in depth
I – Explain defense in depth
I – Explain the role of vendors and uncleared individuals in defense in depth
I – Explain the Model for Information Assurance: An Integrated Approach (2nd Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2002)
I – Summarize defense in depth
A – Verify implementation of defense in depth
A – Verify security architecture provides defense in depth

(9) *Due Care*

E – Address questions from users about due care
E – Monitor adherence to due care rules
E – Remind users of due care rules
I – Explain generally accepted systems security principles (GASSP)
I – Identify standards upon which GASSP are based
A – Integrate GASSP into standard operating procedures
A – Interpret due care rules
A – Verify due care concerns are addressed
A – Verify GASSP is implemented
A – Verify implementation of due care rules
A – Report to management and SA of status of due care rules
A – Report on GASSP implementation
A – Report violations of due care rules

(10) ***Education, Training, & Awareness***

E – List topics for inclusion into education, training and awareness plan
E – Recognize AT&E is a countermeasure
I – Develop education, training, and awareness plan

(11) ***Industrial Security***

E – Explain industrial security

(12) ***Information Warfare (INFOWAR) Concepts***

E – Explain INFOWAR concepts
A – Discuss INFOWAR

(13) ***Intellectual Property Rights***

E – Explain intellectual property rights
A – Verify SSM, viz., CIO, DAA, CTO, etc. understands intellectual property rights

(14) ***Interim Approval to Operate (IATO)***

E – Explain interim approval to operate
A – Verify SSM, viz., CIO, DAA, CTO, etc. can discuss IATO

(15) ***Investigative Authorities***

E – Explain investigative authorities
A – Verify SSM, viz., CIO, DAA, CTO, etc. can discuss investigative authorities

(16) ***Knowledge of Security Laws****

E – Discuss Clinger-Cohen Act
E – Discuss Computer Fraud and Abuse Act
E – Discuss Computer Security Act
E – Discuss Copyright Law of the United States and related laws
E – Discuss Copyright protection and licenses
E – Discuss Electronic Freedom of Information Act
E – Discuss Electronic Records Management and Federal Records Act
E – Discuss Federal Information System Management Act
E – Discuss Federal Managers Financial Integrity Act
E – Discuss Federal Property and Administration Service Act
E – Discuss Freedom of Information Act
E – Discuss Government Paperwork Elimination Act/Paperwork Reduction Act
E – Discuss Government Information Security Reform Act
E – Discuss Millennium Copyright Act
E – Discuss National Archives and Records Act
E – Discuss Privacy Act/Privacy Act issues
E – Discuss USA Patriot Act
E – Discuss computer crime and the various methods
E – Discuss international legal issues which can affect Information Assurance
E – Discuss the legal responsibilities of the SSM, viz., CIO, DAA, CTO, etc.
* As amended

(17) ***Lattice Model***

E – Define lattice model

(18) ***Law Enforcement Interfaces***

E – Explain law enforcement interfaces
A – Discuss law enforcement Interfaces

(19) ***Multi-level Security***

I – Discuss access control models

(20) ***Need for System Certification***

E – Explain need for system certification
A – Verify SSM, viz., CIO, DAA, CTO, etc. can discuss system certification requirements and processes

(21) ***Operating Security Features***

E – Explain operating security features

(22) ***Risk Management***

E – Explain risk management
I – Explain risks associated with agency policy for access by uncleared individuals and vendors
I – Explain risks associated with agency policy for redeploying classified systems
A – Discuss risk management

(23) ***Security Awareness as a countermeasure***

E – Define security awareness for information system users
I – Develop security awareness plan and materials for information system users
I – Discuss requirements for security awareness

(24) ***Security Education as a countermeasure***

E – Encourage employees to seek education in IA as a countermeasure
I – Discuss security education
I – Monitor changing security education requirements for information system users
A – Develop/design information system education programs

(25) ***Security Training as a countermeasure***

E – Define security training for information system users
I – Develop security training plan and materials for information system users
I – Discuss requirements for security training

(26) ***Software Licensing***

E – Explain software licensing
A – Discuss software licensing

(27) ***Software Piracy***

E – Explain software piracy
A – Discuss software piracy

(28) ***Systems Security Authorization Agreement (SSAA)***

E – Explain SSAA
A – Discuss SSAA

(29) *Systems Security Plan (SSP)*

E – Explain Systems Security Plan (SSP)
A – Discuss SSP

(30) *Standards of Conduct*

E – Explain standards of conduct

(31) *ITSEC/Common Criteria*

I – Discuss ITSEC/Common Criteria

(32) *Waive Policy to Continue Operation*

E – Explain Waive Policy to Continue Operation
A – Discuss Waive Policy to Continue Operation

E. SECURITY MANAGEMENT

(1) *Electronic Records Management*

E – Define electronic records management program and tools
E – Define underlying rules for electronic records management program
E - Describe the effect of electronic records management on the system
I – Explain electronic records management
I – Monitor electronic records management system
A – Verify implementation of records management program

(2) *Records Retention*

E – Discuss electronic records retention program
E – Define underlying rules for electronic records retention program
E – Describe effect of records retention system
E – List use of record retention
I – Monitor records retention program

(3) *E-Mail*

E – Address SA/staff about legal e-mail monitoring restrictions
E – Describe e-mail retention policies as they apply to system
E – Describe e-mail system/e-mail system security
E – Describe e-mail system and its potential vulnerabilities
E – Explain e-mail monitoring management with SA/staff
I – Develop e-mail monitoring management plan
I – Direct implementation of e-mail monitoring management plan
I – Direct operation of e-mail monitoring management plan
I – Direct SA to follow proper e-mail monitoring management procedures
I – Direct SA to help work force with e-mail monitoring management procedures
I – Direct SA/staff to follow appropriate laws and policies for e-mail monitoring
I – Direct SA/staff to follow proper e-mail monitoring procedures
I – Direct SA/staff to restrict access to e-mail monitoring functions and collected log files
I – Direct SA/staff to restrict access to e-mail monitoring system and collected information

