Global Information Assurance Certification Paper

THE BASICS OF APPLYING THE DITSCAP TO DIVISION/CLASS C AND BELOW LEVEL SYSTEMS

Christina King
December 30, 2002

Background

On December 30, 1997, the Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP) came into being. The "objective" of the DITSCAP is to "Establish a DoD standard infrastructure-centric approach that protects and secures the entities comprising the Defense Information Infrastructure (DII)." The DITSCAP was developed in response to requirements identified in two DoD Directives (DoDDs). DoDD 5200.28 states, "All Automated Information Systems (AIS) shall be accredited. Accreditation shall be supported by a Certification plan and report." DoDD 5000.2-R follows with "All AIS shall meet DoDD 5200.28 requirements and be accredited before operation." DITSCAP, outlined in DoD Instruction (DODI) 5200.40, presents a standardized set of activities, specifically Certification and Accreditation (C&A) procedures, designed to assure that the information in a specific Information Technology (IT) entity (e.g., a system or an application) is secure.

Scope

Security Class, in accordance with DoD 5200.28-STD (better known as the Orange Book), is categorized from D "Minimal Protection" through A "Verified Protection". Since the majority of DoD Systems fall within Division C (Discretionary Protection), Class C2 (Controlled Access Protection), the following Certification and Accreditation Procedures address Division C, Discretionary Protection of the Department of Defense Trusted Computer System Evaluation Criteria and below.

Division D: Minimal Protection

Division D, Minimal Protection applies to any system that does not comply with any other category, or has failed to receive a higher classification. D-level certification is essentially non-existent when it comes to Certification and Accreditation.

DIVISION C: Discretionary Protection

Discretionary protection applies to Trusted Computing Bases (TCB's) with optional object (i.e. file, directory, devices etc.) protection.

Division C, Class (C1): Discretionary Security Protection

The Trusted Computing Base (TCB) of a class (C1) system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data. The class (C1) environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

Division C, Class (C2): Controlled Access Protection
Systems in this class enforce a more finely grained discretionary access control than (C1) systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

Certification and Accreditation (C&A)
Certification is evaluation of the technical and non-technical security features of an Information Technology (IT) system.

Accreditation is the formal declaration by the Designated Approving Authority (DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

There are four phases in the development of a C&A package; Definition, Verification, Validation, and Post Accreditation. These phases may overlap and will not be developed in sequence to the SSAA format since the information needed for some sections may not be available until another section is completed. The four DITSCAP Phases are summarized in Table 1.

Table 1. The DITSCAP C&A Process

Definition Phase (1)	Verification Phase (2)	Validation Phase (3)	Post Accreditation Phase (4)
Analyze of Develop Mission Needs Registration Negotiation	Initial Certification Analysis: • System Architecture • Software Design • Network Connection • Product Integrity • Life Cycle Management • Vulnerability Assessment • Prepare Security and Certification Test and Evaluation Plan	Certification/Evaluation: • Certification Test & Evaluation • Security Test & Evaluation • Penetration Testing • System Mgmt Analysis • Site Accreditation Survey • Contingency Plan Risk Mgmt Review Develop Accreditation Recommendation	Maintain Accreditation: • Ongoing Maintenance • System Changes • Change Management • Compliance Validation

The standard phase development is as follows;

Phase 1 (Definition)
In the Definition phase, the C&A team defines the levels of effort in the C&A; identifies the Certification Authority (CA), the Designating Approval Authority (DAA), the system Program Manager (PM), and the user representative; and documents the system mission, target environment and architecture, and threats. The C&A team then identify the security requirements for the system based on the system's classification, data types, users, and threats. Sections 1 through 6 of the SSAA and Appendices A-F should be started as a first draft.

Phase 1 of DITSCAP ends when the CA, DAA, PM, and user representative sign an agreement on the accuracy of the data gathered during the definition phase and on the method for implementing the security requirements.

Phase 2 (Verification)
The activities of Verification Phase are designed to verify whether the developed system complies with the requirements agreed on in Phase 1. Update sections 1 through 6 of the SSAA and Appendices A-F to reflect any changes and additions. Appendices G-O and part of Appendix P must be drafted in Phase 2.

