



INFORMATION ASSURANCE
CERTIFICATION AND ACCREDITATION
(C&A)
PUBLICATION
VOLUME III
Program of Record Information Systems



DEPARTMENT OF THE NAVY (DoN)
INFORMATION ASSURANCE (IA)
PUBLICATION

MODULE 5239-13 VOL III

Distribution:

Electronic versions of this document may be downloaded via anonymous ftp from infosec.navy.mil or via the DoN INFOSEC/IA Web Site on the NIPRNET at <http://infosec.navy.mil> and on the SIPRNET at <http://infosec.navy.smil.mil>.

For further assistance, the INFOSEC Technical Assistance Center (ITAC) may be reached at:

Commercial 1-800-304-4636
DSN 588-5428 / 4286

Local reproduction is authorized.

FOREWORD

Naval Information Assurance Program Publications (IA Pub) are issued by the Chief of Naval Operations (CNO) N643. The IA Pub series provides modules that guide the implementation of the policy direction established in Chief of Naval Operations Instruction (OPNAVINST) 5239.1B. These modules provide procedural, technical, administrative, and supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data. Each module focuses on a distinct subject and describes a standard methodology for planning, implementing and executing that element of the IA program within the Department of the Navy (DON).

This module, "Information Assurance Certification and Accreditation Publication," provides the DON IA C&A approach for program of record systems.

Reviewed and Approved by:

COMSPAWARSYSCOM PMW-161 Carl Siel //

CNO N643 Louise Davidson //

TABLE OF CONTENTS

1.0 INTRODUCTION..... 1

1.1 SCOPE AND PURPOSE..... 1

2.0 PROGRAM OF RECORD INFORMATION SYSTEMS CERTIFICATION AND ACCREDITATION PROCESS 1

2.1 DEFINITION PHASE..... 1

 2.1.1 Document Mission Need 2

2.1.2 Registration..... 2

 2.1.3 Negotiation..... 2

2.2 VERIFICATION PHASE..... 3

2.3 VALIDATION PHASE 3

 2.3.1 Security Test and Evaluation 3

 2.3.2 Operational Site Certification Letter 4

 2.3.3 Residual Risk Assessment 4

 2.3.4 DAA Accreditation Decision..... 4

2.4 POST ACCREDITATION PHASE 4

3.0 APPLICATION OF THE PROCESS 6

Appendix A 7

System Security Authorization Agreement 7



1.0 INTRODUCTION

This module introduces the third volume of the DON Information Assurance (IA) Certification and Accreditation (C&A) Publication (IA Pub). This Pub provides IA guidance, procedures, and processes to help the Department of the Navy (DON) implement its Information Assurance C&A processes as directed by the Chief of Naval Operations in OPNAV Instruction (OPNAVINST) 5239.1B, Department of the Navy Information Assurance Program. Subsequent versions of this publication will provide greater detail into the C&A activities.

1.1 SCOPE AND PURPOSE

This volume of module 5239-13 provides the Navy's approach to C&A for Program Of Record (POR) information systems. These information systems are typically weapons systems, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems and other systems procured through the processes of DODD 5000.1, Defense Acquisition. This volume also applies to locally acquired operating in the Compartmented or Multilevel mode of operation.

2.0 PROGRAM OF RECORD INFORMATION SYSTEMS CERTIFICATION AND ACCREDITATION PROCESS

It is DON Information Assurance Policy that information and resources are appropriately safeguarded at all times, to support defense in depth across DON and DOD. Safeguards shall be applied such that information and resources maintain the appropriate level of confidentiality, integrity, availability, and accountability based upon mission criticality, level of required IA, and classification or sensitivity level of information entered, processed, stored, and/or transmitted. The safeguarding of information and information systems shall be accomplished through the employment of defensive layers that include the IA disciplines.

Certification is the means by which these safeguards are assessed. Certification is applied to provide an approving authority with the details required to make an informed decision about the protection and defense of the information and/or information system. This section addresses how DON locally acquired information systems engage the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) phases.

2.1 DEFINITION PHASE

"The Definition phase shall include activities to document the system mission, environment, and architecture; identify the threat; define the levels of

effort; identify the certification authority (CA) and the DAA; and document the necessary security requirements for C&A. Phase 1 shall culminate with a documented agreement, between the program manager, the DAA, the CA, and the user representative of the approach and the results of the phase 1 activities.”

