NSTISSI No. 4012
August 1997

NATIONAL TRAINING STANDARD

FOR

DESIGNATED

APPROVING AUTHORITY (DAA)

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY

NATIONAL MANAGER

FOREWORD

1. This instruction establishes the minimum course content or standard for the development and implementation of training for Designated Approving Authorities in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this instruction from:

NATIONAL SECURITY AGENCY
NSTISSC SECRETARIAT
ATTN: V503 STE 6716
FORT GEORGE G. MEADE, MD 20755-6716

KENNETH A. MINIHAN
Lieutenant General, USAF

NATIONAL TRAINING STANDARD FOR DESIGNATED APPROVING AUTHORITY (DAA)

SECTION I - PURPOSE

1. This instruction establishes the minimum training standard for the development and implementation of training for a Designated Approving Authority (DAA) in the disciplines of telecommunications and information systems (IS) security.

SECTION II - APPLICABILITY

2. National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501 establishes the requirement for federal departments and agencies to implement training programs for information systems security (INFOSEC) professionals. As defined in NSTISSD 501, an INFOSEC professional is an individual responsible for the security oversight or management of national security systems during phases of the life cycle. That directive is being implemented in a synergistic environment among departments and agencies which are committed to satisfying these INFOSEC 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 4014). The definitions for words used in this instruction are derived from the National INFOSEC Glossary, NSTISSI No. 4009. The references pertinent to this instruction are listed in ANNEX B.

3. The body of knowledge listed in this instruction may be obtained from a variety of sources, i.e., the National Cryptologic School, the General Services Administration (Office of Information Security), and Government contractors, as well as from adaptations of existing department/agency training programs, or from a combination of experience and formal training. ANNEX A lists the minimal INFOSEC performance standard for a DAA.

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 DAAs in the disciplines of telecommunications and IS security.

SECTION III - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure that DAAs 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:

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

b. ensure that appropriate INFOSEC training courses for DAAs are developed; and

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

ANNEX A

MINIMAL INFOSEC PERFORMANCE STANDARD FOR THE DAA

Job functions using competencies identified in:

DoD 5200.28-M, Automated Data Processing Security Manual
NCSC-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities For Automated Information Systems
NCSC-TG-029, Version 1, Introduction to Certification and Accreditation
NCSC-TG-005, Trusted Network Interpretation
FIPS Publication 102, Guideline for Computer Security Certification and Accreditation.

The INFOSEC functions of a DAA are:

(1) granting final approval to operate an IS or network in a specified security mode;
(2 reviewing the accreditation documentation to confirm that the residual risk is within acceptable limits;
(3) verifying that each Information System complies with the IS security requirements, as reported by the Information Systems Security Officer (ISSO);
(4) ensuring the establishment, administration, and coordination of security for systems that agency, service, or command personnel or contractors operate;
(5) ensuring that the Program Manager (PM) defines the system security requirements for acquisitions;
(6) assigning INFOSEC responsibilities to the individuals reporting directly to the DAA;
(7) approving the classification level required for applications implemented in a network environment;
(8) approving additional security services necessary to interconnect to external systems (e.g., encryption and non-repudiation);
(9) reviewing the accreditation plan and sign the accreditation statement for the network and each IS;
(10) defining the criticality and sensitivity levels of each IS;
(11) reviewingthe documentation to ensure each IS supports the security requirements as defined in the IS and network security programs;
(12) allocating resources to achieve an acceptable level of security and to remedy security deficiencies;
(13) establishing working groups, when necessary, to resolve issues regarding those systems requiring multiple or joint accreditation. This may require documentation of conditions or agreements in Memoranda of Agreement (MOA); and
(14) ensuring that when classified or sensitive but unclassified information is exchanged between logically connected components, the content of this communication is protected from unauthorized observation by acceptable means, such as cryptography, and Protected Distribution Systems (PDS).

Terminal Objective:

Given a final report requesting approval to operate a hypothetical information system at a specified level of trust, the DAA will analyze and judge the information for validity and reliability to ensure the hypothetical system will operate at the proposed level of trust. This judgement will be made based on system architecture, system security measures, system operations policy, system security management plan, and provisions for system operator and end user training.