I – Direct SA/staff to review relevant policy and procedures for e-mail monitoring management
I – Direct SA/staff to use e-mail monitoring management procedures
I – Discuss current e-mail monitoring management with necessary parties
I – Discuss e-mail monitoring management policies, laws, and penalties with personnel
I – Explain monitoring management plan
I – Monitor e-mail monitoring management plan training
I – Summarize e-mail monitoring management plan
I – Verify that necessary parties understand e-mail monitoring management plan and where it is maintained
A – Establish e-mail monitoring management policy for infractions
A – Implement e-mail monitoring management policy
A – Implement e-mail monitoring management reporting
A – Influence management on importance of having properly trained SA/staff to perform e-mail monitoring management plan on mission critical systems
A – Interpret legal aspects of e-mail monitoring systems
A – Propose e-mail monitoring management plan
A – Test e-mail monitoring management plan
A – Verify adherence to appropriate laws and policies for e-mail monitoring
E – Discuss appropriate laws and policies for e-mail monitoring
A – Verify adherence to e-mail monitoring procedures
A – Verify current e-mail monitoring management plan is available and accurate
A – Verify e-mail monitoring and auditing procedures and that they are being followed
A – Verify e-mail monitoring management plan is executed
A – Verify e-mail monitoring management policy is followed
A – Verify SA understands rules for e-mail monitoring management
A – Verify that a process for maintaining signed consent to monitoring forms exists
A – Verify that consent to monitoring banners are in place
A – Write e-mail monitoring management plan

(4) *Non-Repudiation*

E – Describe non-repudiation and its application to system
I – Explain non-repudiation
A – Verify non-repudiation is enforced
A – Verify non-repudiation is implemented

(5) *Hardware Asset Management*

E – Describe agency policy for access by uncleared individuals and vendors
E – Describe agency policy for redeploying classified systems
E – Describe hardware asset management program
E – Describe hardware asset management program and how it applies and is used on the system
I – Explain agency policy for access by uncleared individuals and vendors
I – Explain agency policy for redeploying classified systems
I – Propose hardware asset management process

A – Verify hardware accountability is performed at all levels
A – Verify reconstitution planning is implemented

(6) *Software Asset Management*

E – Describe agency policy for access by uncleared individuals and vendors
E – Describe agency policy for redeploying classified systems
E – Describe software asset management program
E – Describe software asset management program and how it applies and is used on the system
E – Describe software asset management program and how it applies/is used on system with emphasis on license and copyright issues, and cross reference to ethics
I – Enforce policies and procedures
I – Explain agency policy for access by uncleared individuals and vendors
I – Explain agency policy for redeploying classified systems
I – Promote compliance
A – Propose software asset management process
A – Report non-compliance
A – Verify software accountability is performed at all levels
A – Verify reconstitution planning is implemented

F. ACCESS CONTROLS

(1) *Human Access*

Require users and system support personnel to have required security clearances, authorizations and need-to-know; indoctrinate before granting access.

(a) Access Authorization

E – Address access management with SA/staff
E – Address SA/staff about legal access restrictions
E – Address work force about access management procedures
E – Describe agency policy for access by uncleared individuals and vendors
E – Address access management with SA/staff
E – Address SA/staff about legal access restrictions
E – Address work force about access management procedures
I – Develop access authorization processes plan
I – Develop access management plan
I – Direct implementation of access management plan
I – Direct operation of access management plan
I – Direct SA to follow proper access management procedures
I – Direct SA to help work force with access management procedures
I – Direct SA/staff to follow access control access procedures
I – Direct SA/staff to follow appropriate laws and policies
I – Direct SA/staff to follow proper access procedures
I – Direct SA/staff to restrict access to access system and collected information
I – Direct SA/staff to restrict access to access functions and collected log files
I – Direct SA/staff to review relevant policy and procedures for access management
I – Direct SA/staff to use access management procedures

I – Discuss access management policies, laws, and penalties with personnel
I – Discuss current access management with necessary parties
I – Develop access authorization processes plan
I – Develop access management plan
I – Direct implementation of access management plan
I – Direct operation of access management plan
I – Direct SA to follow proper access management procedures
I – Direct SA to help work force with access management procedures
I – Direct SA/staff to follow access control access procedures
I – Direct SA/staff to follow appropriate laws and policies
I – Direct SA/staff to follow proper access procedures
I – Direct SA/staff to restrict access to access functions and collected log files
I – Direct SA/staff to restrict access to access system and collected information
I – Direct SA/staff to review relevant policy and procedures for access management
I – Direct SA/staff to use access management procedures
I – Discuss access management policies, laws and penalties with personnel
I – Discuss current access management with necessary parties
I – Explain access authorization processes
I – Explain access management plan
I – Explain agency policy for access by uncleared individuals and vendors
I – Monitor access management plan training
I – Propose access management plan
I – Summarize monitoring management plan
I – Verify that necessary parties understand access management plan and where it is maintained
A – Establish access management policy for infractions
A – Implement access management policy
A – Implement access management reporting
A – Influence management on importance of having properly trained SA/staff to perform access management plan on mission critical systems
A – Interpret legal aspects of access systems
A – Revise policy document
A – Test access management plan
A – Verify access and auditing procedures and that they are being followed
A – Verify access authorization processes are implemented
A – Verify access management plan is executed
A – Verify access management policy is followed
A – Verify adherence to access procedures
A – Verify adherence to appropriate laws and policies access
A – Verify current access management plan is available and accurate
A – Verify SA understands rules for access management
A – Verify strategic items being under access management
A – Verify strategic placement of access systems
A – Verify that consent to access banners are in place
A – Write access management plan

(b) Access Control Software

E – Address access control software management with SA/staff
E – Address SA/staff about legal access restrictions
E – Address work force about access control software management procedures
E – Discuss access control software management policies, laws and penalties with personnel
E – Discuss current access control software management with necessary parties
I – Develop access control software management plan
I – Direct SA to follow proper access control software management procedures
I – Direct SA to help work force with access control software management procedures
I – Direct SA/staff to follow access control procedures
I – Direct SA/staff to follow appropriate laws and policies for access control software
I – Direct SA/staff to follow proper access control software procedures
I – Direct SA/staff to restrict access control software to access control software system and collected information
I – Direct SA/staff to restrict access control software to access control software functions and collected log files
I – Direct SA/staff to review relevant policy and procedures for access control software management
I – Direct SA/staff to use access control software management procedures
I – Explain access control software management plan
I – Monitor access control software management plan training
I – Summarize monitoring management plan
I – Verify that necessary parties understand access control software management plan and where it is maintained
A – Direct implementation of access control software management plan
A – Direct operation of access control software management plan
A – Establish access control software management policy for infractions
A – Implement access control software management policy
A – Implement access control software management reporting
A – Influence management on importance of having properly trained SA/staff to perform access control software management plan on mission critical systems
A – Interpret legal aspects of access control software systems
A – Propose access control software management plan
A – Revise policy document
A – Test access control software management plan
A – Verify access control software and auditing procedures and that they are being followed
A – Verify access control software management plan is executed
A – Verify access control software management policy is followed
A – Verify adherence to access control software procedures
A – Verify adherence to appropriate laws and policies for access procedures
A – Verify current access control software management plan is available and accurate
A – Verify SA understands rules for access control software management
A – Verify strategic items being under access control software management