Appendix A contains a template is for use by INFOSEC practitioners who are Certifying and Accrediting their information systems. This template provides the outline for capturing the following elements within the DITSCAP Phase I.

- System Mission
- System Environment
- Threat Identification
- System Architecture
- System Security Requirements
- Certification and Accreditation Plan
- Identification of the Certification Authority
- Identification of the Designated Approving Authority

Phase 1, as stated in the DITSCAP, “contains three process activities, document mission need, registration, and negotiation. Phase 1 starts with the input of the mission need statement (or other justification for the system) and ends by producing the SSAA.”

2.1.1 Document Mission Need

When a procurement is initiated for the purchase of an IT product the justification for purchase includes the mission need.

2.1.2 Registration

Registration is the process activity of the DITSCAP that initiates the dialogue among the DAA, the Program Manager, the Certification Authority (PMW-161), and the user representative. As part of the Registration tasks, information is collected and evaluated, applicable requirements are determined, risk management and vulnerability assessment actions begin, and the level of effort required for C&A is determined and planned.

2.1.3 Negotiation

Negotiation is the process activity of the DITSCAP, where all the participants involved in the information system's acquisition and operation, and certification and accreditation agree on the implementation strategy to be used to satisfy the security requirements identified during system registration. The key party who must reach agreement during the negotiations information systems is the DAA. During phase 1 the DAA is the typically the DAA for command developing the system.

2.2 VERIFICATION PHASE

“The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1, there is a corresponding set of security activities that shall verify compliance with the security requirements and evaluate vulnerabilities.”

The process activities of the DITSCAP phase 2 verify the evolving system's compliance with the agreed set of requirements in the SSAA. Phase 2 process activities include continuing refinement of the SSAA, system development or modification, certification analysis, and analysis of the certification results.

During phase 2 the Program Manger

- Develops, executes, and documents a Certification and Evaluation Plan and Procedures.
- Documents system operating procedures including any system specific contingency planning guidance.
- Issues a residual risk statement.
- Provides system certification evidence to the Certification Authority.

2.3 VALIDATION PHASE

“The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.”

Phase 3 process activities, as established in the DITSCAP, validate that an information system operates in a specified computing environment with an acceptable level of residual risk. This phase consists of process activities that occur after the system is integrated and culminates in the accreditation of the IT system. To support the accreditation the Program Manager provides a copy of the system certification to activities receiving the system.

2.3.1 Security Test and Evaluation

The objective of this ST&E is to assess the technical and non-technical security features and assumptions of the configuration and implementation to ascertain that security features affecting confidentiality, integrity, availability, and accountability have been implemented, and perform properly. Certification Test and Evaluation (CT&E) is typically performed during the Verification Phase. The CT&E verifies the correct operation of the designed technical security

requirements. For information systems that are locally acquired without the C&A evidence from Phase II, this ST&E shall validate the correct implementation of technical security configuration (i.e., Communications Security, Computer Security, Emission Security (i.e., TEMPEST)) in addition to the traditional ST&E focus on Physical Security, Personnel Security, Procedural Security, and Security Education, Training, and Awareness countermeasures to perceived threat.

ST&E is typically performed using the procedures detailed in IA Publication 5239-13 Volume II.

2.3.2 Operational Site Certification Letter

The ISSO issues a statement that documents the extent to which the information system meets the requirements implied by the Security Test and Evaluation Checklist and automated security assessment tool. Supplemental recommendations might be made to improve the system's security posture. Such recommendations should provide input to future system enhancements and change management decisions.

An example of the Operational Site Certification letter is provided in IA Publication 5239-13 Volume I and posted on the DON INFOSEC web site at infosec.navy.mil.

2.3.3 Residual Risk Assessment

This risk-based management review task assesses the operation and implementation of the system to determine if the risk to confidentiality, integrity, availability, and accountability security objectives is being maintained at an acceptable level. The risk management review assesses the vulnerabilities with respect to the threat method of attack, capability, motivation, and objective. The operational procedures and safeguards shall be evaluated to determine their effectiveness and ability to offset risk.