List of performance items under competencies

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

1. LEGAL LIABILITIES ISSUES

a. Legal Issues

(1) explain the legal responsibilities of the DAA;
(2) discuss the Computer Fraud and Abuse Act, P.L. 99-474, 18 U.S. Code 1030;
(3) discuss Copyright Protection and License, Copyright Act of 1976, Title 17 U.S. Code, P.L. 102-307, amended the Copyright Act of 1976, 1990;
(4) discuss the Freedom of Information Act;
(5) discuss the purpose and history of NSD 42;
(6) discuss implications of the Privacy Act;
(7) list and discuss the issues of Computer Security Act of 1987 (P.L. 100-235); and
(8) list international legal issues which can affect INFOSEC.

b. Liabilities

(1) state the importance of annual loss expectancy;
(2) list the damage which can occur when anti-virus programs are not used;
(3) determine the responsibilities associated with the business aspects of INFOSEC; and
(4) explain the legal responsibilities of the data owner.

c. Crime

(1) explain how audit analysis tools can be useful in crime analysis;
(2) explain the importance of written procedures for evidence collection and preservation;
(3) illustrate the importance of written procedures for investigation of security breaches;
(4) describe how collection methods can affect evidence acceptability;
(5) list the ways logs/journals can be important evidence in a suspected criminal investigation; and
(6) describe the DAA role in witness interview and interrogation.

d. Issues

(1) explain the dangers of not using your agency's Computer Emergency Response Team (CERT);
(2) discuss the effects of disregarding COMSEC policy and guidance;
(3) illustrate the ramifications of improper disposition of classified information;
(4) determine the effects of threats to electronic data interchange to systems in your agency;
(5) explain the consequences of damage occurring to electronic funds transfer to systems in your agency;
(6) explain how unauthorized modifications to electronic mail affect your agency;
(7) outline the vulnerabilities associated with electronic records management;
(8) describe the liabilities associated with electronic monitoring;
(9) illustrate how fraud, waste, and abuse of computer resources can affect your agency's system security;
(10) define the term "Information Warfare" (INFOWAR);
(11) explain the DAA's role in information warfare through the use of INFOSEC;
(12) describe ways in which connecting to the National Information Infrastructure can create risks to your systems;
(13) define the term "national security information";
(14) explain the DAA's role in the security violations reporting process;
(15) discuss the importance of separation of duties;
(16) explain software piracy; and
(17) explain DAA responsibility for preventing unauthorized disclosure of information.

e. Contracts, Agreements, and Other Obligations

(1) define for the contractor the DAA involvement in the development of new systems;
(2) explain to the contractor the DAA involvement in maintenance agreements; and
(3) describe to the contractor the DAA involvement in classified systems.

2. POLICY

a. Computer Security Policy

(1) define the term “computer security policy"; and
(2) identify national security information using Executive Order 12958.

b. P. L. 100-235, Computer Security Act of 1987

(1) explain the purpose of P. L. 100-235; and
(2) outline the roles and responsibilities assigned by P. L. 100-235.

c. OPM 5 CFR 930, Training Requirements for the Computer Security Act

(1) explain the purpose of OPM 5 CFR 930; and
(2) describe responsibilities under OPM 5 CFR 930.

d. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems

(1) evaluate the purpose of OMB Circular A-130; and
(2) summarize the responsibilities assigned by OMB Circular A-130.

e. Freedom of Information Act

discuss importance of the Freedom of Information Act.

f. National Security Directive (NSD) 42

explain the purpose and history of NSD 42.

g. Electronic Records Management

(1) identify public law related to electronic records management; and
(2) discuss the concept of electronic mail as an electronic record.

h. Other Federal Statutes

relate the following Federal Acts to INFOSEC:
Federal Managers Financial Integrity Act of 1982
Federal Property and Administration Service Act
Federal Records Act
National Archives and Records Act
Privacy Act of 1974 (P. L. 93-579, U.S. Code 532(a))

i. Copyright Protection and License

(1) acknowledge that copyright laws protect literary expression only if a copyright has been

registered;
(2) distinguish between patent laws which protect products and contract laws which cover trade secrets;
(3) determine which protection (copyright, patent, or contract) applies to a computer applications program;
(4) identify basic concepts of software licensing;
(5) identify legal policy against software piracy; and
(6) discuss system software contracts.

j. Guiding Directives

(1) state the purpose of federal information processing standards;
(2) explain the purpose of National Security Telecommunications and Information Systems Security (NSTISS) publications;
(3) discuss the purpose of National Institute of Standards and Technology (NIST) publications;
(4) explain the DAA responsibilities assigned by the Department of Defense Trusted Computer System Evaluation Criteria (DOD 5200.28-STD), or Orange Book; and
(5) explain the content of the Rainbow Series of documents.