A – Verify strategic placement of access control software systems
A – Verify that access to access control software is restricted
A – Write access control software management plan

(c) Account Management

E – Address account management with SA/staff
E – Address work force about account management procedures
I – Develop account management plan
I – Direct SA to follow proper account management procedures
I – Direct SA to help work force with account management procedures
I – Direct SA/staff to review relevant policy and procedures for account management
I – Direct SA/staff to use account management
I – Discuss account management policies, laws, and penalties with personnel
I – Discuss current account management with necessary parties
I – Explain account management plan
I – Monitor account management plan training
I – Revise policy document
I – Summarize account management plan
I – Verify that necessary parties understand account management plan and where it is maintained
A – Direct implementation of account management plan
A – Direct operation of account management plan
A – Establish account management policy for infractions
A – Implement account management policy
A – Implement account management reporting
A – Influence management on importance of having properly trained SA/staff to perform account management plan on mission critical systems
A – Propose account management plan
A – Revise policy document
A – Test account management plan
A – Verify account management plan is executed
A – Verify account management policy is followed
A – Verify current account management plan is available and accurate
A – Verify system administrator (SA) understands rules for account management
A – Write account management plan

(d) Authentication Policy

E – Address authentication with SA/staff
E – Address work force about authentication procedures
E – Discuss authentication policies, laws, and penalties with personnel
E – Discuss current authentication with necessary parties
I – Develop authentication plan
I – Direct SA to follow proper authentication procedures
I – Direct SA to help work force with authentication procedures
I – Direct SA/staff to review policy and procedures for authentication
I – Direct SA/staff to use authentication
I – Explain authentication plan
I – Monitor authentication plan training

I – Summarize authentication plan
I – Verify that necessary parties understand authentication plan and where it is maintained
A – Direct implementation of authentication plan
A – Direct operation of authentication plan
A – Establish authentication policy for infractions
A – Implement authentication policy
A – Implement authentication reporting
A – Influence management on importance of having properly trained SA/staff to perform authentication plan on mission critical systems
A – Propose authentication plan
A – Revise policy document
A – Test authentication plan
A – Verify authentication plan is executed
A – Verify authentication policy is followed
A – Verify current authentication plan is available and accurate
A – Verify SA understands rules for authentication
A – Write authentication plan

(e) Biometric Access Management

E – Address biometric access management with SA/staff
E – Discuss biometric access management policies, laws and penalties with personnel
E – Discuss current biometric access management with necessary parties
I – Develop biometric access management plan
I – Direct SA/staff to review relevant policy and procedures for biometric access
I – Direct SA/staff to use biometric access management techniques
I – Explain biometric access management plan
I – Monitor biometric access management plan training
I – Summarize biometric access management plan
I – Verify that necessary parties understand biometric access management plan and where it is maintained
A – Direct implementation of biometric access management plan
A – Direct operation of biometric access management plan
A – Implement biometric access incident notification policy
A – Implement biometric access incident reporting
A – Influence management on importance of having properly trained SA/staff to perform biometric access management plan on mission critical systems
A – Propose biometric access management plan
A – Test biometric access management plan
A – Verify biometric access plan is executed
A – Verify current biometric access management plan is available and accurate
A – Verify SA understands rules for biometric access management
A – Write biometric access management plan

(f) Clearance Verification

I – Develop clearance policy
A – Revise policy document
A – Verify clearance policy is implemented

(g) Need-to-Know Controls

I – Develop policy for need-to-know controls implementation
A – Revise policy document
A – Verify need-to-know controls are implemented

(h) Password Management

E – Address password management with SA/staff
E – Address work force authentication procedures
E – Discuss current password management with necessary parties
E – Discuss password management policies, laws, and penalties with personnel
I – Direct SA to follow proper authentication procedures
I – Direct SA to help work force with authentication procedures
I – Direct SA/staff to review policy and procedures for password
I – Direct SA/staff to review relevant policy and procedures for passwords
I – Direct SA/staff to use password management
I – Explain password management plan
I – Monitor password management plan training
I – Summarize password management plan
I – Verify that necessary parties understand password management plan and where it is maintained
A – Develop password management plan
A – Direct implementation of password management plan
A – Direct operation of password management plan
A – Establish policy for password infractions
A – Implement password incident notification policy
A – Implement password incident reporting
A – Influence management on importance of having properly trained SA/staff to perform password management plan on mission critical systems
A – Propose password management plan
A – Revise policy document
A – Test password management plan
A – Verify authentication policy is followed
A – Verify current password management plan is available and accurate
A – Verify password plan is executed
A – Verify SA understands rules for password management
A – Write password management plan

(i) Roles and Responsibilities (RBAC – Role Based Access Control)

I – Develop roles, responsibilities, and access controls policy
I – Explain roles, responsibilities, and access controls
A – Revise policy document
A – Verify roles, responsibilities and access controls are implemented

(j) Unauthorized Access

E – Address unauthorized access incident reporting with SA/staff
E – Discuss unauthorized access policies, laws, and penalties with personnel
I – Develop unauthorized access incident reporting plan
I – Direct implementation of unauthorized access incident reporting plan
I – Direct operation of incident reporting plan

I – Direct SA/staff to review relevant policy and procedures for unauthorized access
I – Direct SA/staff to review relevant policy and procedures for unauthorized access incident reporting
I – Direct SA/staff to use incident reporting
I – Discuss current incident reporting plan with necessary parties
I – Explain unauthorized access incident reporting plan
I – Monitor incident reporting plan training
I – Summarize unauthorized access incident reporting plan
I – Verify that necessary parties understand unauthorized access incident reporting plan and where it is maintained
A – Establish policy for unauthorized access infractions
A – Implement unauthorized access incident reporting
A – Implement unauthorized access notification policy
A – Influence management on importance of having properly trained SA/staff to perform unauthorized access incident reporting plan on mission critical systems
A – Propose incident reporting plan
A – Revise policy document
A – Test incident reporting plan
A – Verify current unauthorized access incident reporting plan is available and accurate
A – Verify SA understands rules for unauthorized access incident reporting
A – Verify unauthorized access incident reporting plan is executed
A – Write incident reporting plan

