DRAFT

NSTISSI No. 4015

NATIONAL EDUCATION AND

TRAINING STANDARD

FOR

SYSTEM CERTIFIERS

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

DRAFT

National Security Telecommunications and Information Systems Security Committee

NATIONAL MANAGER

FORWARD

1. This instruction establishes the minimum course content or standard for the development and implementation of education and training for System Certifier professionals 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: I42
9800 SAVAGE ROAD (SAB 3)
FT. GEORGE G. MEADE, MD 20755-6716

MICHAEL V. HAYDEN
Lieutenant General, USAF

DRAFT

NSTISSI 4015

NATIONAL EDUCATION AND TRAINING STANDARD
FOR
SYSTEM CERTIFIERS

SECTION I - PURPOSE

1. This instruction and the attached annexes establish the minimum education and training standard for the development and implementation of education and training for System Certifier(s) 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 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 committed to satisfying these INFOSEC education and training requirements in the most effective and cost 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). Concomitant capabilities required by the System Certifier(s) to perform the job functions competently are provided in ANNEX B of this instruction. The definitions for terminology used in this instruction are derived from the National INFOSEC Glossary, NSTISSI No. 4009. The references pertinent to this instruction, as well as other documents which can be used in conjunction with it, are listed in ANNEX C.

3. The body of knowledge required by this instruction may be obtained from a variety of sources, i.e., DISA, NSA, and Government contractors, as well as from adaptations of existing department/agency education and training programs, or from a combination of

experience and formal training. ANNEX A lists the minimal INFOSEC performance standard for a System Certifier(s).

4. This instruction is applicable to all U.S. Government departments and agencies as well as Government contractors responsible for the development and implementation of education and training for telecommunications and IS security System Certifier(s).

SECTION III - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure System Certifiers (or their equivalents) are made aware of the body of knowledge outlined in this instruction, and provide such education and training to those requiring it at the earliest practicable date.

6. The National Manager shall:

a. maintain and provide an INFOSEC education and training standard for System Certifier(s) to U.S. Government departments and agencies;

b. ensure appropriate INFOSEC education and training courses for System Certifier(s) are developed; and

c. assist other U.S. Government departments and agencies in developing and/or conducting INFOSEC education and training activities for System Certifier(s) as requested.

SECTION IV - PREFACE

7. The System Certifier is an individual or a member of a team which performs the comprehensive multidisciplined assessment of the technical and non-technical security features and other safeguards of an information system in an operational configuration, made in support of the accreditation process. The Certifier(s) identifies the assurance levels achieved in meeting all applicable security policies, standards and requirements for the Designated Approving Authority (DAA), who in turn determines whether or not an information system and/or network is operating within the bounds of specified requirements and at an acceptable level of risk. For the purposes of this document, we have defined "System Certifier" to avoid any confusion between it and the Department of Defense definition of "certification authority," as well as the NSTISSC definition of "certification agent." In this document, the term "System Certifier" is used as defined above.

8. The designated Certification Authority (sometimes referred to as "certification agent," as defined in NSTISSI 4009) is ultimately responsible for determining the correct skill sets required to adequately certify the system, and for identifying personnel to accomplish the

comprehensive evaluation of the technical and non-technical security features of the system. The scope and the complexity of the information system determine whether the Certifier will be an individual or a member of a team performing the certification. The Certifiers' responsibilities evolve as the system progresses through the life-cycle process. Because an in-depth understanding and application of the certification and accreditation (C&A) process is required of the System Certifier(s), these professionals operate at the highest level of the Information Technology Security Learning Continuum model referenced in the National Institute of Standards and Techology (NIST) Special Publication No. 800-16. According to this model, learning starts with awareness, builds to training, and evolves into education, the highest level. Overall the performance items contained in this training standard are at that advanced level.

9. To be a qualified System Certifier, one must first be formally trained in the fundamentals of INFOSEC, and have field experience. It is recommended that System Certifier(s) have system administrator and/or basic information system security officer (ISSO) experience, and be familiar with the knowledges, skills and abilities (KSAs) required of the Designated Approving Authority (DAA). Throughout the complex information systems certification process, the Certifier(s) exercises a considerable amount of INFOSEC-specific as well as non-INFOSEC-specific KSAs. ANNEX A lists the actual performance items under each of the System Certifier KSAs, which in turn are outlined under each of the major job functions. Concomitant capabilities, provided in ANNEX B, are those capabilities which are exercised together with and simultaneously while performing a specified Certifier job function.

10. While this Instruction was developed using the National Information Assurance Certification and Accreditation Process (NIACAP) as a framework, this training standard employs common knowledge, skill, and attribute requirements that can be extended to develop courseware for any certification and accreditation process.

DRAFT

ANNEX A

MINIMAL INFOSEC PERFORMANCE STANDARD FOR SYSTEM CERTIFIER(S)

Job functions using competencies identified in:

NSTISSI 1000, National Information Assurance Certification and Accreditation Process (NIACAP)
DoD Instruction 5200.40, DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)
NCSC-TG-029, Version 1, Introduction to Certification and Accreditation
FIPS Publication 102, Guideline for Computer Security Certification and Accreditation
NCSC-TG-031, Certification and Accreditation Process Handbook for Certifiers
I942-TR-002, Version 1, Accreditor's Guideline
SC-2610-143-93, DoD Intelligence Information Systems (DoDIIS) Site Certifier's Guide
DoDIIS Security Certification and Accreditation Guide

Job Functions

The INFOSEC functions of System Certifiers are performed during the following phases of the certification process:

(1) Documenting Mission Need

The System Certifier(s) needs to develop a comprehensive understanding of the mission and the functional responsibilities in order to ensure the success of the C&A processes. Certifiers must possess a global understanding of the C&A process, the system and the mission it supports.