Phase 3 (Validation)
Update the SSAA and all previous Appendices and complete Appendices P-R.
In Phase Three of DITSCAP, Validation, the C&A team validates that the system operates as described with an acceptable level of risk (security risk). System testing occurs in this phase, and the SSAA is updated to reflect any changes and the results of tests. This phase ends when the DAA issues a system accreditation an Authority To Operate (ATO). The ATO is issued only when the DAA is satisfied that the system is properly protected, as described in the SSAA.

Phase 4 (Post Accreditation)
Phase 4 is the maintenance phase. The C&A package has been completed and been given a "Authority To Operate" (ATO). An ATO is good for three years unless there are significant changes that would warrant re-accreditation. The maintenance phase should be used to keep all documentation for your C&A package current. Too often organizations drop the ball at phase 4 and neglect to update changes to their system or changes within their organization. A very basic example of this is failing to keep your personnel roster current within a Contingency Plan or Incident Response Plan. These two documents are both worthless if your contact list isn't up to date.

Certification and Accreditation (C&A) Package

System Security Authorization Agreement (SSAA)
The System Security Authorization Agreement is key to the DITSCAP. This document is the C&A "roadmap". It defines the "accreditation boundary" (what it is, exactly, that is being certified and accredited), system specifications as well as documenting where to find all other amplifying documents (Information System Security Policy, Incident Response Plan, Contingency Plan etc.) A description of the system mission,

environment (physical and virtual), application/network architecture, security requirements, and applicable data access policies are provided. The SSAA also describes the applicable set of planning and certification actions, resources, and documentation required to support the certification and accreditation. In essence, the SSAA is the vehicle that guides the implementation of INFOSEC requirements and the resulting certification and accreditation actions.

The key to writing a good SSAA is to ensure it is clearly written. Try to eliminate redundancy by addressing the finite details in the appropriate Appendix rather than the SSAA itself. The SSAA should give a brief overview and tell where to find the finite details.

SSAA OUTLINE (IN DEPTH)

Title Page
The title page should state "System Security Authorization Agreement for *System Name*" as well as Date of Issue. It is extremely helpful to add a version number, using the phase numbers. For example "Version 1.0" for the first draft in phase 1, "Version 2.2" as the second draft of phase 2. Finally, "Issuing Organization", you must identify the organization issuing the document.

A signature page should be added behind the title page listing the name, signature, and date signed, for the four key DITSCAP roles. Designated Approving Authority, Certification Authority, Program Manager, and User Representative.

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION
This is a paragraph title and should not contain any information. The following subparagraphs will identify the Mission Description and System Identification.

1.1. System name and identification
Identify the system being accredited. Provide the name, organization, and address/location of the organization requesting accreditation. This will normally be the Program Management Office.

1.2. System description
The system description should clearly state the purpose of the system to be accredited and must describe ALL components. It needs to include a high level description of the system architecture, to include network/system drawings or diagrams to give a visual of what is being accredited.

1.3. Functional description
This is a paragraph title and should not contain any information. The following subparagraphs will break out the functional description.

1.3.1. System capabilities

Define the capabilities and functions (current and future) of the system as well as the mission the system is used for. This is where functional diagrams and data flow diagrams can be added.

1.3.2. System Certification Level

DITSCAP activities can be tailored to meet the specific needs of the system, security requirements, and program requirements. Determining the System Certification Level is the means by which the activities are tailored and establishes the level of analysis to be performed. It is important to remember that while the activities may vary the C&A phases remain the same.

The System Certification Level is obtained using the algorithm provided in the DITSCAP Application Manual, DoD 8510.1-M. Table 2 indicates the seven categories assessed and the assigned weight for each characteristic.