2.3.4 DAA Accreditation Decision

The DAA can use the Operational Site Certification Statement and the assessment of the checklist and automated security tool to determine if the risk in operating the information system is acceptable. The courses of action a DAA can take are discussed in IA Publication 5239-13 Volume I.

Accreditation is the authorization that permits an information system to process, store, and/or transmit information. This authorization is an informed decision about the protection and defense of the information and/or information system based upon the certification process.

2.4 POST ACCREDITATION PHASE

The Post Accreditation phase shall include activities to monitor system management and operation to ensure an acceptable level of residual risk is preserved. Security management, change management, and periodic compliance validation reviews are conducted.

Phase 4 begins after the system has been integrated into the operational computing environment and accredited. Phase 4 shall continue until the information system is removed from service, a major change is planned for the system, or a periodic compliance validation is required.

3.0 APPLICATION OF THE PROCESS

This section will be provided in greater detail in following versions of this publication.

Appendix A

System Security Authorization Agreement

Template

for

Program of Record Information Systems

1.0 MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

[assignment: *This section shall describe the system and the mission that the system supports. This includes a statement on how the system's mission supports the organization's mission, the name of the organization, the system's name, the longevity and the placement of the system within its life cycle, a discussion of the information categories to be processed to support the mission, a high level information flow specification, a functional description, a statement on personnel clearances, and a stipulation of the system criticality. The mission description is a concise, high level system specification and needs statement. It describes whom the system will serve, how it will work, what information it will process, how important it is, and why it is being developed. It does not contain implementation specifics. The mission description should come from the mission need document (e.g., Mission Need Statement, Mission Impact Statement, Operational Requirements Document, the purpose statement of the using organization. This description of the mission should focus on the security relevant features of that system.]*

1.1 System Name and Identification

[assignment: *This section should identify the system that is being developed or entering the C&A process. This section provides the name and organization of the element developing the mission need and the organizations containing the ultimate user. It identifies the general user, which helps to define operational scenarios that may be encountered, especially for tactical systems.]*

1.2 System Description

[assignment: *The system description should provide a complete high-level description of the system architecture. Diagrams or drawings should be included to amplify the description. All components of the system should be described. If the information is insufficient or the understanding of the system is insufficient for the system description to be written, the system is not ready to begin the C&A process. The system description should include all of those critical elements required for inclusion in the mission need.]*

1.3 Functional Description

[assignment: *Provide a functional description of the system and the purpose for which it will be used. Provide functional diagrams of the system. Describe functions performed jointly with other systems and identify the other systems. Include high level functional diagrams. Provide the intended flows of data into the system, data manipulation, and output of the resultant products. The mission need should clearly state the purpose for which the system is needed and the capabilities desired. For example, "a system is required for a local area network (LAN) within an office environment to permit the access of all LAN stations to LAN server*

resources. In addition, a connectivity is required to a wide area network (WAN) for interactive sessions with all other resources having access to the WAN.”]

1.3.1 System Capabilities

[assignment: The system functional description and system capabilities information provides a summary of the system mission and function statements. The system capabilities description should clearly delineate what function or capability is expected to be present in the fully accredited system.]

1.3.2 System Criticality

[assignment: This section examines the consequences of a loss of the system. It assesses the effect upon local operations, organizational operations, and national operations if they were denied the reliable use of this system. From this analysis, a determination of the system's criticality is made.]

1.3.3 Classification and Sensitivity of Data Processed

[assignment: This section should state the general classification of information intended (unclassified, confidential, secret, top secret) along with any special compartment or subcompartments. The mission need statement should be examined to determine the classification of information to be processed (unclassified, confidential, secret, top secret) along with any special compartment. The information category will also be used to determine the overall system class. This requires the identification of the type of information processed (Privacy Act, financial, critical operational, proprietary, and administrative).]

1.3.4 System User Description and Clearance Levels

[assignment: This section should define the various user and administrative roles on the system. The ultimate security architecture, level of security assurance, and security design requirements depends a great deal on the security clearances of the users, the users' access rights to the specific categories of information processed, and the actual information the system is required to process. Therefore, it is essential that the mission need clearly state the user population's security clearances and access rights to other restricted information. For example, “a system may be required to have contractor personnel as authorized users; however, under classification of data processed, the mission need states that proprietary information from

commercial organizations other than the users would be processed. This situation creates a security problem in that sufficient controls must be designed into the system to preclude having the contract users gain intentional or unintentional access to the proprietary data.”]