(2) Conducting Registration

Registration involves the collection of information needed to address the certification process in a repeatable, understandable, and effective manner. These tasks involve gathering information to determine the security requirements and the level of effort necessary to accomplish C&A. The level of effort is influenced by the degree of assurance needed in the areas of confidentiality, integrity, accountability, and availability. Certifiers must consider the mission, environments, system life-cycle, existing documentation, risk, architecture, users, data classifications, external interfaces, etc.

(3) Performing Negotiation

Negotiation is involved in every facet of the C&A process. Given the potentially large numbers of people and functional organizations involved, Certifiers must draw upon many sub-disciplines and roles to accomplish this mission. To this end, Certifiers must possess broad, well-developed negotiation skills. Negotiation skills are especially important for determining methodologies, defining the scope of the certification process, and acquiring the resources necessary to support the mission. Effective written and oral communication skills, flexibility, creativity, political acumen, and objectivity all contribute to effective negotiation activities.

(4) Preparing the System Security Authorization Agreement (SSAA)

The Certifier(s) is part of a team composed of the Certification Authority, the program sponsor, a threat specialist and others. This team prepares the SSAA, a document that describes the planned operating condition of the system being certified and the expected residual risk in operating the system. The Designated Approving Authority (DAA) approves the SSAA and the system is then implemented with the security requirements that have been determined for it. It is important to note that the SSAA is a living document, and as such will require periodic maintenance throughout the life-cycle management of the system.

(5) Supporting Systems Development

During the systems development phase of a system certification, the Certifier(s) is responsible for evaluating the design of the system and ensuring that the security requirements are being properly addressed and satisfied. The specific activities are a function of the overall program strategy, the life-cycle management process, and the position of the information system in the life-cycle. As in the Certification Analysis phase, the system development activities ensure that the requirements of the SSAA are followed during each life-cycle phase of the development and modification of the information system.

(6) Performing Certification Analysis

Certification Analysis is the process of interacting with the system developer or owner/operator, and reviewing the documentation to carefully assess the functionality of the developing system, ensuring that it meets the security requirements as defined for its users, environment, connectivity, and other technical and non-technical factors in the SSAA.

(7) Certification Evaluation

Security certification evaluation is the process whereby the Certifier(s) verifies and validates through formal security testing and evaluation (ST&E), that the implementation of the information system (IS) complies with the technical and non-technical security requirements stated in the SSAA, and that any observed deficiencies are fully documented and presented to the DAA for consideration in the accreditation decision.

(8) Developing Recommendation to the DAA

The Certifier(s) prepares appropriate documentation regarding all findings resulting from the ST&E, and recommends to the DAA the degree to which the evaluated system satisfies all the defined security requirements. In addition, this documentation offers the Certifier's opinion concerning any identified residual risk that may preclude accreditation of the system for operation.

(9) Compliance Validation

The Certifier's focus during this phase is the audit of the accredited IS, which is operating under the approval of the DAA, who has accepted any identified residual risk. Therefore, the Certifier(s) audits operations to ensure they remain consistent with the DAA-accepted level of risk.

(10) Maintenance of the SSAA

The Maintenance of the SSAA function involves determining whether or not any IS implementation changes that dictate a need to recertify the implementation of the IS will

require an update of the SSAA. If changes occur that dictate a need for a recertification effort, then the Certifier functions as defined in the C&A process are again performed for these changes, or for the entire IS as necessary. Additionally, Certifiers must ensure that the recertification effort is reported to the DAA for continued approval to operate.

Terminal Objective:

Given an information system, the System Certifier(s) will explain and apply a recognized methodology leading to the security certification of that system in accordance with a prescribed set of criteria (i.e., the International Common Criteria), and provide an accreditation recommendation to the DAA for consideration in the accreditation decision. To be acceptable, the certification must be performed in accordance with applicable INFOSEC regulations, policies and guidelines.

List of performance items under competencies

In each of the competency areas listed below, the System Certifier(s) shall perform the following functions:

1. DOCUMENTING MISSION NEED

a. Knowledge and/or Awareness of Security Laws

(1) identify relevant nation-state security laws, treaties, and/or agreements;
(2) interpret nation-state security laws, treaties, and/or agreements in relation to mission accomplishment;
(3) relate the identified nation-state security laws, treaties, and/or agreements to the mission needs;
(4) discuss identified nation-state security laws, treaties, and/or agreements with involved site personnel; and
(5) explain interpretation in support or denial of certification to involved site personnel.

b. Coordination with Related Disciplines

(1) identify the related disciplines required for accomplishing the IS certification; and
(2) discuss mission-specific discipline relationships and IS requirements with involved site personnel.

c. Understand Mission

(1) study the mission critical elements, to include system mission, functions, and system interfaces;
(2) verify that mission critical elements are completely identified (e.g., operational procedures and classification requirements);

(3) confirm the mission description is complete as it relates to documented IS needs, to include system life cycle; and
(4) discuss the interpretation of mission critical elements in support or denial of certification with involved site personnel; and
(5) research and discuss mission operational environment (e.g., charter, scope of authorities, activation call-up procedures, Information Warfare Condition (INFOCON) processes).

d. Contingency Planning

(1) assess the need for contingency planning;
(2) study the identified critical contingency elements;
(3) confirm that the critical elements of mission contingency planning have been identified in relation to the specific operational environment;
(4) discuss the critical contingency elements and IS requirements in relation to mission accomplishment to assure system recovery and reconstitution;
(5) explain the appraisal in support or denial of certification to involved site personnel; and
(6) verify that the documented mission need elements are identified in the critical system contingency plan.