Table 2. Determining Certification Level

Characteristic	Description	Selections	Weights
Interfacing Mode	The interfacing mode categorizes interaction. The question concerns containment of risk; for example, if a problem were to occur with the operation, data, or system, what would be the risk to other operations, data, or systems with which it interacts. The interactions of systems may be through either physical or logical relationships.	Benign (w=0) Passive (w-2) Active (w=6)	
Processing Mode	The processing mode distinguishes the way processing, transmission, storage, or data is handled. It reflects the use of the system by one or more different sets of users or processes.	Dedicated (w=1) System High (w=2) Compartmented (w=5) Multi-level (w=8)	
Attribution Mode	Determine the complexity required to attribute the processing, transmitting, or storing of data to a specific user or process, and to determine changes in status.	None (w=0) Rudimentary (w=1) Selected (w=3) Comprehensive (w=6)	
Mission-Reliance	Determine the degree to which the mission is dependent on the site's operation, infrastructure, or data. This is not an indicator of mission criticality.	None (w=0) Cursory (w=1) Partial (w=3) Total (w=7)	

Characteristic	Description	Selections	Weights
Availability	Determine how accessible the system must be to as it relates to security risks (does not include performance). How available must the system be to avoid non-tolerable operational impacts?	Reasonable (w=1) Soon (w=2) ASAP (w=4) Immediate (w=7)	
Integrity	Determine how accurate the system must be as it relates to security risks (does not include performance). How accurate must the system be to avoid non-tolerable operational impacts?	Not-applicable (w=0) Approximate (w=3) Exact (w=6)	
Information Categories	Determine the information category for the system. If more than one category of information is involved in a system, the system must satisfy all the security requirements of each of the information categories. The information categories can be unclassified, sensitive, confidential, secret, top secret, or compartmented/special access classified.	Unclassified (w=1) Sensitive (w=2) Confidential (w=3) Secret (w=5) Top Secret (w=6) Compartmented/ Special Access Classified (w=8)	
TOTAL		Level 1: < 16 Level 2: 12 - 32 Level 3: 24 - 44 Level 4: 38 - 50	

1.3.3. System criticality

System Criticality will affect the level of risk that is acceptable. Criticality is a security term that measures the importance of the system, (including the data it stores or processes), with respect to the adverse impact of its mission, in terms of the length of time the system is out of operation. The level of criticality of a system depends upon the organization's ability to support wartime operations without the system. The levels of criticality are:

Category 1: National Security System, Command and Control of military forces, integral to a weapon or weapons system, system critical to fulfillment of military or intelligence missions.

Category 2: If not functional, would preclude the CINC from conducting missions across the full spectrum of operations.

Category 3: Required to perform Department-level and Component-level core functions.

Not Mission Critical:

1.3.4. Classification and sensitivity of data processed

Define the type and sensitivity of the data processed by the system. Determine the national security classification of information to be processed (unclassified, confidential, secret and top secret) Special handling requirements must also be identified. Systems processing sensitive but unclassified information will also have additional security requirements. Identify the type of information processed (Privacy Act, financial, critical operational, proprietary, and administrative).

It is important to pay special attention to the data being processed and ensure that sensitive but unclassified is truly that. There are times when sensitive unclassified data becomes classified due to compilation. Meaning, when you start combining an enormous amount of sensitive unclassified in a single server or database, it then becomes classified.

1.3.5. System user description and clearance levels

This section is used to describe whom your system users are and how access for the users is set up. Each type of user must be defined (Government or Contractor, US Citizen or Foreign National, Basic User or System Administrator) and their security clearance level stated. Here is where you list all your users (by type, not each individual). You must also briefly go into what security mechanisms or procedures are in place to prevent intentional or unintentional access to sensitive data.

1.3.6. Life-Cycle of the System

Define the life-cycle of the system and at what point in the life-cycle the system is. It is best to give a brief description as well as providing a flow chart or snapshot of the Project Plan.

1.4. System CONOPS Summary

Note, this section says “Summary”. Provide a brief description of the CONOPS to include functions performed jointly with other systems. The full CONOPS should be added as an Appendix. Provide the summary and state “*System* CONOPS provided in Appendix D”.

2. ENVIRONMENT DESCRIPTION

This is a paragraph title and should not contain any information. The following subparagraphs 2.1 and 2.2 (and their subsequent subparagraphs) are used to break out the full spectrum of Environment Descriptions.

2.1. Operating environment

Paragraph 2.1 is a paragraph title and should not contain any information. The following subparagraphs will break out the specific Operating Environment Descriptions.