(2) *Key Management*

(a) COMSEC

E – Explain to users and managers what COMSEC process is and how COMSEC process is relevant to them
E – Identify COMSEC
E – Identify use for COMSEC material on system
E – Integrate services and advice of COMSEC Manager (Custodian) with operations
E – List national COMSEC policies
E – List national COMSEC procedures
I – Explain COMSEC policies and their relevance to users
I – Explain COMSEC policies and their relevance to SA
I – Explain COMSEC policies and their relevance to SSM, viz., CIO, DAA, CTO, etc.
I – Summarize COMSEC process
A – Report on COMSEC process
A – Review local COMSEC policies and procedures from an information assurance standpoint
A – Revise local policy document IAW national policies

(b) Key Certificate Administration (EKMS)

E – Define EKMS
E – Demonstrate knowledge of how to operate an EKMS system
E – Describe to users and managers what EKMS is, and how/why it is used

E – Describe to users and managers what key management is, and how/why EKMS is used
E – Identify components of EKMS as it applies to system
E – Identify EKMS requirements
E – Outline EKMS national policies and procedures and explain their relevance to users
E – Outline EKMS policies and procedures and explain their relevance to users
E – Outline national & agency EKMS management policies and procedures, and explain their relevance to users
E – Submit EKMS requirements
E – Use EKMS management in a system
I – Describe EKMS methodology
I – Design specific EKMS procedures for system in line with policies
I – Discuss EKMS
I – Explain EKMS
I – Prepare EKMS operating procedures for a system
I – Recommend approved EKMS technology
I – Use appropriate EKMS system
A – Compare differing public EKMS methodologies
A – Evaluate EKMS process for a system
A – Integrate EKMS management into overall system and procedures
A – Manage EKMS certificates
A – Report on EKMS implementation
A – Resolve EKMS conflict with procedures and policies, and variances thereof
A – Revise policy document
A – Verify EKMS procedures are in line with policy
A – Verify EKMS supports security management requirements
A – Verify implementation of EKMS

(c) Key Escrow

E – Describe to users and managers what key escrow is, and how/why it is used
E – Explain national key escrow policies and procedures
E – Use key escrow management in a system
A – Revise policy document IAW national policies
A – Verify key escrow procedures are in line with policy

(d) KMI

E – Define KMI
I – Discuss KMI
A – Report on KMI implementation

(e) Peer-to-Peer Security

E – Define peer-to-peer
E – Identify peer-to-peer requirements
I – Discuss peer-to-peer
I – Explain peer-to-peer
I – Submit peer-to-peer requirements
A – Report on peer-to-peer implementation
A – Revise policy document

A – Verify implementation of peer-to-peer
A – Verify peer-to-peer security concerns are addressed

(f) Public Key Infrastructure (PKI)

E – Define Public Key Infrastructure (PKI)
E – Demonstrate knowledge of how to operate a PKI system
E – Describe to users and managers what key management is, and how/why PKI is used
E – Describe to users and managers what PKI is, and how/why it is used
E – Identify components of PKI as it applies to system
E – Identify PKI requirements
E – Outline national & agency PKI management policies and procedures, and explain their relevance to users
E – Outline PKI national policies and procedures and explain their relevance to users
E – Outline PKI policies and procedures and explain their relevance to users
E – Submit PKI requirements
E – Use PKI management in a system
I – Describe PKI methodology
I – Design specific PKI procedures for system IAW national/local policies
I – Discuss PKI
I – Explain PKI
I – Manage PKI Certificates
I – Prepare PKI operating procedures for a system
I – Recommend approved PKI technology
I – Use appropriate PKI system
A – Compare differing public PKI methodologies
A – Evaluate PKI process for a system
A – Integrate PKI management into overall system and procedures
A – Report on PKI implementation
A – Resolve PKI conflict with procedures and policies, and variances thereof
A – Revise policy document
A – Verify implementation of PKI
A – Verify PKI procedures are in line with policy
A – Verify PKI supports security management requirements

G. INCIDENT RESPONSE

Security Investigation Procedures

E – Assist in investigations as requested
E – Describe process of investigating security incident
E – Follow procedures
E – Identify investigating authorities
I – Explain procedures to users and managers, significance of actions, and consequences for variations
I – Monitor compliance with procedure
I – Propose changes to procedures
I – Recommend training to avoid incident
A – Modify SSAA to reflect changes to mediate impact of incident
A – Review SA response

A – Review SSAA in light of incident
A – Verify higher authority/organizational/agency systems emergency/incident response team notification
A – Verify incident is reported
A – Verify remediation is executed

3. ENFORCE AND VERIFY SYSTEM SECURITY POLICY

A. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY/ACCOUNTABILITY (CIA)

(1) *Planning*

(a) Continuity Plans

E – Discuss continuity plans
I – Develop continuity plan
I – Enforce continuity plan
I – Explain continuity plans
A – Evaluate results of test of continuity plan
A – Prescribe changes resulting from evaluation of continuity plan
A – Prescribe oversight of continuity plans
A – Propose plan changes
A – Test continuity plan
A – Verify continuity plans are implemented
A – Verify continuity plans are reflected in SSAA
A – Verify items in continuity plan are in force
A – Evaluate execution of continuity plan
A – Evaluate execution of contingency plan

(b) Contingency Plans

E – Discuss contingency plans
I – Enforce contingency plan
I – Explain contingency plan
I – Develop contingency plan
I – Summarize contingency plan
A – Propose plan changes
A – Verify contingency plans are implemented
A – Verify items in contingency plan are in force
A – Prescribe oversight of contingency plans
A – Evaluate results of test of contingency plan
A – Test contingency plan
A – Verify contingency plan test results
A – Prescribe changes resulting from evaluation of contingency plan
A – Verify contingency plans are reflected in SSAA

(c) Reconstitution

E – Discuss reconstitution plans
I – Enforce reconstitution plan
I – Explain reconstitution plans
I – Develop reconstitution plan
A – Verify reconstitution plans are implemented
A – Verify items in reconstitution plan are in force
A - Propose plan changes