2. CONDUCTING REGISTRATION

a. System Certification Memorandum of Understanding (MOU) or Other Instruments

(1) propose the development of a MOU or other appropriate instruments;
(2) describe the purpose, scope, and contents of a particular MOU or other instruments;
(3) identify the respective parties and their roles;
(4) discuss anticipated challenges to a MOU or other instruments;
(5) explain the various details of a MOU or other instruments;
(6) interpret the agreements specified in a MOU or other instruments;
(7) use a MOU or other instruments to define the responsibilities and requirements for team members with specialized knowledge;
(8) use a MOU or other instruments to assist in SSAA and other policy development;
(9) comply with the requirements of a system certification MOU or other instruments;
(10) verify the integrity of a MOU or other instruments; and
(11) report the status of MOUs or other instruments to the DAA.

b. Collect Security Requirements

(1) describe the security requirement collection process;
(2) research security requirements; and
(3) describe to the DAA, program management office (PMO), etc., the appropriate requirements for system security.

c. Knowledge and/or Awareness of Security Laws Required for System Being Evaluated

(1) explain the applicable laws, statutes, and regulations;
(2) discuss how the system will operate according to legal mandates; and
(3) identify the organizational point of contact for legal advice.

d. Audit Collection Requirements

(1) describe the audit collection requirements relative to system certification; and
(2) assist in the identification of audit requirements.

e. Coordination with Related Disciplines

(1) discuss the role of related security disciplines in the overall protection of the system;
(2) describe the related security disciplines and how they apply to the certification of the system; and
(3) identify the related disciplines needed for the certification team.

f. Configuration Control Policies

(1) advise in the development of configuration control policies;
(2) assess the system configuration control plan against policy; and
(3) report to the DAA the deficiencies/discrepancies in the configuration control policy.

g. Contingency Planning

(1) assess the need for contingency planning;
(2) propose contingency planning activities;
(3) discuss the contingency planning process;
(4) assess contingency planning; and
(5) report to the DAA any discrepancies or deficiencies in contingency plans.

h. Personnel Selection

(1) explain the criteria for personnel selection for the certification team; and
(2) perform personnel selection for the certification team based on the requisite skills for the IS involved.

i. Roles and Responsibilities

(1) identify and define the roles and responsibilities of the certification team; and
(2) propose the roles and responsibilities of individual certification team members.

j. Scope and Parameters of the Certification

(1) describe, define, and present the scope and parameters of the certification.

k. Set Certification Process Boundaries

(1) define and describe the certification process boundaries; and
(2) identify and propose the boundaries of the certification process.

l. Risk Management

(1) select the appropriate risk management methodology for the IS to be certified;
(2) discuss the risk management methodology and threat mitigation using examples and explanations; and
(3) describe the risk management methodology appropriate to the certification of the system.

m. System Description

(1) verify that the system description is consistent with the documented mission need.

n. System Security Policy

(1) ensure the development and inclusion of a comprehensive system security policy; and
(2) assess policy to ensure it conforms with applicable laws and directives and data owner requirements.

o. Budget/Resources Allocation

(1) define and describe budget elements related to the certification process; and
(2) identify the resource requirements necessary to accomplish the certification process.

p. Timeline/Scheduling

(1) establish certification milestones; and
(2) relate the milestones to roles and responsibilities.

q. Life-Cycle System Security Planning

(1) assess life-cycle security planning against requirements, directives and laws;
(2) describe life-cycle security planning; and
(3) assist in life-cycle security planning with respect to the certification requirements.

3. PERFORMING NEGOTIATION

a. Life-Cycle System Security Planning

(1) explain life-cycle system security planning;
(2) propose life-cycle system security attributes to involved site personnel; and
(3) propose improvements to the plans developed by site personnel.

b. Set Certification Process Boundaries

(1) discuss setting certification boundaries;
(2) describe setting certification boundaries;
(3) influence certification boundaries;
(4) justify setting certification boundaries; and
(5) report the setting of certification boundaries as part of the SSAA.

c. Risk Management

(1) appraise elements of life-cycle activity versus the risk management process components of mission, vulnerabilities, threat, and countermeasures to determine if system development activity is ready for certification.

d. Knowledge and/or Awareness of Security Laws

(1) use the knowledge and awareness of security laws to ensure system development activities follow legal guidelines.

4. PREPARING SSAA

a. Access Control Policies

(1) categorize access control policies;
(2) describe access control policies; and
(3) relate access control policies to appropriate "umbrella" guidance and policies.

b. Security Policies and Procedures

(1) define and understand the topics that security policies and procedures must address as part of the certification process;
(2) discuss the impact of policy and procedures on risk and operations;
(3) explain how the system operating policies and procedures define the implementation of the security requirements;
(4) integrate the identified security policies and procedures (i.e. audit policies, access control policies) as minimum requirements into the ST&E plan;

(5) interpret the relationship between security policy and procedures and the security requirements;
(6) assist the DAA, program manager (PM), and user in understanding the security policies and procedures; and
(7) describe the security solutions and implementations that meet the specified system security requirements.

c. Documentation Policies

(1) identify documentation policies that apply to the preparation of the SSAA; and
(2) ensure that the appropriate documentation policies are followed in preparing the SSAA.

d. Requirements Derivation

(1) categorize security certification requirements;
(2) discuss how technical and non-technical security requirements are derived;
(3) identify requirements that are applicable to the system under certification and accreditation;
(4) identify the source of the security requirements;
(5) identify the source of the security requirements for use during negotiations, development of the SSAA, and compliance validation;
(6) interpret security requirements for the specific mission, environment, data classification level, and architecture;
(7) summarize the security requirements and construct a requirements traceability matrix (RTM);
(8) use security requirements to assist in the development of ST&E plans;
(9) verify that security certification requirements are included in the ST&E plan; and
(10) explain the security requirements in order to develop a common understanding among the DAA, PM, and Certification Authority.