2.1.1 Facility Description

The full scope of the facility description can be addressed in this section or simply a brief overview with details provided in a separate appendix. Describe the physical environment(s) in which the system will operate, to include floor plans, equipment placement, electrical and plumbing outlets, telephone outlets, air conditioning vents, sprinkler systems, other fire prevention systems, fences, and extension of walls from floor to ceiling. A room diagram may be added in this section. If the system being accredited is in more than one location, each location must be annotated in this section.

2.1.2 Physical Security

Identify the procedures in place to counter physical threats from inside and outside of they system organization. Provide an overview of physical security practices in place that ensure unauthorized access to system resources. This will include perimeter security such as fences and security patrols, as well as door locks and alarm systems used to physically secure the systems resources.

2.1.3 Administrative Issues

Define the administrative security procedures in place that counter threats within your organization. This includes addressing separation of administrative duties that are designed to make fraud, abuse, or espionage difficult without collusion.

2.1.4 Personnel

Identify the number and type of personnel required to operate and maintain the system. Define clearance level for access as well as measures in place for the separation of duties that are not defined in section 2.1.3 (Administrative Issues).

2.1.5 COMSEC

Determine if National Security Agency (NSA) approved COMSEC and COMSEC key management procedures are required. Systems that deal with only unclassified information will not have COMSEC requirements, and COMSEC procedures will not apply. If that is the case for your system, so state.

2.1.5 TEMPEST

Determine if the equipment and site are required to meet TEMPEST and RED-BLACK requirements. Systems that deal with only unclassified information will not have TEMPEST requirements, and TEMPEST procedures will not apply. If that is the case for your system, so state.

2.1.7 Maintenance Procedures

Identify routine maintenance procedures. Certain categories of information mandate special maintenance procedures to ensure physical security protection against unauthorized access to the information or system resources.

2.1.8. Training Plans

Provide a brief summary of the training for individuals associated with the system's operation and determine if the training is appropriate to their level and area of responsibility. Training Plans should be more thoroughly addressed in Appendix O, “Security Education, Training, and Awareness Plan”. This training plan should provide

information about the security policy governing the information being processed as well as potential threats and the nature of the appropriate countermeasures.

2.2 Software Development and Maintenance Environment

Identify and describe the software development and maintenance environment. Address if software is developed on-site or off-site, as well as procedures for integration and testing of updated software.

2.3. Threat Description

Define the potential threats and single points of failure that can affect the confidentiality, integrity, and availability of the system. State the nature of the threat that is expected and where possible, the expected frequency of occurrence. System design weaknesses, human error, and intentional actions on the part of authorized as well as unauthorized users can cause these events. Most systems have common threats, such as penetration attempts by hackers, damage or misuse by disgruntled or dishonest employees, and misuse by careless or poorly trained employees. Generic threat information is available but it should be adapted to clearly state the threats expected to be encountered by the system (perceived threat). (The National Security Telecommunications and Information Systems Security Committee (NSTISSIC) prepares the "Annual Assessments of the Status of National Security Telecommunications and Information Systems Security within the United States Government" that includes generic threat statements that may be tailored to the specific system. The intelligence organization that is responsible for supporting the organizations that will operate the system may also have a threat statement.

3.0 SYSTEM ARCHITECTURAL DESCRIPTION

This is a paragraph title and should not contain any information. The following subparagraphs will identify System Architecture Description, System Interfaces and External Connections, Data Flow, and Accreditation Boundary.

The architecture description in the following subparagraphs provides the framework for the system architecture and includes a physical description of the hardware, software, firmware, and interfaces. Against this framework, the architecture description must identify and stipulate the security architecture. Existing or planned system features that facilitate expansion or external connection should be mentioned in this section. During the concept 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 provided.

3.1 System Architecture Description

This section must provide a complete system architecture description. Diagrams or drawings should be included to amplify the description. All components of the system should be described, e.g., user workstations, operating platforms, application software, database, communications, and other infrastructure. Identify and describe the hardware used and whether it is a standard commercial product, unique, or on the DoD Evaluated

Product List (EPL). Include an equipment list as separate Appendix. Describe the target hardware and its function. If this development effort involves an existing hardware change, identify the specific hardware components being changed. 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 commercial-off-the-shelf (COTS), government-off-the-shelf (GOTS), and on the EPL. Describe the target software and its intended use.