1.3.5 Life Cycle of the System

[assignment: This section describes the life cycle program and where the system is in relationship to its life cycle. For example, if the mission need states that a sensor support system is needed urgently to provide tactical support to ongoing operations, an accelerated development and acquisition process is most likely to be used. The C&A process must be prepared to keep pace with this effort, and that requires resource allocation on the part of the CA and DAA as well.]

1.4 System CONOPS Summary

[assignment: This information supplements the system description and function statements. What is needed in this section is a high level description of the concept for the system to satisfy the mission need. Provide a description of those functions that are jointly performed with other systems, and identify the other systems.]

2.0 ENVIRONMENT DESCRIPTION

[assignment: The environment description documents the intended operational environment, software development and maintenance environment, the threat environment, external electronic connections, and the political environment (if applicable). This will include the connection layer information. If more than one location is used, provide details for each as a separately numbered heading]

2.1 Operating Environment

[assignment: Identify and describe the physical environment in which the IT system will operate]

2.1.1 Facility Description

[assignment: Identify and describe the physical location in which the IT system will operate including floor plans, equipment placement, electrical and plumbing outlets, and telephone outlets.]

2.1.2 Physical Security

[assignment: Describe the access control procedures provided by the environment and any other standard operating procedures that support a secure environment. Include existing security features mandated by the operational situation in this section. Provide a description of

existing environmental security features that will mitigate the implementation of specific security requirements in that environment rather than in the system architecture and design.]

2.1.3 Administrative Issues

[assignment: Identify the organizations that will use the system and any impacts to security.]

2.1.4 Personnel

[assignment: Identify and describe the different personnel roles that will have access to the system and the physical environment.]

2.1.5 COMSEC

[assignment: Communications Security. Identify and describe the measures and controls established to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Note: Communications security includes cryptographic security, transmission security, emission security, and physical security of COMSEC material.]

2.1.6 TEMPEST

[assignment: For classified systems, identify any TEMPEST requirements identified by a Navy Certified TEMPEST Technical Authority (CTTA). Identify any requirement for operating location to submit TEMPEST Requirements Questionnaire (TRQ).]

2.1.7 Maintenance Procedures

[assignment: Describe any maintenance procedures necessary for the continued security of the system.]

2.1.8 Training Plans

[assignment: Describe any system unique training provided for users and administrators.]

2.2 Software Development and Maintenance Environment

[assignment: Identify and describe the software development and maintenance environment - open or closed.]

2.3 Threat Description

[assignment: Identify and describe the vulnerability-induced threats, environmentally based threats, and the impact these threats have on mission need. Definition of the potential threats

shall consider the intentional and unintentional events that can affect the integrity, confidentiality, and availability of the system.]

3.0 SYSTEM ARCHITECTURAL DESCRIPTION

[assignment: The architecture description provides the framework for the information system architecture and includes a physical description of the hardware, software, firmware, and interfaces. Against this framework, the architecture description stipulates the security architecture. Existing or planned system features that facilitate expansion or external connection should be mentioned in this section. During the concepts development phase, the architecture may not be fully developed. A broad description of these areas may be provided. However, once the information system has entered the design phase, the architecture description must be updated and details filled in. Areas may exist that do not apply to the information system (e.g., firmware). For such an instance, it is appropriate to enter the term "nonapplicable." For complex systems it is appropriate to include the details in Appendix I and reference them here.]

3.1 Hardware

[assignment: Identify and describe the hardware used and whether it is a standard commercial product, unique, or on the EPL. Include an equipment list as an attachment. Describe the target hardware and its function. Hardware is the physical equipment as opposed to programs, procedures, rules, and associated documentation. If this development effort involves an existing hardware change, identify the specific hardware components being changed.]