e. Understand Mission

(1) describe the system mission focusing on the security relevant features of the system required for the SSAA;
(2) discuss the purpose of the system and its capabilities in the SSAA;
(3) explain the impact of the mission statement on security requirements;
(4) summarize the mission and prepare a summary for the SSAA; and
(5) use the mission statement to identify applicable security certification requirements in the SSAA.

f. Security Domains

(1) identify any specific security domains as they apply to the system mission and function; and
(2) relate the interactions between different security domains in support of the system mission and functions.

g. System Description

(1) appraise the system concept of operations (CONOPS);
(2) assess the system's criticality and its impact on the level of risk that is acceptable;
(3) define the system user's characteristics and clearances;
(4) define the security clearances of the user population and the access rights to restricted information;
(5) define the type of data and data sensitivity;
(6) describe the system CONOPS and security CONOPS in the SSAA;
(7) describe the system criticality in the SSAA;
(8) describe the system functions and capabilities;
(9) examine the mission to determine the national security classification of the data processed;
(10) identify the system acquisition strategy and system life-cycle phase; and
(11) use the data sensitivity and labeling requirements to determine the system classification.

h. Environment and Threat Description

(1) derive the system operating environment and threat descriptions from the mission documentation; and
(2) prepare a description of potential threats based upon an analysis of the operating environment, and the system development environment for inclusion in the certification reports for the DAA.

i. System Operating Environment

(1) describe the administrative security procedures appropriate for the system being certified;
(2) analyze the physical environment in which the system will operate; address all relevant parts of the system's environment, including descriptions of the physical, administrative, developmental and technical areas; describe any known or suspected threats specifically to be considered for the described environment;
(3) describe the security features that will be necessary to support site operations (the physical security description should consider safety procedures for personnel operating the equipment);
(4) identify maintenance procedures needed to ensure physical security protection against unauthorized access to protected information or system resources;
(5) identify procedures needed to counter potential threats that may come from inside or outside of the organization;
(6) identify the physical support features of the facility, including air conditioning, power, sprinkler system, fences, and extension of walls from true-floor to true-ceiling construction, sensitive space, work space, and the building;
(7) determine if training procedures match the users' levels of responsibility, and provide information on potential threats and how to protect information; and
(8) identify aspects of physical security, such as a defined secure work area; the means used to protect storage media (e.g., hard drives and removable disks); protecting access to workstation ports (e.g., communication ports); a controlled area for shared resources (e.g., databases and file servers); and the means of protection used for cable plant and

communication hubs and switches which are used to connect workstations and shared resources.

j. System Development, Integration, and Maintenance Environment

(1) describe the system development approach and the environment within which the system will be developed and maintained;
(2) describe the information access and configuration control issues for the system; and
(3) determine the appropriate types of system development and maintenance environments.

k. Threat Description and Risk Assessment

(1) define in conjunction with the system owner the potential threats that can affect the confidentiality, integrity and availability of the system, clearly stating the nature of the threat that is expected, and where possible, the expected frequency of occurrence;
(2) identify threats, such as penetration attempts by hackers, damage or misuse by disgruntled or dishonest employees, and misuse by careless or inadequately trained employees;
(3) identify unintentional human error, system design weaknesses, and intentional actions on the part of authorized as well as unauthorized users that can cause these events; and
(4) describe insider threat, including the good intentions of a trusted employee who circumvents security in order to accomplish the job.

l. System Architectural Description

(1) describe the accreditation boundary of the system;
(2) describe the system architecture including the configuration of any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information and includes computers, ancillary equipment, software, firmware, and similar procedures and services, including support services and related resources;
(3) describe the system's internal interfaces and data flows;
(4) identify and describe the system's external interfaces and the relationship between the interfaces and the system;
(5) describe the proposed and appropriate hardware and its function (note: hardware is the physical equipment, as opposed to programs, procedures, rules, and associated documentation);
(6) describe the proposed and appropriate software and its intended use (note: software includes the entire set of application programs, software procedures, software routines, and operating system software associated with the system; this includes manufacturer-supplied software, other commercial off-the-shelf software, and all program-generated application software);
(7) determine the types of data and the general methods for data transmission (note: if specific transmission media or interfaces to other systems are necessary, these needs may influence the security requirements for the system);

(8) develop an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communications processors, networks, and remote interfaces;
(9) develop diagrams or text to explain the flow of critical information from one component to another;
(10) identify and include diagrams or text that clearly delineate the components that are to be evaluated as part of the C&A task;
(11) identify components which are not to be included in the evaluation; and
(12) prepare a high level overview of the types of hardware, software, firmware and associated interfaces envisioned for the completed system.

m. Identify C&A Organizations and Resources

(1) enlist the assistance of a contractor team or other government organizations (note: the CA has the responsibility to form the team, coordinate the C&A activities, conduct the analysis and prepare or validate the SSAA);
(2) identify the appropriate statutory authorities, and the resource and training requirements necessary to conduct the certification;
(3) identify the organizations, individuals and titles of the key authorities involved in the C&A process;
(4) determine the certification team's roles and responsibilities;
(5) form the C&A team after the CA knows the certification level and tasks required;
(6) identify the roles of the certification team members as needed and their responsibilities; and
(7) include team members who have composite expertise in the whole span of activities required, and who are independent of the system developer or PM.

n. Tailor the Agency-specific C&A Guidelines (e.g., NIACAP, DITSCAP) and Prepare the C&A Plan

(1) adjust and document the C&A guideline (e.g., NIACAP, DITSCAP) activities to fit the program strategy;
(2) conduct a review of the C&A guideline plan and SSAA by the DAA, CA, PM, and user representative;
(3) determine the skills needed to perform the analysis and the supporting documentation;
(4) prepare a process diagram of the system life-cycle activities and identify the current phase of life-cycle activity;
(5) schedule the C&A guideline activities to meet the system schedule (for example, if the system has already completed preliminary design, all C&A guideline phase one activities should be completed as soon as possible);
(6) tailor the C&A process as agreed upon in the SSAA;
(7) tailor the C&A guideline process to the system life-cycle at the current system phase or activity;
(8) tailor the process to the incremental development strategy (if one is used);
(9) tailor the security activities to system development activities to ensure that the security activities are relevant to the process and provide the required degree of analysis;
(10) determine the appropriate certification analysis level and adjust the C&A guideline activities to the program strategy and system life-cycle;