k. Access Control Policy

(1) define the DAA's responsibility for security policy statements relating to access control;
(2) explain the general concept underlying access control models; and
(3) establish an access authorization process.

l. Sensitive Data

(1) define policy statements relating to accountability for sensitive data;
(2) use an approved method of providing individual accountability and access verification; and
(3) define process for designation of sensitive data, applications and systems and marking and handling of sensitive data.

m. Local Policy

(1) establish agency specific INFOSEC policy and procedure;
(2) identify command authority(s) relating to INFOSEC;
(3) identify INFOSEC roles and responsibilities by local policy; and
(4) determine policy for local storage area controls.

n. Accreditation

(1) define the term "accreditation authority";
(2) establish accreditation policy;
(3) identify the directive allowing delegation of authority;
(4) delegate responsibilities in the accreditation process, if permitted;
(5) establish policy for recertification; and
(6) define security requirements for accreditation.

o. Threats, Vulnerabilities, and Incidents

(1) identify policy which must be followed for handling computer security incidents;
(2) establish policy for handling computer security incidents;
(3) incorporate information from assistance programs into local policy as appropriate for the organization (e.g., the Computer Security Technical Vulnerability Reporting Program (CSTVRP),

the Automated Information Systems Security Incident Support Team (ASSIST), The Computer Incident Advisory Capability (CIAC), and the CERT);
(4) identify legal investigative authorities by agency specific charter;
(5) identify requirements for the CERT; and
(6) identify requirements for vulnerability reporting to the CERT.

p. Documentation Policies

(1) state documentation policies to which the DAA must adhere;
(2) establish documentation policies as required; and
(3) establish change control policies.

q. Issues

(1) discuss the concept of common criteria;
(2) define computer matching responsibilities;
(3) define intellectual property rights;
(4) discuss legal liabilities issues;
(5) explain legal liability issues for maintenance procedures for contract employees;
(6) explain legal liability issues for maintenance procedures for local employees;
(7) discuss policy requiring separation of duties; and
(8) discuss local and national policy for national security systems monitoring.

3. THREATS AND INCIDENTS

a. Definitions

(1) define the term “adversary"; and
(2) define the term “threat.”

b. Compromise

(1) discuss the impact of a compromise by these definitions: the disclosure of classified data to an unauthorized person; an unauthorized disclosure, modification, destruction, or loss of sensitive information; disclosure of a password, or part of a password, to someone not authorized to know, have, or use the password; authorized disclosure or loss of sensitive data; and

(2) describe why the common thread among compromise definitions is “an unauthorized disclosure.”

c. Computer Crime

(1) summarize how computer crime can involve either the computer as a tool or the computer as a target; and
(2) outline the methods of computer crime: fraud, embezzlement, and unauthorized access.

d. Security Incident

outline the categories of security incidents: compromise, possible compromise, inadvertent disclosure, deviation, and any adverse event associated with a computer system that is a failure to comply with departmental security regulations or directives.

e. Malicious Code

(1) define the term “malicious code”;
(2) define the term “malicious logic”; and

(3) give examples of effects of the following malicious code or logic: logic bomb, time bomb, trap door, trojan horse, virus, worm, back-door, maintenance hook, and spoofing.

f. Malicious Actions

give example of the effects of the following malicious actions: active attack, wire tapping, browsing, covert channel, jamming, software piracy, passive attack, traffic analysis, and monitoring.

g. Non-Specific Concerns

discuss the following types of non-specific threats to systems and information: contamination, data contamination, data corruption, and cascading.

h. Protection Techniques

discuss the effects of the following protection techniques: anti-virus program, audit analysis tools, electronic monitoring, intrusion detection, monitoring (e.g., dataline, sniffer), and traffic analysis.

i. Incident Handling

(1) explain the role of the DAA in criminal prosecution;
(2) explain the importance of evidence acceptability in incident handling;
(3) explain the impact of evidence collection and preservation in incident handling;
(4) identify responsibilities associated with evidence collection and preservation in incident handling;
(5) discuss responsibilities for investigation of security breaches; and
(6) explain the DAA role in security violations reporting.