3.2 Software

[assignment: Identify and describe the operating system(s), database management system(s), and applications. Identify and describe the features of any security packages used on the information system. Identify any software packages that are COTS, GOTS, and on the CC EPL. Describe the target software and its intended use. Software includes the entire set of application programs, software procedures, software routines, and operating system software associated with the system in question. This includes manufacturer supplied software, other commercial off-the-shelf software, and all program generated applications software.]

3.3 Firmware

[assignment: Identify and describe the firmware used and whether it is a standard commercial product (such as a Personal Computer Basic Input Output System (BIOS) or unique. Describe the software that is stored permanently in a hardware device that allows reading and executing the software, but not writing or modifying it. For example, items such as programmable read-only

memory (PROM) and enhanced PROM (EPROM) devices are considered firmware.]

3.4 System Interfaces and External Connections

[assignment: System interfaces and external connections. Provide a statement of the significant features of the communications layout. Include a high level diagram of the communications links and encryption techniques connecting the components of the information system, associated data communications, and networks.]

3.5 Data Flow (including data flow diagrams).

[assignment: Describe the system's external interfaces. The description shall include a statement of the purpose of each external interface and the relationship between the interface and the system. The types of data and the general methods for data transmission should be stated if specifically required. If specific transmission media are not necessary for the mission need, the mission need should state the basic transmission capability desired. From this the security engineer, working with the PM, can make an initial assumption on a suitable method for processing the data flow requirements.]

3.6 Accreditation Boundary

[assignment: Describe the boundary of the system under consideration. The description shall include diagrams or text to clearly delineate which components are to be evaluated as part of the C&A task, and which are not included. All components included shall be described in the systems description. Elements outside the accreditation boundary shall be included in the description of the external interfaces.]

4.0 SYSTEM SECURITY REQUIREMENTS

[assignment: The system security requirements are derived from the security policy. Examples of requirements are I&A, contingency planning, access controls, etc. The security analysis levels stipulate the high-level security requirements. Requirements of all ITSEC disciplines (COMPUSEC, COMSEC, TEMPEST, physical security, personnel security) must be included. For systems requiring a more rigorous certification defining the requirements in the terminology of ISO 15408 if recommended as this allows reuse of existing Security Profiles and Security Targets. A typical approach to support this section is to construct a Requirements Traceability Matrix (Appendix F).]

4.1 National and DoD Security Requirements

[assignment: DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements,

providing security solutions, and managing information system security activities.]

4.2 Governing Security Requisites

[assignment: Those security requirements that must be addressed in all systems. These requirements are set by policy, directive, or common practice set, e.g., by Executive Order, OMB, Office of the Secretary of Defense, a military service or DoD agency. They are typically high-level. While their implementations will vary from case to case, these requisites are fundamental and must be addressed.]

4.3 Data Security Requirements

[assignment: Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.]

4.4 Security CONOPS

[assignment: The security concept of operations provides a detailed description of system input, system processing, and intermittent and final outputs. Descriptions of all interactions and connections with external systems must be included. Use of diagrams, maps, pictures, and tables are encouraged. This section must be understandable by nontechnical managers. For detailed CONOPS, that material should be placed in Appendix D and referenced here.]

4.5 Network Connection Rules

[assignment: Describe any restrictions on network connectivity (e.g. SIPRNET, NIPRNET, etc...).]

4.6 Configuration Management Requirements

[assignment: Management of security features and assurances through control of changes made to hardware, firmware, software, documentation, test, test fixtures, and test documentation of an automated information system throughout the development and operational life of a system.]

4.7 Reaccreditation Requirements

[assignment: Identify any requirements to reaccredit the system because of system changes occurring within a three year interval.]

5.0 ORGANIZATIONS AND RESOURCES

[assignment: The organization description shall describe the organization responsible for ensuring compliance with the SSAA. A chart may be used. This section will address issues of staffing, training, and support needs. Section 3, task 1-7 provides additional guidance on the preparation of this section.]

5.1 Organizations

[assignment]: Describe the organization responsible for ensuring compliance with the SSAA and list the roles and responsibilities of all participants, including the DAA, CA, user representative, ISSO, and any other organizations that may be needed to support this C&A effort.