(11) determine where to focus the analysis and testing; and
(12) identify the appropriate level of effort.

o. Prepare SSAA Added Material

(1) consolidate documentation drawing together all pertinent materials into a logical, sequential, and coherent document which will support the DAA's decision to approve or disapprove;
(2) identify constraints, assumptions, and dependencies of the C&A process being implemented; and
(3) identify the conditions under which certification activities were accomplished.

p. Requirements Traceability

(1) develop the security certification test plan documentation;
(2) develop the ST&E evaluation report documentation;
(3) identify the source of the security requirements for use during negotiations, development of the SSAA, and compliance validation;
(4) specify the required security evaluation documentation;
(5) use security requirements to develop the ST&E plans and procedures;
(6) develop security certification test procedures; and
(7) outline any unique certification analysis documentation requirements.

5. SUPPORTING SYSTEMS DEVELOPMENT

a. Coordination with Related Disciplines

(1) explain to the development team and to the accreditor the need for coordination with related disciplines;
(2) perform coordination with the various offices responsible for the related disciplines; and
(3) verify coordination with related security disciplines, e.g., physical, emanations, personnel, operations, and cryptographic security.

b. Configuration Control

(1) appraise current system configuration control;
(2) discuss configuration control with the development team for compliance with required INFOSEC policy and technology;
(3) propose configuration control changes;
(4) report the configuration control deficiencies to the developer; and
(5) verify that the activities associated with configuration control, i.e., physical and functional audits, inventory of the hardware and software components, etc., are adequately documented and performed.

c. Information Security Policy

(1) identify applicable information security policy;
(2) explain information security policy to the development team for the secure operation of the system; and
(3) use information security policy to ensure the appropriate secure operation of the system.

d. Life-Cycle System Security Planning

(1) appraise the life-cycle system security planning proposed by the development team;
(2) assist with the information security planning for life-cycle system security;
(3) explain the life-cycle system security planning to the development team;
(4) influence the development team's approach to life-cycle system security planning; and
(5) verify that life-cycle system security planning has been accomplished.

e. Parameters of the Certification

(1) propose alterations to the parameters of the certification process as the system development progresses and the design is modified;
(2) compare the parameters of the certification to those of similar systems or during parallel certification;
(3) determine the parameters of the certification to ensure mission accomplishment;
(4) explain the parameters of the certification to system developers and maintainers;
(5) use the parameters of the certification; and
(6) verify adherence to the parameters of the certification.

f. Principles and Practices of Information Security

(1) understand the principles and practices of information security;
(2) identify principles and practices of information security that pertain to the certification;
(3) adhere to recognized principles and practices of information security; and
(4) explain the principles and practices of information security that pertain to the certification to the developers.

g. Network Vulnerabilities

(1) identify any network vulnerabilities for the system developers and maintainers;
(2) demonstrate to the system developers and maintainers the network vulnerabilities that are present during the development of the system;
(3) evaluate the impact of network vulnerabilities;
(4) explain unacceptable network vulnerabilities to the developers;
(5) respond to network vulnerabilities by suggesting corrective measures when possible; and
(6) stay current on network vulnerabilities.

h. Security Engineering

(1) assist developers and maintainers with system security engineering principles as required for information security and certification and accreditation;
(2) define security engineering principles that are applicable to information security;
(3) explain security engineering principles and practices;
(4) review security engineering principles and practices for compliance with information security policies; and
(5) outline best security engineering practices as defined by the National Information Assurance Partnership (NIAP).

i. Access Control Policies

(1) be aware of access control policies;
(2) evaluate for the developers and maintainers the strengths and weaknesses of access control policies;
(3) explain the need for access control policies;
(4) identify to the developers and maintainers access control policies that are applicable to information security; and
(5) recommend access control policy changes that are appropriate for the system being certified.

6. PERFORMING CERTIFICATION ANALYSIS

a. Access Control

(1) appraise access control privilege assignment;
(2) appraise access controls defined as appropriate for the IS under review for subjects (e.g., local and remote users and/or processes);
(3) appraise access controls for objects (e.g., data, information, and applications);
(4) appraise access controls for privileged users and/or processes;
(5) appraise management of the access control tables and lists;
(6) appraise identification and authentication mechanisms which identify users and/or processes;
(7) appraise the implementation of user privileges and group management assignments;
(8) appraise managed and default file permission settings and factory settings;
(9) appraise the effectiveness of password management implemented to enforce policies and procedures;
(10) appraise whether the identification and authentication mechanism can correctly identify users and/or processes;
(11) identify the requirement for discretionary/mandatory access controls (DAC/MAC);
(12) explain to other team members and managers how access privileges are set;
(13) match data ownership and responsibilities with access control rights;
(14) match the requirements for respective access control features with appraised controls implemented;
(15) match the access control requirements with user roles and group management;
(16) determine the security countermeasures to implement effective access control;

(17) verify the contents of the user registry and access control tables;
(18) verify the effectiveness of password management software in enforcing policies and procedures;
(19) identify representative processes which must use an appropriate identification and authentication mechanism;
(20) propose the security test and evaluation plan/procedures and schedule to test and evaluate agreed upon security countermeasures for access control; and
(21) report recommended changes to the implemented access control mechanisms as needed to meet the requirements identified in the access control policies.