4. ACCESS

a. Access Concepts

(1) define the term “access";
(2) identify who can issue access authorization;
(3) discuss how access levels are determined;
(4) explain how privileges are derived from the risk management process;
(5) define the term “least privilege";
(6) explain the concept of discretionary access control; and
(7) explain the concept of mandatory access control.

b. Access Control Measures

(1) explain the purpose of access control rosters and list-based access controls as means of discretionary access control;
(2) discuss the function of access control software;
(3) discuss the purpose of role-based access controls; and
(4) state the criteria for rules-based access controls.

c. Access Tools

(1) explain how biometrics mediate access;
(2) compare the concept of access mode to attributes;
(3) determine responsibilities associated with password management;

(4) state the purpose of one-time passwords;
(5) explain the concept of single sign-on;
(6) discuss issues of smart card/token authentication;
(7) identify personnel responsible for clearance verification; and
(8) define the term “access period.”

5. ADMINISTRATIVE (DAA administrative responsibility)

a. Responsibilities for Account Administration

(1) specify local accreditation procedures;
(2) identify accreditation authority;
(3) state policy for ADP security documentation;
(4) identify ADP security staff personnel and their location;
(5) outline audit collection requirements;
(6) recognize importance of audit tools;
(7) describe business aspects of information systems security as they apply to proprietary information;
(8) state procedures for disseminating information from the Computer Emergency Response Team (CERT);
(9) state procedures for reporting to the CERT;
(10) outline procedures for providing information to or gathering information from the CSTVRP, the ASSIST, the CIAC, or the CERT, as appropriate for the organization;
(11) outline procedures for handling computer security incidents;
(12) discuss contractor security standards;
(13) outline procedures for contractor security safeguards under National Industrial Security Program Operations Manual (NISPOM);
(14) outline DAA responsibilities for contracts, agreements, and other obligations;
(15) discuss the importance of customer information technology security needs;
(16) describe the results of a customer service orientation and whether they support information systems security policy and procedures;
(17) outline policy for deletion of accounts;
(18) outline policy for required documentation;
(19) discuss the risks associated with electronic funds transfer; and
(20) discuss issues associated with electronic monitoring.

b. Administration

(1) discuss the risks associated with electronic records management;
(2) evaluate the significance of reliability testing;
(3) plan procedures which protect against remanence;
(4) discuss the purpose of security functional testing;
(5) outline security inspection procedures;
(6) describe the security product testing/evaluation process;
(7) describe DAA responsibilities for security staffing requirements;
(8) discuss the security principles related to separation of duties; and
(9) explain the concept of electronic digital signature.

6. COMSEC

a. General

(1) explain the impact of a COMSEC compromise;
(2) outline responsibilities for COMSEC accounting;

(3) identify the COMSEC custodian or COMSEC manager;
(4) explain how COMSEC material destruction and procedures can affect INFOSEC;
(5) describe methods of COMSEC material identification;
(6) identify responsibilities for COMSEC policy and guidance; and
(7) identify responsibilities associated with a controlling authority.

b. Technology

(1) identify cryptographic techniques;
(2) summarize the importance of the Electronic Key Management System to INFOSEC;
(3) evaluate encryption modes;
(4) define private key cryptography;
(5) define public key encryption;
(6) explain the concept of protective technology;
(7) discuss how the concept of two-person control may enhance information systems security; and
(8) associate voice communication security with INFOSEC.

7. TEMPEST

a. General

(1) identify the TEMPEST manager for your agency;
(2) list the responsibilities of the TEMPEST manager;
(3) identify the Certified TEMPEST Technical Authority (CTTA);
(4) list the responsibilities of the CTTA;

(5) discuss the principle of compromising emanations in relation to INFOSEC; and
(6) define the term “control zone.”

b. Technical

(1) discuss the principle of electromagnetic interference in relation to INFOSEC;
(2) explain the concept protected distribution system to include: approved telecommunications system for the transmission of unencrypted sensitive information; system must have safeguards: electromagnetic, physical, acoustical, electrical, and the transmission may be optical or electrical;
(3) discuss the red/black concept;
(4) define the term “shielded enclosures"; and
(5) compare a TEMPEST zone to a shielded enclosure.