Designated Approval Authority (DAA) Point of Contact:

DAA:
Command:
Phone:
Fax:
Email:

Certification Authority (CA) Points of Contact:

Certifier: Carl Siel
Command: COMSPAWARSYSCOM PMW-161
Phone: (619) 524-7511
Fax: (619) 524-7514
Email: sielc@spawar.navy.mil

Certification Agent (CAg) Points of Contact:

Certifier:
Command:
Phone:
Fax:
Email:

Program Manager (PM) Points of Contact:

PM:
Command:
Phone:
Fax:
Email:

User Representative Points of Contact:

OPTEVFOR Coordinator:
Phone:
Fax:
Email:
]

5.2 Resources

[assignment: This section should provide a description of the personnel staffing requirements.]

5.3 Training

[assignment: This section describes the training requirements, types of training, who is responsible for preparing and conducting the training, equipment that will be required to conduct training, and training devices that must be developed to accomplish training.]

5.4 Other Supporting Organizations

[assignment:]

6.0 DITSCAP PLAN

[assignment: The plan documents the level of certification analysis, the tasks and milestones, the schedule, the level of effort, and the roles and responsibilities. The section provides the vehicle to develop a mutual understanding of the system among organizations.]

6.1 Tailoring Factors

[assignment: Identify those factors which affect the level of effort expended in certifying and accrediting the system.]

6.1.1 Programmatic Considerations

[assignment: Identify programmatic factors such as schedule and resources that will affect certification activities.]

6.1.2 Security Environment

[assignment: Describe unique characteristics of the security environment that affect certification efforts. For example, "the stand-alone Secret LAN is installed in a Top Secret open storage area".]

6.1.3 IS Characteristics

[assignment: Describe unique characteristics of the system that affect certification effort. For example, "all trusted code is stored in EAROM and can only be altered by authorized maintenance personnel".]

6.1.4 Reuse of Previously Approved Solutions

[assignment: Identify components of the system which have been previously evaluated, certified, or accredited.]

6.2 Tasks and Milestones

[assignment: The tasks and milestones detail security-related functions, schedule, estimated duration, responsible activity, and completion criteria. The considerations, detailed information on activities, and tradeoffs are associated with each list item.]

6.3 Schedule Summary

[assignment: The schedule of security activities is a calendar of the certification analysis and other events that lead to an accreditation schedule. This information is presented in chronological sequence and details the development and current status of the agreement. The schedule contains information similar to the tasks and milestones but in time order for scheduling.]

6.4 Level of Effort

[assignment: The certification analysis serves as a mechanism to ensure that the appropriate security solutions are in place. The certification levels specify the level of effort required to execute the certification activity. For other activities, negotiated and planned levels of effort are recorded here.]

6.5 Roles and Responsibilities

[assignment: This section details the responsibilities and identities of the persons and organizations responsible for the development, execution, maintenance, and evaluation of the SSAA.]

Appendices must include system C&A artifacts. Optional appendices may be added to meet specific needs. Include all documentation relevant to the C&A process.

APPENDIX A	Acronyms
APPENDIX B	Definitions
APPENDIX C	References
APPENDIX D	System Concept of Operations
APPENDIX E	Information System Security Policy
APPENDIX F	Security Requirements and/or Requirements Traceability Matrix
APPENDIX G	Certification Test and Evaluation Plan and Procedures (Type only)
APPENDIX H	Security Test and Evaluation Plan and Procedures (as required)
APPENDIX I	Applicable System Development Artifacts or System Documentation
APPENDIX J	System Rules of Behavior
APPENDIX K	Incident Response Plan (as required)
APPENDIX L	Contingency Plan(s) (as required)
APPENDIX M	Personnel Controls and Technical Security Controls (as required)
APPENDIX N	Memorandums of Agreement – System Interconnect Agreements (as required)
APPENDIX O	Security Education, Training, and Awareness Plan (as required)
APPENDIX P	Test and Evaluation Report(s)
APPENDIX Q	Residual Risk Assessment Results

APPENDIX R Certification and Accreditation Statements

Note: Appendices marked “as required” are often completed in DITSCAP phase III by the site receiving the system. Portions of the ST&E, such as verification of correct installation, may be completed by the Program Manager as part of system installation. Other appendices can also be completed by the PM. Identification of these documents should be identified in paragraph 6, the DITSCAP plan.