b. Audits

(1) appraise the system's ability to produce viable, inclusive audit data for review and analysis (e.g., selection capabilities for review of audit information);
(2) appraise the alert capabilities provided by audit/intrusion detection tools;
(3) verify the criteria for generating alerts provided by audit/intrusion detection tools;
(4) appraise the availability of audits including recovery from permanent storage;
(5) appraise the identification of anomalies which indicate successful violation/bypass of security capabilities;
(6) appraise the inherent audit capabilities and the proposed implementation;
(7) appraise the processes for analyzing audit information;
(8) appraise the report generation capability;
(9) appraise the use of audit information to identify attempts to violate/bypass the proper operation of system security capabilities;
(10) appraise the use of audit information to validate the proper operation of automated system security capabilities;
(11) identify the audit elements and capabilities available on the system being evaluated;
(12) identify the audit event characteristics and their granularity (i.e., type of event, success/failure, date/time stamp, user ID);
(13) summarize the data which supports trend analysis;
(14) verify that the audit elements capture information that meets specified security requirements;
(15) verify that the audit log overflow policy is correctly implemented;
(16) verify that audit procedures exist to implement the policy (i.e., data reviews, audit retention and protection, response to alerts, etc);
(17) verify that audit processes support interpretation of the audit data;
(18) verify that the audit retention capability meets the system security requirements;
(19) verify that protections are in place to prevent the audit trails from being modified by any means, including direct edits of media or memory;
(20) report the audit collection requirements to meet a stated authorization policy;
(21) report any alternative means to satisfy the audit collection requirements;
(22) propose aperiodic security test and evaluation plans and procedures to test and evaluate agreed upon audit functionality and events;
(23) verify that system resources are sufficient to log all required events;
(24) interpret the audit policy to be implemented (to include which events are to be recorded, what action should occur when the log fills, how long audits are to be retained, etc.);

(25) determine the impact of audit requirements on the system operation requirements; and
(26) appraise the capabilities of the add-on audit analysis and intrusion detection tools that are implemented.

c. Applications Security

(1) appraise the effectiveness of applications security mechanisms and their interactions with other systems and network security mechanisms;
(2) differentiate between the operating system and application system security features; and
(3) propose security test and evaluation plans and procedures to test and evaluate agreed upon security countermeasures provided by application security mechanisms.

d. Confidentiality, Integrity and Availability (CIA)

(1) explain the stated system requirements for confidentiality, integrity, and availability **in** the system design/SSAA documentation;
(2) appraise the network architecture and what security mechanisms are used to enforce the CIA security policy; and
(3) appraise the network security posture in light of the CONOPS and the abilities of the expected users and system administrators.

e. Countermeasures

(1) appraise the requirements for additional countermeasures based on the security policy being implemented (e.g., routers, firewalls, guards, intrusion detection devices);
(2) study the security countermeasures documented in the SSAA; and
(3) propose security test and evaluation plans and procedures to test and evaluate agreed upon security countermeasures documented in the SSAA.

f. Documentation

(1) identify the documentation of security-related function parameters, defaults and settings;
(2) report the review of the documentation, noting the adequacy of detail; and
(3) identify the deficiencies in the system documentation, whether they be missing documents or inadequate detail in the existing documentation.

g. Network Security

(1) appraise the network connectivity policy and the proposed implementation for connection;
(2) appraise the security requirements for interconnectivity with other systems/networks;
(3) verify that formal approvals have been granted for other systems and networks for which interconnectivity is sought;
(4) appraise the security attributes of both the data and users accessing the connected system to determine whether additional security requirements result; and

(5) propose security test and evaluation plans and procedures to test and evaluate agreed upon security countermeasures for network connectivity.

h. Maintenance Procedures

(1) appraise the proposed system maintenance and upgrade procedures to ensure that they comply with configuration management procedures (e.g., remote software updates).

i. Operating System Security

(1) appraise the documentation and system configuration of security function defaults and settings, ensuring that all inappropriate factory defaults have been changed;
(2) appraise how the system handles error conditions;
(3) appraise the system recovery capability during loss of power situations;
(4) assess and report any variance between documented and actually installed software and operating systems;
(5) propose security test and evaluation plan/procedures to test and evaluate agreed upon security countermeasures enforced by the operating system;
(6) verify that capabilities are employed to enforce the protection of the operating system by preventing programs or users from writing over system areas;
(7) verify that protections are in place to prevent configuration files and pointers that can run in a supervisory state from unauthorized access or unauthorized modifications, deletions, etc.; and
(8) verify that protections are in place to prevent the operating system kernel from being modified by any process, program or individual except through an approved organizational configuration management procedure.

j. Vulnerabilities

(1) identify vulnerabilities inherent to the system's specific operating system, applications, and network configuration.

k. Contingency Operations

(1) appraise whether the disaster recovery mechanism adequately addressees the needs of the site;
(2) appraise whether the plan sufficiently protects the security of the information and the investment made in life-cycle security processes;
(3) match the requirements for disaster recovery/continuity of operation with mission requirements; and
(4) match the requirements for emergency destruction procedures with mission requirements.

7. CERTIFICATION EVALUATION

a. Evaluation Techniques

(1) use appropriate evaluation techniques, e.g., documentation review, automated tools, and written test plan and procedures, etc., in the conduct of the security test and evaluation;
(2) choose the evaluation technique(s) to exercise and evaluate security countermeasures or capabilities documented in the SSAA; and
(3) generate and/or validate the security test and evaluation plan and procedures.

b. Access Control

(1) verify that access controls meet the criteria established in the SSAA;
(2) document the results of the ST&E access control tests; and
(3) describe the ST&E testing results for access controls.

c. Contingency Planning/Testing

(1) appraise the effectiveness of the contingency plan as described in the SSAA; and
(2) document the effectiveness of the contingency plan.

d. Audit Trail

(1) demonstrate that the audit trail is secure from unauthorized alteration and deletion, and document the results; and
(2) appraise whether the audit trail meets the requirements as defined in the SSAA and document the results.