A – Prescribe oversight of reconstitution plans
A – Evaluate results of test of reconstitution plan
A – Test reconstitution plan
A – Prescribe changes resulting from evaluation of reconstitution plan
A – Verify reconstitution plans are reflected in SSAA
A – Evaluate reconstitution plan

(d) Disposition of Classified Material & Emergency Destruction Procedures (EDP)

E – Discuss disposition of classified material & EDP
I – Explain disposition of classified material & EDP
I – Enforce disposition of classified material & EDP
A – Prescribe oversight of disposition of classified material & EDP
A – Perform EDP
A – Evaluate results of test of EDP
A – Propose plan changes
A – Prescribe changes resulting from evaluation
A – Evaluate and test disposition of classified material and EDP

(e) Recovery

I – Summarize recovery plan
A – Verify recovery plan test results
A – Verify recovery plans are implemented

(f) Accountability

A – Verify individuals understand their accountability

(2) *Monitoring and Auditing*

(a) Alarms, Signals, & Reports

E – Discuss alarms, signals, and reports requirements
I – Enforce alarms, signals, and reports requirements
I – Explain alarms, signals, and reports requirements
I – Use analysis of intrusion indicators, when appropriate, and generate results
A – Prescribe changes that result from analysis
A – Prescribe oversight associated with alarms and signals
A – Prescribe changes resulting from evaluation alarms, signals, & reports
A – Test alarms, signals, and reports

(b) Intrusion Detection

E – Discuss intrusion detection problems
I – Direct intrusion detection enforced
I – Enforce intrusion detection requirements
I – Explain intrusion detection problems
A – Prescribe oversight associated with intrusion detection process
A – Test intrusion detection system
A – Verify intrusion detection is in accordance with policy

(c) Intrusion Deterrents

A – Verify SA/staff monitors intrusion deterrents status
A – Verify intrusion deterrents are current, operational, and tested
A - Verify intrusion deterrents are implemented and enforced

(d) Investigation of Security Breaches

E – Discuss security breaches
E– Define security breach
I – Discuss security breaches
I – Enforce requirements associated with investigations
I – Evaluate significance of security breaches
A – Evaluate results of security breaches
A – Implement policy for security breach
A – Prescribe changes resulting from evaluation of security breaches
A – Prescribe oversight associated with investigations
A – Test security breach detection systems
A – Verify security breach policy is implemented

(e) Monitoring

E – Define keystroke monitoring
E – Ensure legal requirements for monitoring are enforced
E – Identify potential monitoring problems
I – Discuss monitoring management policies, laws, and penalties with personnel
I – Enforce keystroke monitoring policy
I – Explain monitoring
I – Review reports of monitoring events
I – Explain consequences of unapproved monitoring
A – Implement monitoring policy
A – Prescribe changes that were identified as problems
A – Verify strategic items being monitored
A – Verify that consent to monitoring banners are in place
A – Verify that process for maintaining signed consent to monitoring forms exists

(f) Network Monitoring

E – Discuss network monitoring problems
E – Explain consequences of unapproved monitoring
I – Direct network monitoring
I – Enforce network monitoring requirements
I – Explain network monitoring problems
A – Evaluate results of network monitoring process
A – Prescribe changes resulting from evaluation of network monitoring process
A – Prescribe oversight associated with monitoring process
A – Test network monitoring system
A – Verify network monitoring is in accordance with policy

(3) *Environmental Controls*

E – Discuss environmental control issues
I – Direct environmental control testing as required
I – Explain environmental control requirements
A – Evaluate results from environmental control testing
A – Prescribe changes resulting from evaluation environmental control testing
A – Prescribe oversight associated environmental controls
A – Verify environmental control requirements are enforced

(4) *Filtered Power*

E – Discuss filtered power issues
I – Direct filtered power testing as required
I – Explain filtered power requirements
A – Evaluate results from filtered power testing
A – Prescribe changes resulting from evaluation of filtered power testing
A – Prescribe oversight associated filtered power
A – Verify filtered power requirements are enforced

(5) *Fire Prevention*

E – Discuss fire prevention issues
I – Direct fire prevention testing as required
I – Explain fire prevention requirements
A – Evaluate results from fire prevention testing
A – Prescribe changes resulting from evaluation of fire prevention testing
A – Prescribe oversight associated fire prevention
A – Verify fire prevention requirements are enforced

(6) *Grounding*

E – Discuss grounding issues
I – Direct grounding testing as required
I – Explain grounding requirements
A – Evaluate results from grounding testing
A – Prescribe changes resulting from evaluation of grounding testing
A – Prescribe oversight associated grounding
A – Verify grounding requirements are enforced

(7) *Safety*

E – Discuss safety issues
I – Direct safety testing as required
I – Explain safety requirements
A – Evaluate results from safety testing
A – Prescribe changes resulting from evaluation of safety testing
A – Prescribe oversight associated safety
A – Verify safety requirements are enforced

B. SECURITY MANAGEMENT

(1) *Electronic Records Management*

A – Verify electronic records management system is operated in accordance with policy
A – Verify implementation of records management program and describe effect on system

(2) *Records Retention*

I – Monitor records retention program
A – Verify electronic records retention management system is operated in accordance with policy

A – Verify implementation of records retention program and describe effect on system

(3) *E-Mail*

I – Monitor e-mail program
A – Verify e-mail system is operated in accordance with policy
A – Verify implementation of e-mail system and describe effect on system
A – Verify that privacy laws are enforced

(4) *Non-Repudiation*

A – Verify implementation of non-repudiation

(5) *Hardware Asset Management*

A – Verify hardware asset accountability is enforced at all levels

(6) *Software Asset Management*

A – Verify software asset accountability is enforced at all levels

C. ACCESS CONTROLS

(1) *Human Access*

Require users and system support personnel to have required security clearances, authorizations and need-to-know, and are indoctrinated before granting access
E – Describe agency policy for access by uncleared individuals and vendors
I – Explain agency policy for access by uncleared individuals and vendors

(a) Access Authorization

A – Revise access authorization policy document
A – Verify access authorization policy is integrated into overall system and procedures
A – Verify access authorization procedures are enforced

(b) Access Control Software

A – Revise access control software policy document
A – Verify access control software policy is integrated into overall system and procedures
A – Verify access control software procedures are enforced

(c) Account Administration

E – Verify requested access
I – Direct account administration tests
I – Enforce account administration policy
A – Prescribe oversight associated with account administration tests
A – Revise account management policy document
A – Verify account management policy is integrated into overall system and procedures
A – Verify account management security procedures are enforced