8. GENERAL

a. Introductory

(1) explain information security problems which may occur at an access node;
(2) explain the property of accountability to include: traceability of activities to individual users; assigning responsibility for violations, attempted violations, and activities;
(3) explain the purpose for the Assessed Products List (APL);
(4) define the term “approved circuit";
(5) discuss why authentication is an important process in INFOSEC to include:
  (a) positive validation for a claimed identity which may be: station, originator, individual, transmission, message, user, device;
  (b) positive validation may also be called: identification or verification; and
  (c) protective measure used to deter fraudulent transmissions.
(6) identify who is involved in the Authorization process (the DAA, his/her designee(s), and the

extent of their authority) in your organization;
(7) describe the resources and methods of an automatic message processing system; and
(8) list general operations security (OPSEC) principles and sources of information.

b. DAA Authority

(1) explain the objectives of the information systems security program: availability, denial of service, confidentiality, integrity;
(2) outline the business aspects of information security;
(3) describe the components of a classified COMSEC program;
(4) explain why compartmentalization is an important aspect of INFOSEC;
(5) describe how connectivity impacts both your systems and external systems;
(6) define the term “critical processing";
(7) identify critical systems within your purview;
(8) describe how criticality is a parameter which indicates the degree of dependence of your organization on an asset;
(9) explain the purposes for a computer security working group;
(10) define the term “data owner";
(11) explain the purpose for degaussing magnetic media;
(12) explain why the disposition of classified data is important for secure processing;
(13) demonstrate the differences between INFOSEC education, training, and awareness (ET&A);

(14) illustrate how electronic data interchange (EDI) is susceptible to security incidents;
(15) describe the contents of the Evaluated Products List (EPL);
(16) outline the principles of ethics as they apply to INFOSEC;
(17) identify the ISSO in your agency;
(18) define the term “INFOWAR";
(19) outline the INFOSEC dangers in the National Information Infrastructure;
(20) compare open system security and closed security;
(21) describe operating system security features;
(22) define the term “platform specific security;”
(23) list the importance of maintaining professional interfaces;
(24) identify professional interfaces;
(25) illustrate the importance of quality assurance to INFOSEC;
(26) explain the importance of security architecture in a distributed system;
(27) list the forms in which security products are available: hardware, firmware, software;
(28) identify sensitive systems for which you are responsible;
(29) outline the components of technical security as listed in NSD 42: equipment, components, devices, associated documentation, media;
(30) define the term “trust” as it applies to INFOSEC;
(31) apply the term “warranties (assurance)” to the concept of INFOSEC; and
(32) explain the consequences of improper or damaged cabling.

9. LIFE CYCLE MANAGEMENT

a. Role

(1) discuss the DAA role and responsibilities associated with life cycle management;
(2) discuss the DAA role and responsibility in acquisition;
(3) discuss the DAA role in development life cycle phase; and
(4) outline responsibilities for validation reporting.

b. Impact

(1) discuss the importance of an acceptance inspection;
(2) outline responsibilities associated with an acceptance test;
(3) discuss the impact of an acceptance trial;
(4) explain the impact of a critical design review (CDR);
(5) describe the value of a contract data requirements list (CDRL);
(6) recognize the importance of conformance testing;
(7) evaluate the significance of requirements traceability in INFOSEC; and
(8) compare a software architecture study and system security architecture study.

10. CONTINUITY OF OPERATIONS (COOP)

a. COOP Concepts

(1) explain how alternate routing can affect INFOSEC measures;
(2) compare PBX security and alternate routing;
(3) compare application development control to COOP;
(4) distinguish between backup, contingency, disaster, and recovery plans;
(5) discuss the importance of continuity of operations;
(6) define the elements of a continuity plan;
(7) outline the procedures for continuity planning;
(8) examine the relation of emergency destruction procedures to COOP;
(9) associate the risks associated with environmental/natural threats to COOP to include: wind, earth movement, fire, water, dust, temperature, humidity static, and power;
(10) recognize system fault tolerance limits;
(11) recommend basic recovery procedures;
(12) evaluate the importance of redundancy to COOP; and
(13) explain how the system testing & evaluation process relates to COOP.

b. Backup

(1) outline the responsibilities associated with a backup plan; and
(2) specify backup procedures.

c. Configuration Management

(1) discuss how change controls affect COOP;
(2) discuss the role of the Configuration Control Board;
(3) specify configuration controls;
(4) explain the purpose of configuration documentation maintenance; and
(5) discuss the role of the Configuration Review Board.

d. Contingency Management

(1) define contingency planning;
(2) specify the requirements within a contingency plan; and
(3) specify requirements for contingency plan testing.

e. Disaster Recovery

(1) discuss the actions required by disaster recovery planning; and
(2) clarify the importance of disaster recovery plan testing.

f. Storage Area Controls

(1) justify the importance of storage area controls;
(2) explain the contents of storage area controls;
    (a) backup of data, information, software;
    (b) protection of the original diskettes for software;
    (c) protection of the storage media;
    (d) storage area locale; and
    (e) storage area access; and
(3) compare storage media protection and control to storage area controls.