e. Intrusion Detection

(1) verify the presence of intrusion detection capabilities as defined in the SSAA and document the results;
(2) demonstrate that the intrusion detection mechanisms work as outlined in the SSAA and document the results; and
(3) analyze the effectiveness of the intrusion detection capabilities and document the results.

f. Security Processing Mode

(1) verify that the security processing mode has been identified;
(2) justify any suggested change in the security processing mode, if found to be inadequate or inappropriate, and document the results; and
(3) appraise whether or not the defined security processing mode is adequate for approving system certification, and document the results.

g. Automated Security Tools

(1) identify appropriate security tools and document the results;
(2) appraise and document whether or not the automated security tools produce the expected results;
(3) use the available security analysis tools appropriate to the defined information system to find security anomalies and document the results;
(4) interpret the results of automated security analysis; and
(5) justify any suggested security relevant changes found by the tools and document the results.

h. Application Security

(1) appraise whether or not application security features produce the expected results and document the results; and
(2) verify the presence of and the appropriate use of application security features, and document the results.

i. Disaster Recovery Planning

(1) verify the presence of a disaster recovery plan as documented in the SSAA;
(2) appraise the effectiveness of the disaster recovery plan as described in the SSAA; and
(3) document the results of this verification and appraisal.

j. Change Control Policies

(1) verify the implementation of the change control management processes;
(2) verify the presence of change control policies as documented in the SSAA; and
(3) document the results of this verification.

k. Labeling

(1) verify and document that labeling is accomplished in accordance with the requirements documented in the SSAA.

l. Marking of Media

(1) verify and document that all media in use is marked as appropriate, based on the requirements defined in the SSAA.

m. Documentation Issues

(1) report conformance/non-conformance to the specified system certification documentation requirements;
(2) verify the presence of system standard operating procedures;
(3) verify that the SSAA has been validated from the DAA/CA perspective;
(4) verify that the appointment of personnel with any level of privileged access has been

identified in writing, as required; and

(5) verify the presence of documentation or a manual used by the system administrator (SA) and information system security officer (ISSO) to set up the system security configuration.

n. Operating System Integrity

(1) demonstrate that the operating system integrity capabilities are present in the information system by incorporating operating system configuration management guidelines, including installing the latest patches and consulting with available experts and references, and by updating and testing these guidelines often;
(2) report the results of the ST&E pertaining to operating system integrity; and
(3) verify that the operating system integrity capabilities present in the information system are managed and work as defined in the SSAA.

o. Protecting From Malicious/Mobile Code

(1) use the available tools to test the system capabilities in order to identify residual risk;
(2) verify that appropriate capabilities are resident in the system to mitigate risk from malicious/mobile code contamination; and
(3) document the results of testing to support the system residual risk analysis.

p. Coordination with Related Security Discipline

(1) report, when required, the results of related security discipline testing; and
(2) verify that there are countermeasures defined in the SSAA for physical security, personnel security, all aspects of INFOSEC, etc.

q. Testing Implementation of Security Features

(1) test and verify the effectiveness of all security features, such as password aging and internal labeling, and document the results; and
(2) analyze the impact of the absence of security features that are necessary for secure systems operations, and categorize the residual risk.

8. DEVELOPING RECOMMENDATION TO DAA

a. Access Control Policies

(1) explain the access control policies as implemented in the current system to the DAA;
(2) define who in the current system has access to information views, who grants the access authorization, and the parameters which will be used to validate access authorization;
(3) identify the adequacy of the implemented access control mechanisms identified in the access control policy and comment on this in the report;
(4) evaluate the access control mechanisms implemented in accordance with the policy, and include the results of this evaluation in the report; and

(5) recommend changes to the implemented access control mechanisms in the report as needed to meet requirements identified in the access control policies.

b. Administrative Security Policies and Procedures

(1) address all pertinent security policies and procedures not covered under the laws, agency-specific procedures, etc. (note: this review examines these procedures and policies in respect to applicable national laws and governing regulations consistent with security requirements); and
(2) recommend administrative security policies and procedures to limit the impact of system technical security deficiencies.

c. Certification

(1) recommend the conditions upon which an accreditation decision is to be made, including the technical evaluation of security features, as well as other safeguards;
(2) identify the deficiency and alternative safeguards and procedures that could be employed to limit the impact of system deficiency;
(3) recommend the adoption of requirements which were previously unspecified, but which may be crucial to secure deployment and operation of the system; and
(4) report on the comprehensive evaluation of the technical and non-technical security features of the IS and other safeguards, to meet the security and accreditation requirement.

d. Roles and Responsibilities

(1) outline current roles and responsibilities of personnel assigned access to the systems being certified; and
(2) recommend changes to include additions for improving the roles and responsibilities and accountability for personnel with various levels of access to the information systems being certified.

e. Brief and Defend ST&E Results

(1) describe the ST&E results; and
(2) explain and defend the specific findings, including risk analysis/mitigation.

f. Communicate Results of ST&E

(1) render the technical findings into comprehensible language for non-technical managers; and
(2) communicate the results/findings to technical personnel who would be responsible for correcting the findings.

g. Identify Potential Corrective Approaches

(1) identify potential avenues of corrective action;

(2) provide corrective approaches to the DAA as potential mitigating factors, if adopted; and
(3) address the technical aspects of the system to meet the technical security requirements for its intended use and to identify those areas where non-technical means such as procedures or restrictions are needed to reduce the risk of operating the system to an acceptable level.

h. Determine Residual Risk

(1) report the findings and the overall level of residual risk in the current system; and
(2) compare and contrast the non-technical and technical test/evaluation results, the impact of any countermeasures, and determine the residual risk.