3.2 System Interfaces and External Connections

Provide a statement of the significant features of the communications layout. Include a diagram of the communications links and encryption techniques connecting the components of the information system, associated data communications, and networks.

3.3 Data Flow

Describe the system's external interfaces. The description should 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 specific transmission media are not necessary for the mission need, the mission need should state the basic transmission capability desired.

3.4 Accreditation Boundary

Describe the functional and physical boundary of the system. The description must include diagrams or text to clearly delineate what components are to be evaluated as part of the C&A task. All components included must be described in the systems description. Elements outside the accreditation boundary should be included in the description of the external interfaces.

4.0 SYSTEM SECURITY REQUIREMENTS

This is a paragraph title and should not contain any information. The following subparagraphs will identify specific requirements.

Security requirements are derived from the security policy, threats and vulnerabilities, and user need. Identify additional system-specific security requirements as needed.

4.1 National and DoD Security Requirements

Determine the security instructions or directives applicable to the system and from which the majority of system security requirements will be derived. You may use the following boilerplate content for most C2 and below level DoD systems. There are numerous revisions and new directives pending final approval, such as DoDD 8500.aa. The boilerplate provided should only be used for initial guidance.

National and DoD security instructions or directives applicable to *SYSTEM NAME* include:

National Security Decision Directive 145 (NSDD 145). The National Policy on Telecommunications and Automated Information Systems Security, September 1984, later revised and reissued in 1990 as National Security Directive 42, mandates the

protection of both classified and unclassified sensitive information processed, stored, and transmitted. NSDD 145 requires *SYSTEM NAME* to be as secure as necessary to prevent access by unauthorized individuals.

Public Law 100-235, known as the Computer Security Act of 1987, requires that every U.S. Government computer system, including *SYSTEM NAME*, that processes sensitive information, to have a customized computer security plan for the system's management and use. This law also requires that such system users receive periodic training in computer security.

Executive Order 12958, Classified National Security Information, signed 17 April 1995 to update Executive Order 12356, prescribes a uniform system for classifying, safeguarding, and declassifying national security information. *SYSTEM NAME* is to follow the prescribed actions of this Executive Order.

All applicable National/DoD security requirements derived from this list are must be shown as Requirements in Appendix F.

4.2 Governing Security Requirements

Determine requirements stipulated by local agencies and the DAA.

All applicable governing security requirements necessary to implement the above security services must be included in the security requirements list at Appendix F.

4.3 Data Security Requirements

Determine the type of data processed by the system. The type of data may require additional protections. Contact the data owner or organizations that have access to the system or share data with the system to determine their security requirements.

All applicable data security requirements necessary to implement the above security services must be included in the security requirements list at Appendix F.

4.4 Security CONOPS

The Security CONOPS should provide a detailed description of security processes as applied to system input, system processing, and intermittent and final outputs. Descriptions of all interactions and connections with external systems must be included.

4.5 Network Connection Rules

If the system is to be connected to any other network or system, there may be additional requirements incurred by connection to that system. A DAA for another system may have defined more stringent connection requirements for all systems to be connected to that system. These impose additional security requirements that must be evaluated in the C&A. These requirements and those of other systems that may be connected to this system or network must be added to the list at Appendix F. All interconnecting systems must be identified.

4.6 Configuration Management Requirements

This section should reference the system's organizational regulations or instructions regarding the review and approval of modifications or changes to the system. Configuration management policy or Configuration Management Review Board charter requirements must also be included. The requirements must be added to the list at Appendix F.

4.7 Reaccreditation Requirements

Information processing assets are re-accredited at least every 3 years or when a major change has been made that impacts security. The level of effort required for re-certification and re-accreditation action depends on the scope of the change to the security environment. Review of configuration management activities and the current environment by the DAA and certifying authority determines the actions required for re-accreditation. Re-accreditation may include the same steps accomplished for the original accreditation; however, portions of the security documentation, which remains valid, will not need to be redone. The following is a representative (not all-inclusive) example of events that may impact security and could require re-accreditation action. The ISSO must submit a request for re-accreditation under the conditions that follow:

- A change in criticality or sensitivity level of the information processed.
- A breach of security or violation of system integrity which reveals a flaw in security design, system security management, policy, or procedure.
- A change in the threat environment impacting overall system risks.
- A change in the system security mode of operation.
- A change in the operating system, security software, or hardware that affects the accredited security countermeasure implementation.