(d) Authentication Policy

A – Revise authentication policy document
A – Verify authentication policy is integrated into overall system and procedures
A – Verify authentication procedures are enforced

(e) Biometric Access Management

A – Revise biometric access management policy document
A – Verify biometric access management policy is integrated into overall system and procedures
A – Verify biometric access management procedures are enforced
A – Prescribe oversight associated with biometric access management tests

(f) Clearance Verification

A – Revise clearance verification policy document
A – Verify clearance verification policy is integrated into overall system and procedures
A – Verify clearance verification procedures are enforced

(g) Need-to-Know Controls

I – Direct need-to-know tests
I – Enforce need-to-know policy
A – Evaluate need-to-know requirements
A – Evaluate results of need-to-know tests
A – Implement need-to-know policy
A – Prescribe need-to-know changes resulting from evaluation
A – Prescribe oversight associated with need-to-know tests
A – Revise need-to-know policy document
A – Verify need-to-know policy is integrated into overall system and procedures
A – Verify need-to-know procedures are enforced

(h) Password Management

A – Prescribe oversight associated with password management tests
A – Revise password management policy document
A – Verify password management policy is integrated into overall system and procedures
A – Verify password management procedures are enforced

(i) Roles and Responsibilities (RBAC – Role Based Access Control)

A – Revise RBAC policy document
A – Verify RBAC policy is integrated into overall system and procedures
A – Verify RBAC procedures are enforced

(j) Unauthorized Access

E – Discuss unauthorized access attempts
A – Evaluate results of test of unauthorized access policy
A – Perform test of unauthorized access procedures
A – Prescribe changes resulting from evaluation
A – Prescribe oversight for access policy
A – Revise unauthorized access policy document
A – Verify unauthorized access policy is integrated into overall system and procedures
A – Verify unauthorized procedures are enforced

(2) *Key Management*

(a) COMSEC

E – List national COMSEC policies

E – List national COMSEC procedures
A – Revise policy document
A – Verify COMSEC procedures are enforced

(b) Key Certificate Administration (EKMS)

A – Revise policy document
A – Verify EKMS management is integrated into overall system and procedures
A – Verify EKMS procedures are enforced

(c) Key Escrow

E – Explain national key escrow policies and procedures
A – Revise policy document
A – Verify key escrow procedures are enforced

(d) Peer-to-Peer Security

A – Revise policy document
A – Verify peer-to-peer security management is integrated into overall system and procedures
A – Verify peer-to-peer security procedures are enforced

(e) Public Key Infrastructure (PKI)

A – Verify PKI management is integrated into overall system and procedures
A – Verify PKI procedures are enforced

(3) *Configuration Management*

E – Identify configuration management requirements
I – Direct configuration management tests
I – Direct change control
I – Enforce configuration management policy
I – Enforce change control
I – Explain configuration management
I – Explain change control
I – Explain configuration management requirements
I – Perform security testing prior to implementation ensuring changes made to systems do not violate security policy
I – Require accountability of copyrighted software in accordance with software licensing agreements
A – Evaluate configuration management requirements
A – Evaluate change control
A – Evaluate results of configuration management tests
A – Implement configuration management policy
A – Implement change control
A – Prescribe configuration management changes resulting from evaluation
A – Prescribe oversight associated with configuration management tests

(4) *Protective Technology*

E – Identify protective technology requirements
I – Direct protective technology tests
I – Enforce protective technology policy
I – Explain protective technology requirements

A – Evaluate protective technology requirements
A – Evaluate results of protective technology tests
A – Implement protective technology policy
A – Prescribe oversight associated with protective technology tests
A – Prescribe protective technology changes resulting from evaluation

(5) *Media Security*

(a) FAX Security
I – Enforce procedures governing FAX security

(b) Lines (Fiber, Copper, Wireless)
I – Enforce appropriate security measures for each type of media
I – Enforce security needs for leased lines
I – Enforce security needs for owned lines

(c) Modems
I – Enforce policy and practices for modem security

(d) Phone Mail
I – Enforce procedures governing phone mail security

(e) TEMPEST
I – Enforce procedures governing EMSEC/TEMPEST security

(f) Voice Communication Security
I – Enforce procedures governing voice communications security

(g) Wireless communication security
I – Enforce procedures governing wireless communications security

(6) *Network Assurance*

(a) Network Security
I – Direct network security tests
I – Enforce network security requirements
A – Evaluate results of network security tests
A – Monitor use of network security
A – Prescribe changes resulting from evaluation
A – Prescribe oversight associated with network security tests

(b) Network Boundaries and Perimeters
I – Direct network boundaries and perimeters security tests
I – Enforce network boundaries and perimeters security requirements
A – Evaluate results of network boundaries and perimeters security tests
A – Monitor use of network boundaries and perimeters security
A – Prescribe changes resulting from evaluation
A – Prescribe oversight associated with network boundaries and perimeters security tests

D. AUTOMATED SECURITY TOOLS

(1) *Automated Security Tools*

E – Use expert system tools (i.e., audit reduction and intrusion detection) available
I – Direct automated security tools tests
I – Enforce use of automated security tools

A – Evaluate results of automated security tools and tools tests
A – Integrate use of automated security tools
A – Monitor use of automated security tools
A – Prescribe changes resulting from evaluation
A – Prescribe oversight associated with use of automated security tools

(2) *Initiate Protective and/or Corrective Measures*

I – Enforce protective or corrective measures
I – Enforce security clearance, authorization, and need-to-know requirements

E. HANDLING MEDIA

(1) *Handling Media*

I – Enforce media/information handling requirements

(2) *Labeling*

I – Enforce security media/information marking requirements
A – Verify labeling procedure policy is implemented

(3) *Marking of Media/Information Systems Oversight Office (ISOO) Rules*

I – Enforce security media/information marking requirements
A – Verify Information Systems Oversight Office (ISOO) procedure policy is implemented

(4) *Marking of Sensitive Information*

I – Enforce security media/information marking requirements
A – Verify marking procedure policy is implemented

(5) *Physical Controls & Accounting*

I – Enforce security physical controls and accounting requirements
A – Verify physical controls and accounting procedure policy is implemented

(6) *Remanence*

E – Execute non-automated data remanence tools
I – Enforce information remanence requirements
A – Verify remanence procedure policy is implemented

(7) *Transportation*

I – Enforce transportation security requirements
A – Verify transportation procedure policy is implemented