9. COMPLIANCE VALIDATION

a. Automated Tool

(1) conduct post-accreditation periodic compliance validation reviews in accordance with the timelines identified in the SSAA or as requested by the DAA;
(2) identify and discuss the testing tools with site personnel, if necessary; and
(3) verify that the identified tools remain compliant with the current accreditation.

b. Process Review

(1) discuss the identified life-cycle processes and procedures with cognizant site personnel;
(2) identify the life-cycle processes and procedures to support mission accomplishment;
(3) manage the review in accordance with the identified timelines;
(4) review the physical, environmental, technical, and procedural security disciplines;
(5) review the SSAA and assist in its revision, if necessary;
(6) verify that the identified life-cycle processes and procedures remain compliant with the current accreditation;
(7) verify the status of the system's current risks; and
(8) explain the results and the recommendations, based on the findings, in support or denial of continued certification to the DAA.

c. Connection Requirements

(1) verify that connections of systems to networks or to each other follow a defined set of requirements as found in the SSAA.

10. MAINTENANCE OF THE SSAA

a. Life-Cycle Security Planning

(1) discuss, when consulted, proposed changes to the SSAA;
(2) propose, where required, a need for recertification and reaccreditation; and

(3) interpret, when consulted, changes that may affect the existing certification.

b. Documentation Policies

(1) appraise the documentation policies for continued applicability;
(2) identify the documentation policies for updates; and
(3) verify changes against the original documentation policies.

c. Configuration Control/Change Management

(1) appraise the configuration control for continued applicability;
(2) identify the configuration control in place versus that which has been specified in the current SSAA;
(3) list proposed changes to the previously approved system configuration and/or operating environment, to include system retirement;
(4) analyze the above changes to determine if an assessment of the impact is required;
(5) outline the process for an assessment of the impact of changes to the existing SSAA; and
(6) revise the SSAA in accordance with the configuration changes.

d. Maintenance of Configuration Documents

(1) appraise the maintenance of configuration documents; and
(2) compare the maintenance of configuration documents for conformance to the SSAA.

e. Periodic Review of System Life-cycle

(1) appraise the periodic review of the system/product life-cycle for conformance to the SSAA;
(2) initiate the periodic review of the system/product life-cycle for conformance to the SSAA; and
(3) report on the periodic review of the system/product life-cycle.

f. Communicate Results

(1) report the results of changes to the SSAA to the accreditor (DAA).

g. Convey Magnitude of Risk

(1) identify the inherent and residual risks and the potential corrective approaches to the accreditor (DAA).

h. Brief and Defend ST&E Results

(1) prepare and deliver the ST&E results to the accreditor (DAA).

ANNEX B

CONCOMITANT CAPABILITIES FOR SYSTEM CERTIFIERS

These requirements do not imply that the System Certifier(s) need be an expert in these global and specific concomitant capabilities, but he or she must be qualified to discuss, explain, and employ them. The concomitant System Certifier(s) capabilities include but are not limited to the following:

GLOBAL CAPABILITIES:

administrative security
personnel security
physical security
communications security
network security
server security
client/workstation security
database security
application security
cryptographic key management
understanding how a system will be used, in what environment, and by whom
documentation
business background
computer science background
creativity in achieving solutions
creativity in functional solutions
decision-making and management skills
engineering background
flexibility
interpersonal skills
quick learner
ability to see the "big picture"
self-starter/motivated
ability to work well in a team
ability to think outside the box/system
ability to accept challenges
TEMPEST

SPECIFIC CAPABILITIES:

INFOSEC
OPSEC
communication/writing skills
political skills

acquisition and C&A processes
assessment and testing methodology
addressing client server security to evaluate that portion of the system
client/server security
vulnerability self-audit capabilities (analyzing the capabilities of the system system to detect changes and vulnerabilities)
ability to appraise the client/server security posture in light of the concept of operations and the abilities of the expected users and system administrators
configuration management processes
developing data flow diagrams.
documenting security violations
functional job requirements for INFOSEC personnel (SA, ISSO, ISSM, DAA, etc.)
best practices in information assurance
hardware, software, firmware
updating operating procedures
maintaining currency of the CONOPS
knowledge of certification tools
legal aspects of testing (limitations to

monitoring, etc.) knowledge of operating systems risk management methodologies roles and responsibilities of C&A personnel technical knowledge of networks, servers,	workstations, operating systems, etc. understanding of current threats and incidents

ANNEX C

REFERENCES AND BIBLIOGRAPHY

The following references pertain to this Instruction:

a. NSTISSD No. 501, National Training Program for Information Systems Security (INFOSEC) Professionals, November 16, 1992

b. NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), April 2000

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

d. DoD Directive No. 5200.28, Security Requirements for Automated Information Systems March 21, 1988

d. Public Law No. 100-235, Computer Security Act of 1987, January 8, 1988

e. NCSC-TG-031, Certification and Accreditation Process Handbook for Certifiers

f. NCSC-TG-034, Certification and Accreditation Planning Guide for Program Managers

g. DoD Instruction No. 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

h. Office of Management and Budget Circular No. A-130, Management of Federal Information Resources, February 8, 1996

i. Director of Central Intelligence Directive No. 6/3, Protecting Sensitive Compartmented Information Within Information Systems, June 1999

j. I942-TR-002, Version 1, Accreditor's Guideline, July 1994

k. SC-2610-143-93, Defense Intelligence Management Document, DoD Intelligence Information Systems (DoDIIS) Site Certifier's Guide, November 1993

l. DoDIIS Systems Security Certification and Accreditation Guide, March 2000

m. NIST Special Publication No. 800-16, Information Technology Security Requirements: A Role- and Performance-Based Model, April 1998

n. Common Criteria for Information Technology Security Evaluation (CC) version 2.1, International Standards Organization (ISO) International Standard 15408, January 31, 2000

o. National Information Assurance Partnership (NIAP), URL: http://niap.nist.gov