5.0 ORGANIZATIONS AND RESOURCES

This is a paragraph title and should not contain any information. The following subparagraphs will identify Organizations and Resources.

5.1 Organizations

Identify the organizations, individuals, and titles of the key authorities in the Certification and Accreditation (C&A) process. Include the names of the DAA, CA, PM, User Representative(s), and Information System Security Officer (ISSO).

5.2 Resources

Describe the personnel staffing and funding requirements required in conducting the C&A. If a contractor is involved or individuals from other government organizations are temporarily detailed to assist in the C&A process, funding requirements must be defined and included in the SSAA. The composition and size of the team will depend on the size and complexity of the system. The team should have members with composite

expertise in the whole span of activities required, and who are independent of the system developer or project Program Manager.

5.3 Training for the Certification Team

This section should briefly describe 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

Identify any other organizations or working groups that are supporting the C&A process.

6.0 DITSCAP Plan

This is a paragraph title and should not contain any information. The following subparagraphs will document the program's tasks and milestones for security-related functions, their schedules, estimated duration, responsible activity, and levels of effort.

6.1 Tailoring Factors This section is blank; it is a title.

6.1.1 Programmatic Considerations

Adjust the DITSCAP tasks to the system's specific program strategy. The DITSCAP Application Manual describes the DITSCAP for the grand design acquisition strategy (see Chapter 7). Other program strategies may require tailoring.

6.1.2 Security Environment

Identify any security constraints that might effect the level of effort required for the C&A process. Possible constraints may be associated with personnel, physical, administrative, procedural, operational, computer, network, and communications security components.

6.1.3 IS Characteristics

Identify the characteristics of the system that will determine the appropriate certification level (one of four levels). While the C&A phases and activities remain the same for any system, the level of analysis is tailored to the system. Four levels of certification are identified in Table C3.T8 of the DoD DITSCAP Application Manual where the analysis process is fully described.

Table 2 in Section 1.3.2 (System Certification Level) is the determining factors for the four levels of Certification.

6.1.4 Reuse of Previously Approved Solutions

Identify any software components reused from a previously approved security solution.

6.2 Tasks and Milestones

Describe C&A tasks and milestones to include schedules, estimated duration, responsible activity, and completion criteria.

6.3 Schedule Summary

Summarize the C&A schedule to address, at a minimum, completion dates for each of the C&A Phases.

6.4 Level of Effort

The level of effort in terms of resources required conducting all DITSCAP activities already are addressed in Paragraph 5.2. Therefore, for this section, describe the level of effort required for the specific certification level that was determined in Paragraph 6.1.3.

6.4 Roles and Responsibilities

Identify the roles of the certification team and their responsibilities.

APPENDICES

SSAA Appendices are added to include supplemental information that is relevant to the system's C&A. A sample of possible appendices is included below. Note the lettering of the appendices can change to tailor the C&A package.

APPENDIX A. Acronyms

Include only acronyms referenced within the SSAA.

APPENDIX B. Definitions

Include only definitions for words referenced within the SSAA.

APPENDIX C. References

Include references only for documents or publications referenced within the SSAA.

APPENDIX D. System or Operational Concept of Operations

Many systems have a document that describes the system or operational CONOPS. If so, include a short summary in Paragraph 1.4 of the SSAA and add the CONOPS document as an appendix here or listed as a reference. If a CONOPS is not available, a CONOPS must be prepared.

APPENDIX E. Information System Security Policy (ISSP)

The ISSP specifies the assumptions and objectives and sets the baseline for the definition of security requirements. This document defines the mission security needs related to system/components that must be satisfied by technical, procedural, and environmental controls. The security policy is a high-level document that addresses a target's security needs from the standpoint of the documented operational concept. The ISSP is independent from the design and implementation of the system, and its set of rules is static throughout the system's life cycle.