11. RISK MANAGEMENT

a. General

illustrate the following in the risk acceptance process:
    (a) differentiate between risk, threat, and vulnerability;
    (b) explain the purpose of a risk assessmen;
    (c) clarify the term “residual risk";
    (d) outline the process of a risk analysis;
    (e) identify the individual responsible for determining an acceptable level of risk;
    (f) differentiate between a cost-benefit analysis and a cost-risk analysis for the purpose of risk management;
    (g) identify the automated risk evaluation system used by system certifiers;
    (h) explain the benefits of conducting a threat assessment;
    (i) define the term “acceptance";
    (j) determine what constitutes acceptance certification for the systems for which you are responsible; and
    (k) describe the similarities and differences between the risk analysis process and the OPSEC process.

b. Responsibility

(1) assign responsibilities associated with accreditation for the systems for which you are responsible;
(2) identify vulnerabilities resulting from add-on security;
(3) identify vulnerabilities resulting from propagation of risk;
(4) describe when aggregation of data becomes a risk;
(5) describe how the OPSEC process is used to assess the risk posed by aggregated data acquired through the entire spectrum of intelligence collection systems of the threat;
(6) assign responsibilities for applications security;
(7) determine the procedures for granting approval to operate;
(8) outline the mechanisms which provide assurance;
(9) give an example of a breach;
(10) outline DAA responsibilities for a certification and accreditation program; and
(11) distinguish between certification as a process and as a decision.

c. Procedures & Techniques

(1) complete the following regarding media and memory:
    (a) compare the processes of clearing, purging, and degaussing;
    (b) explain why remanence is an important factor in risk management;
    (c) contrast non-volatile memory with volatile memory;
    (d) explain the importance for written procedures in the disposition of classified information recorded as media and data;
(2) describe common carrier security protection applicable to risk management;
(3) explain the requirements for each of the modes of operation:

compartmented/partitioned mode,
controlled security mode,
dedicated mode,
multilevel security mode,
system high security mode;

(4) determine policies related to decertification;
(5) describe the types of documentation which are important in the risk management process;
(6) define the term “environmental controls";
(7) define the term “evaluation";
(8) outline procedures for “generic accreditation";
(9) identify which identification and authentication techniques are implemented in the risk management process, and evaluate the merits of the techniques;
(10) explain the importance of information sensitivity in the risk management process;
(11) outline procedures for granting interim approval;
(12) explain how intrusion detection can be accomplished;
(13) describe the reasons for joint accreditation;
(14) explain the purpose of a maintenance hook;
(15) describe metrics used by the DAA in the risk management process;
(16) explain the purpose of monitoring (e.g., dataline, sniffer) in the assessment process;
(17) explain the DAA role in multiple accreditation;
(18) explain how firewalls form a protection technique;
(19) determine the procedures involved in an operational procedures review;
(20) illustrate the purpose of penetration testing;
(21) describe the concept of periods processing;
(22) define the term risk management;
(23) state the DAA’s responsibility in establishing security policy;
(24) describe the importance of separation of duties;
(25) outline the DAA’s responsibility for storage area controls;
(26) outline the DAA’s responsibility for storage media protection and control;
(27) identify vulnerabilities arising from system integration;
(28) discuss the concept of a trusted computing base; and
(29) explain the concept of a trusted path.

ANNEX B

REFERENCES

The following references pertain to this Instruction:

a. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, dated 16 November

b. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, June 5, 1992

c. DoD 5200.28-M, Automated Data Processing Security Manual, dated January 1973

d. NCSC-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities For Automated Information Systems

e NCSC-TG-029, Version 1, Introduction to Certification and Accreditation

f. National Computer Security Center TG-005, Trusted Network Interpretation (TNI), dated July 31, 1987

g. FIPS Publication 102, Guideline for Computer Security Certification and Accreditation

h. P.L. 100-235, Computer Security Act of 1987, dated January 8, 1988

i. Office of Personnel Management (OPM), 5 Combined Federal Regulation (CFR) Part 930, Training Requirements for the Computer Security Act, dated January 3, 1992

j. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, dated February 8, 1996

k. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990

l. DoD 5200.28-STD, Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985