(8) *Disposition of Classified Material*

E – Explain disposition of classified media policies and procedures
E – Define disposition reports
A – Report discrepancies with disposition

F. INCIDENT RESPONSE

(1) *Criminal Prosecution*

E – Discuss criminal prosecution requirements
I – Enforce criminal prosecution requirements

(2) *Evidence Acceptability*

I – Enforce rules on evidence acceptability
A – Prescribe oversight associated with evidence acceptability in investigations

(3) *Evidence Collection and Preservation*

I – Assist in evidence collection
I – Discuss problems associated with evidence collection
I – Enforce evidence collection and preservation security requirements
A – Evaluate evidence collection procedures
A – Monitor evidence collection and preservation security
A – Prescribe changes resulting from evidence collection
A – Verify that evidence collection and preservation policy is implemented

(4) *Legal and Liability Issues*

E – Discuss legal liability issues
E – Identify legal liability issues
I – Discuss legal liability issues
I – Enforce legal and liability security requirements
I – Explain legal liability issues
I – Summarize legal liability issues

4. REPORT ON SITE SECURITY STATUS

A. SECURITY CONTINUITY REPORTING

(1) *Contingency Plans*

E – Define contingency plan reporting
I – Report on status of restoration of information systems

(2) *Continuity Plans*

(a) Reconstitution

E – Define continuity plan reporting
E – Define reconstitution reporting
A – Report implementation of Continuity plan
A – Report status of reconstitution of systems

(b) Restoration

E – Define restoration reports
E – Define backup reports
A – Report on status of back ups
A – Report on status of restoration

(3) *Disposition of Classified Material & Emergency Destruction Procedures (EDP)*

E – Define disposition reports
E – Define EDP reports
A – Report discrepancies with disposition
A – Report implementation of EDP

(4) *Monitoring and Auditing*

(a) Audit

I – Discuss auditing reports

(b) Alarms, Signals, & Reports

E – Explain reporting audit alarms and signals
A – Report audit alarms and signals

(c) Assessments (e.g., surveys, inspections)

E – Explain how to report audit assessments
A – Report findings and recommendations

(5) *Identification & Authentication*

(a) Account Administration

E – Describe process to report unauthorized accounts
A – Report unauthorized accounts

(b) Password Management

E – Describe process to report insufficient passwords
A – Report insufficient password

(c) Unauthorized Access

I – Discuss what reporting is required for unauthorized access

A – Report unauthorized access

(6) *Configuration Management*

E – Describe configuration management reporting requirements
A – Report changes in configuration to SSM, viz., CIO, DAA, CTO, etc.
A – Report on recommendations for configuration management
A – Report security issues for configuration management

(7) *Testing*

E – Describe how various types of testing are reported
I – Prepare testing reports
A – Report adverse side affects of testing to SSM, viz., CIO, DAA, CTO, etc.
A – Report when testing is completed to SSM, viz., CIO, DAA, CTO, etc.
A – Report when testing is scheduled to SSM, viz., CIO, DAA, CTO, etc.

B. REPORT SECURITY INCIDENTS

(1) *Computer Organizational/Agency Systems Emergency/Incident Response Team*

E – Identify organizational/agency systems emergency/incident response team
E – Distribute organizational/agency systems emergency/incident response team reports and advisories
A – Report security issues to organizational/agency systems emergency/incident response team
A – Report violations, incidents, and breaches appropriately

(2) *Security Incidents*

A – Report security incidents in accordance with agency-specific/local policy to SSM, viz., CIO, DAA, CTO, etc. when information system compromised
A – Respond to attacks/incidents

(3) *Security Violations Reporting Process (incident response)*

E – Comply with agency specific/local directives when reporting to SSM, viz., CIO, DAA, CTO, etc.
E – Describe process of responding and reporting of security incidents
I – Assist users and managers with reporting
A – Report on evaluated damage done by an incident
A – Report recommended actions, changes, modifications to information assurance program and practices based upon an incident
A – Report results of an incident response

C. LAW

(1) *Investigative Authorities*

E – Identify agencies and offices responsible for investigating security incidents
I – Explain what information is reported to which agencies and offices
A – Report appropriate information as defined in security policy to appropriate agencies and offices
A – Report investigative efforts to SSM, viz., CIO, DAA, CTO, etc.

(2) *Law Enforcement Interfaces (LEI)*

E – Describe how ISSO interfaces with law enforcement agencies
E – Describe how to contact law enforcement interfaces (LEI)
I – Explain how to use assistance from LEI
A – Report and coordinate with LEI
A – Report LEI activities to SSM, viz., CIO, DAA, CTO, etc.

(3) *Witness Interviewing/Interrogation*

E – Assist appropriate authority in witness interviewing/interrogation
E – Describe proper procedures to follow when conducting a witness interview
E – Identify who can conduct interrogations (investigative agencies only)

(4) *Entrapment*

I – Discuss notification requirements to use entrapment techniques
A – Report use of entrapment techniques being instituted for compliance with policies and guidelines
A – Verify that entrapment activities are approved by organizational/agency systems emergency/incident response team and SSM, viz., CIO, DAA, CTO, etc.
A – Verify that entrapment in the legal sense does not occur

(5) *Disgruntled Employees*

E – Identify notification requirements for handling disgruntled employees
I – Know legal rights of disgruntled employees before reporting
A – Report behavior of disgruntled employees to appropriate authorities
A – Report identification of disgruntled employees to appropriate authorities

D. REPORT SECURITY STATUS OF INFORMATION SYSTEM AS REQUIRED BY SSM, VIZ., CIO, DAA, CTO, ETC.

(1) *Administrative Security Policies and Procedures*

E – Explain necessity of reporting on administrative security policies and practices
I – Prepare report of non-compliance to SSM, viz., CIO, DAA, CTO, etc.
I – Propose modifications to current policies and procedures
A – Report recommendations for corrective/remedial action for non-compliance
A – Report shortfalls in current policies and procedures

(2) *Agency Specific Security Policies*

E – Describe how agency specific policies enhance overall security posture of information systems by defining operational environment
I – Comply with agency specific security policies when reporting security status to SSM, viz., CIO, DAA, CTO, etc.