The purpose of the Information System Security Procedure (ISSP) is to:

a. Provide the user an overview of the system.

b. Promulgate security related guidelines and procedures to enhance user security awareness and training on the appropriate use of the system.

c. Enlist the support of all users of the system in the implementation of secure, dependable computer processing minimizing any opportunity for sabotage or denial of service, deliberate or inadvertent access to Sensitive Unclassified material by unauthorized personnel, or the unauthorized manipulation of the system which would lead to the compromise of information. User adherence to the procedures outlined in this document will facilitate timely and reliable operations for the user.

Security Standard Operating Procedures (SSOP's) may also be developed for users and system administrators respectively. They provide consolidated information for each specific audience.

APPENDIX F. Security Requirements Document/Traceability Matrix

As stated in the instructions for Paragraph 4 of the SSAA, you must describe all security requirements here. Please begin with the National/DoD level requirements and add to it additional system-specific requirements as needed. As a reminder, requirements should always be uniquely numbered and contain the word "shall." You also should input each requirement number into the program's traceability matrix for proper tracking in subsequent development and testing activities.

APPENDIX G. Certification Test and Evaluation (CT&E) Plan

The CT&E provides test cases to validate the technical security objectives as stated in Appendix F (Security Requirements Document/Traceability Matrix). Technical security objectives are those that are allocated to the system's hardware, software, and/or firmware. The CT&E tests will be performed on a system in a lab environment to mitigate any potential impact to the in-use network. The Certification Agent will evaluate the security of the system along with the Information System Security Officer (ISSO) or a representative appointed by the system's Program Office to ensure that it is in accordance with (IAW) acceptable standards.

In many situations, a common set of software, hardware, and firmware is installed at multiple locations. Since it is difficult to accredit the common systems at all possible locations, the DAA may issue a type accreditation for a typical operating environment. The type accreditation is the official authorization to employ identical copies of a system in a specified environment. The results of the CT&E will be shown in Appendix P.

APPENDIX H. Security Test and Evaluation (ST&E) Plan

The ST&E will address the confidentiality, integrity, availability, and accountability requirements that provide the necessary protections for the information processed, stored, and/or transmitted on the system. The ST&E plan provides test cases to validate each of the non-technical security objectives as stated in the Information System Security Policy (ISSP) for the system. Non-technical security objectives are those security objectives that are allocated to the environment to compliment the technical security objectives.

In addition to the non-technical security objectives, those technical security objectives that address the configuration and installation of the system are examined during ST&E, since ST&E is an examination of the system in its operational environment.

Security Test and Evaluation plans should address every security requirement included at Appendix F and provide sufficient evidence of the amount of residual risk. Validation of each requirement typically is accomplished by interview, document review, a testing technique, or observation as documented in the security test and evaluation (ST&E) plan. The results of the ST&E will be shown in Appendix P.

APPENDIX I. System Development Artifacts or System Documentation
This appendix contains a list with references to appropriate system development documentation as developed, such as the SRS, Software Requirements Description, change management control procedures, special program memoranda, or other artifacts supporting or affecting the C&A effort. It specifies the availability and source of the documentation. If none is identified, keep the appendix as a placeholder anyway in case artifacts are included at a later date.

APPENDIX J. System Rules of Behavior
Security rules of behavior for a system normally are documented as a standard operating procedure (SOP). If a security SOP or other memoranda have been or will be developed specifically for the system, include them here. Ensure that they clearly convey security installation and configuration requirements for system components and user access rules at user sites. If a separate security SOP or other memoranda do not exist, at a minimum, identify security installation and configuration requirements for system components and user access rules at user sites, and state them here.

APPENDIX K. Incident Response Plan
Every DoD system must have an Incident Response Plan designed to ensure that all security incidents or violations are investigated, documented, and reported to appropriate authorities. Include a copy of your system's plan here.

APPENDIX L. Contingency Plan(s)
This appendix should describe the emergency responses, backup procedures, backup operations, and recovery procedures for the system. The IT environment, the criticality of the functional applications being supported and the user's requirements influence the detail of the contingency plan.

It is essential that this document is kept current.

APPENDIX M. Personnel Controls
Describe here personnel procedures and planned system implementation features that are designed to satisfy the personnel requirements included at Appendix F.