(3) *Organizational/Agency Systems Emergency/Incident Response Team*

E – Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems
I – Compile information from various sources for compilation into status report
A – Disseminate status report

(4) ***Automated Systems Security Incident Support Team (ASSIST)***

E – Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems
I – Compile information from various sources for compilation into status report
A – Disseminate status report

(5) ***Trade Journals, Bulletin Board System (BBS) Notices***

E – Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems
I – Compile information from various sources for compilation into status report
A – Disseminate status report

E. REPORT TO IG

Inspector General (IG) (External) Audit & Assessments

E – Describe areas encompassed by report
E – Identify appropriate reporting channels for IG
A – Integrate IG results into report

5. SUPPORT CERTIFICATION AND ACCREDITATION

Ensure information system is accredited and certified if it processes sensitive information

A. CERTIFICATION FUNCTION

(1) ***Assessments (e.g., surveys, inspections)***

E – Prepare assessments for use during certification of information systems
I – Develop assessments for purpose of certifying information systems
I – Review assessments for purpose of certification of information systems

(2) ***Risk Assessment***

I – Direct risk assessment of information systems

(3) ***Technical Certification***

I – Direct technical certification of information systems

(4) ***Verification and Validation Process***

I – Direct verification and validation process as part of certification of information systems

B. ACCREDITATION FUNCTION

(1) ***ISSO***

E – Monitor system status post accreditation
E – Initiate accreditation process
I – Organize accreditation process
I – Direct efforts of users in accreditation process
A – Complete accreditation process
A – Support obtaining SSM, viz., CIO, DAA, CTO, etc. approval

(2) ***Managers***

I – Ensure the re-accreditation of the system
I – Direct efforts of Managers in accreditation process

(3) ***System Administrator (SA)***

E – Explain contents of Systems Security Plan (SSP)
I – Direct efforts of SA in accreditation process
I – Direct writing of SSP
I – Write SSP for simple information system
A – Write/maintain SSP
A – Write SSP for complex information system

C. RESPOND TO SSM, VIZ., CIO, DAA, CTO, ETC. REQUESTS

(1) ***Approval to Operate***

E – Explain purpose and contents of Approval to Operate (ATO) to users
I – Direct risk assessment to support granting an ATO
A – Conduct risk assessment to support granting an ATO

A –Guide implementation of risk mitigation strategies necessary to obtain ATO

(2) *Assessment Methodology*

E – Explain C&A process for information system
I – Direct C&A effort for information systems
A – Conduct C&A effort for information systems

(3) *Certification Statement*

E – Explain purpose and contents of Certification Statement to users
I – Direct C&A effort leading to Certification Statement
A – Conduct C&A effort leading to Certification Statement

(4) *Certification Tools*

E – Discuss certification tools
E – Discuss ST&E plan and procedures
E – Recommend revisions to ST&E plan and procedures
E – Recommend use of specific certification tools
I – Direct use of certification tools
I – Review results of execution of certification tools
I – Review results of execution of ST&E plan and procedures
A – Analyze results of carrying out ST&E plan and procedures
A – Analyze results of certification tools
A – Develop security test and evaluation plan and procedure
A – Execute certification tools

(5) *Identify Security Changes to SSM, viz., CIO, DAA, CTO, etc.*

E – Differentiate security-related changes from non-security-related changes
E – Explain security-relevant changes to be made to information system
I – Determine if re-certification is warranted

(6) *Interim Approval to Operate (IATO)*

E – Explain purpose and contents of Interim Approval to Operate (IATO) to users
I – Direct risk assessment to support granting an IATO
A – Conduct risk assessment to support granting an IATO
A –Guide implementation of risk mitigation strategies necessary to obtain IATO

(7) *Re-Certification*

E – Explain purpose and process of re-certification
E – Identify information system that needs re-certification
I – Direct re-certification effort
A – Conduct re-certification effort

(8) *Security Test & Evaluation (ST&E)*

E – Discuss ST&E
A – Work with ST&E team to write test plan

(9) *SSAA*

E – Explain contents of SSAA
I – Direct writing of SSP
I – Recommend modifications to the SSAA

I – Write SSAA for simple information system
A – Influence certifier in development of SSAA to ensure mission
A – Write SSAA for complex information system

(10) *Type Accreditation*

E – Explain purpose and contents of type accreditation to users
I – Direct risk assessment to support accreditation
A – Conduct risk assessment to support accreditation
A – Guide implementation of risk mitigation strategies necessary to obtain accreditation

(11) *Waive Policy to Continue Operation*

E – Explain justification for waiver
I – Conduct risk assessment to support granting waiver
A – Guide implementation of risk mitigation strategies necessary to obtain waiver

ANNEX B

REFERENCES

The following references pertain to this instruction:

1. Common Criteria for Information Technology Security Evaluation, dated Aug 1999
2. DoD Directive 8000.1, Management of Information Resources and Information Technology, dated 27 Feb 2002
3. DoD Directive 8500.1, Information Assurance, dated 24 Oct 2002
4. DoD Instruction 8500.2, Information Assurance (IA) Implementation, dated 6 Feb 2003
5. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), dated 30 Dec 1997
6. DoD 8510.1M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, dated 31 Jul 2000
7. EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, dated 3 Apr 1984
8. EO 13231, Critical Infrastructure Protection in the Information Age, dated 16 Oct 2001 as amended by EO 13286, Transfer of Certain Functions to the Secretary of Homeland Security, dated 28 Feb 2003
9. Federal Information Processing Standards Publication (FIPS) Publication 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, dated Jun 1974
10. Federal Information Processing Standards Publication (FIPS) Publication 65, Guideline for Automatic Data Processing Risk Analysis, dated 1 Aug 1993
11. Federal Information Processing Standards Publication (FIPS) 87, Guidelines for ADP Contingency Planning, dated 27 Mar 1981
12. Federal Information Processing Standards Publication (FIPS) Publication 102, Guideline for Computer Security Certification and Accreditation, dated 27 Sep 1983
13. National Computer Security Center (NCSC) TG-005, Trusted Network Interpretation (TNI), dated 31 Jul 1987
14. National Computer Security Center (NCSC)-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities for Automated Information Systems, dated May 1992
15. National Computer Security Center (NCSC)-TG-029, Version 1, Introduction to Certification and Accreditation, dated Jan 1994
16. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, dated Oct 1995
17. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, dated Sep 1996
18. NIST SP 800-16, Information Technology Security Training Requirements: A Role and Performance-based Model, dated Apr 1998
19. NIST SP 800-18, Guide for Development of Security Plans for Information Technology Systems, dated Dec 1998

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