APPENDIX N. Memorandums of Agreement – System Interconnect Agreements

DoD Directive 5200.28 states that when automated information systems (AISs) managed by different DAAs are interfaced or networked, a memorandum of agreement (MOA) is required that addresses the accreditation requirements for each AIS involved. The MOA should include description and classification of the data; clearance levels of the users; designation of the DAA who shall resolve conflicts among the DAAs; and safeguards to be implemented before interfacing the AISs. MOAs are required when one DoD Component's AIS interfaces with another AIS within the same DoD Component or in another DoD Component and when a contractor's AIS interfaces with a DoD Component's AIS or to another contractor's AIS. This appendix should contain a list of such MOAs and should specify the availability and source of the documentation.

If there are no MOAs required for the system, state it within this appendix.

APPENDIX O. Security Education, Training, and Awareness Plan

Every system must have a Security Education, Training, and Awareness Plan designed to provide program and functional managers, end users, system management, operations and programming staff, and security staff with the tools, skills, and procedures required to ensure that the security system is maintained. Include your plan in this appendix.

APPENDIX P. Test and Evaluation Report(s)

All testing, evaluation, and certification analysis results should be documented in this appendix. Subdividing this appendix (P-1, P-2, etc.) may help organize and display the various certification results more clearly.

1. Record of findings.
2. Evaluation of vulnerabilities discovered during evaluations.
3. Summary of the analysis level of effort.
4. Summary of tools used and results obtained.
5. Recommendations.

Task Analysis Summary Report Topics

APPENDIX Q. Residual Risk Assessment Results

A residual risk is the portion of risk remaining after security measures have been applied. The “Conduct DITSCAP Phase 3, Validation” includes test and evaluation tasks to assure the fully integrated system in its specific operating environment and configuration provides an acceptable level of residual risk. For each residual risk identified in Appendix P, a statement should be made to show the rationale for accepting or rejecting the risk and possible future modifications to resolve the problem. It may include an analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. If future solutions are proposed, a tentative implementation schedule should be included. This appendix summarizes all residual risks and their recommendations for the DAA who determines the acceptable level of residual risk and approves the system operation.

APPENDIX R. Certification and Accreditation Statements

This section contains the CA's recommendation to the DAA and the authorization to operate in a formal memorandum signed by the DAA, which is the accreditation memorandum.

Final Accreditation (Authority to Operate)

Accurate completion and DAA approval of all the sections of the SSAA and its appendices constitute a final C&A package. However, this is only the exit criterion of Phase 3 of the DITSCAP. Phase 4 of the DITSCAP requires the C&A package to be reviewed frequently and all information contained within the C&A package to remain current. Authority to Operate is granted for three years unless significant changes to the system (that effect the security posture) warrant re-accreditation.

Responsibilities

Maintaining the security posture of an IT System is the responsibility of everyone within the systems organization, from the basic user to the super users. As information security specialists, ensuring this happens at every level is our responsibility. We must maintain diligence over every aspect of security, whether it is ensuring the system administrators are installing appropriate security patches on the system, to ensuring the everyday users are fully aware of social engineering tactics and basic OPSEC. The DITSCAP is a useful tool for all Information Security Specialists that support the Department of Defense. It is a comprehensive Instruction that makes security a requirement, not an option.

References:

1.) DOD Instruction 5200.40 “DoD Information Technology Security Certification and Accreditation Process (DITSCAP)” December 30, 1997
URL: http://mattche.iiie.disa.mil/ditscap/DitscapFrame.html

2.) Streamlining DITSCAP Documentation
URL: http://www.tcs-sec.com/services/c_and_a/tcs_ditscap.pdf

3.) National Institute of Standards and Technology “System Certification and Accreditation Project”
URL: http://csrc.nist.gov/sec-cert

4.) DoD 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," 7/2000
URL: http://www.dtic.mil/whs/directives/corres/html/85101m.htm

5.) Office of Assistant Secretary of Defense Memorandum, “The Defense Information Systems Security Program (DISSP)”, August 19, 1992.

6.) Public Law 100-235, “Computer Security Act of 1987”, January 8, 1988
URL: http://www.house.gov/science_democrats/archive/compsec1.htm

7.) Office of Management and Budget Circular No. A-130, “Management of Federal Information Resources,” February 8, 1996

8.) DoN IA Publication 5239-13 Volumes I, II, and III, “Department of the Navy Certification and Accreditation” April 30, 1991