Global Information Assurance Certification Paper

UNDERSTANDING NIST 800-37 and DITSCAP

GSEC Practical Assignment Version 1.4c

Sharrie Takewell

1/24/05

ABSTRACT

In May of 2004 the National Institute Standards Technology (NIST) released Special Publication (SP) 800-37, Guide for Security Certification and Accreditation of Federal Information Systems. SP 800-37 is a Certification and Accreditation (C&A) Guide intended to establish a consistent C&A methodology throughout government agencies. It is primarily based on Federal Information Security Management Act (FISMA) and the Office of Management and Budget (OMB) circular A-130 Appendix III. FISMA requires NIST to establish standards and guidelines for information systems. Additionally, FISMA requires federal agencies to establish agency-wide, risk-based, and cost-effective information security programs. (symantec). Certification and accreditation activities of all systems are tracked using performance measures through the annual FISMA report. To meet these FISMA and OMB A-130 requirements, it is expected that agencies will adopt NIST C&A guidance and utilize it to prepare agency specific C&A processes.

There are several C&A agency processes, all having their own methodology and requirements. An example of one such agency process is the Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP), DoD Instruction 5200.40. DITSCAP is a process owned by the DOD and defines how to implement the DOD C&A process. This paper will discuss DITSCAP, SP 800-37, and other Legislative mandates. It will provide the reader with an understanding and the relationship between DITSCAP, NIST SP 800-37, and related legislative policy drivers. Also, it will give the reader a further understanding of DITSCAP and NIST by explaining what has changed since the 1997 release 5200.40 and give a brief explanation of the DoD directives and Instructions that relate to DITSCAP. Finally, it will give a brief overview of the NIST C&A methodology, and compare it to the current DISTCAP.

BACKGROUND INFORMATION

Understanding NIST 800-37 and DITSCAP requires knowledge of C&A concepts and the relationship between NIST and FISMA. This section will provide an overview of the C&A process, FISMA, and NIST.

What is C&A a brief overview:

C&A is a process that emphasizes security testing, analyzing the test results, and accepting the risks for operation of an information system. The main goal of C&A is to ensure acceptable security controls are applied to a system and that these controls reduce the risks at an acceptable level of confidentiality, availability, integrity and accountability. The C&A process consists of two distinct phases:(1)Certification and (2)Accreditation.

Certification must be completed before accreditation may begin. Certification is

basically preparing the system for approval to operate. It involves assessing the system's security controls and writing supporting documentation including tests to meet the security requirements. The requirements come from various sources depending on the agency. For example a majority of the requirements for DODIIS C&A are in DCID 6/3. The type of security requirements depends on the different levels of security. For example a system at the top secret level obviously has more stringent security requirements than a system at the secret level. Each requirement must be verified and validated. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system (SP 800-37,1).

Accreditation is the second phase of the C&A process. During the accreditation phase, the findings from the certification phase are analyzed. Accreditation involves approving the system for operation based on accepting the risks from certification. An assumption is made that the IS can operate at an adequate level of risk. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls (SP 800-37,1).

What is FISMA - a brief overview:

The E-Government Act (Public Law 107-347) was passed by the 107th Congress and signed into law by the President in December 2002. FISMA is Title III of the E-Government Act, entitled the Federal Information Security Management Act.

FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source (NIST Background). This is accomplished by meeting the security requirements and demonstrating these requirements are satisfied by following an effective C&A process. Additionally, FISMA requires federal agencies to establish agency-wide, risk-based, and cost-effective information security programs. Agencies must now create and implement a process to meet the FISMA requirements. These programs must include provisions for identification and resolution of current IT security weaknesses and risks, as well as protection against future vulnerabilities and threats (symantec, 1). FISMA requires each agency to inventory its major computer systems, to identify and provide appropriate security protections, and to develop, document, and implement an agency-wide information security program (Moteff, 2).

FISMA requires agencies to:

- [Develop security policies, plans and procedures
- Conduct periodic risk assessments
- Comply with information security standards
- Develop Personnel Security training
- Conduct periodic testing and evaluation
- Reporting and plans for remedial action, security incident response
- Develop plans and procedures to ensure continuity of operations] (NetSec, 1)

FISMA requires NIST to develop standards and guides to be used by agencies. FISMA also requires annual independent evaluation of federal agency information security programs and practices.

What is NIST – a brief overview:

History of NIST

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life (NIST General Information). 800-37 was prepared to provide C&A guidance to government agencies in accordance with FISMA of 2002, Public Law 107-347 and OMB Circular A –130. In addition to the C&A guide NIST has prepared other documentation to meet FISMA requirements. SP 800-18 was prepared to provide guidance on creating a security plan, and SP 800-30 provides risk management guidance. SP 800-53 is currently released in draft form and contains a list of recommended security controls based on the IS security categorization. For a complete list of NIST security guidelines refer to the following link: <http://csrc.nist.gov/publications/nistpubs/index.html>

Relationship between NIST, OMB Circular A-130, and FISMA

According to FISMA Title III Subparagraph III section 303 NIST shall:

- Have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

- Develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

- Categorize all information systems collected or maintained by each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.

OMB Circular A-130
Agency information security activities are guided by OMB policy and the development of information security standards by the NIST that will include minimum mandatory requirements by risk level (Symantec).
OMB requires Federal Agencies to:

- [Plan for Security
- Ensure that appropriate officials are assigned security Responsibility
- Authorize system processing prior to operations and periodically, thereafter.] (Ross)

Additionally, OMB Circular A-130 requires agencies to implement NIST guidance. Section 8b(3)(a)(ii) states the following:

> Apply OMB policies and, for non-national security applications, NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of harm;

In short, agencies must follow NIST guidance to fulfill the OMB A-130 requirements. OMB A-130 requires agencies to ensure security in IA systems and to follow NIST guidance to meet the OMB A-130 requirements.

UNDERSTANDING DITSCAP
DITSCAP is the DoD C&A process. The purpose of DITSCAP is to establish a standard process, set of activities, general tasks and a management structure to certify and accredit an IS that will maintain the information assurance and security posture of the Defense Information Infrastructure (DII) (8510.1M,23). DITSCAP consists of the following four phases: (i)Definition (ii)Verification, (iii)Validation, and (iv)Post Accreditation.

How DITSCAP relates to other DOD Directives and Instructions
DoD Instruction 5200.40 implements policy, assigns responsibilities, and prescribes procedures under DoD Directive 5200.28 Security Requirements for Automated Systems "(DoD 5200.40, References). However, DoD Directive 8500.1 supersedes 5200.28. Presently the combination 5200.40, D0D8510.1-M establishes the DITSCAP. For the beginner, understanding the relationship between DITSCAP and DoD related Directives, instructions and manuals could be confusing. This section will discuss how DITSCAP relates to other DoD documentation.

DoD Directive 8500.1 Information Assurance is a directive that establishes policy and assigns responsibilities under 10 U.S.C 2224 to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology and supports the evolution to network centric warfare (Defense Acquisition Guidebook, 7.5.2). The Defense –In –Depth approach maintains an appropriate level of confidentiality integrity, authentication non-repudiation, and availability. 8500.1 requires that all DOD

owned or controlled information systems are certified and accredited using the DOD Instruction 5200.40. It requires DoD IA systems to be organized in four categories.

- Automated info system application
- Enclaves
- Outsourced IT-based processes
- Platform IT interconnections

DoD 8510.1-M DITSCAP Application Manual - Provides implementation guidance to standardize the certification and accreditation process throughout the DoD (DoD 8510.1-M, forward).

DoD 8500.2 February 6, 2003 is an instruction for Information Assurance Implementation. It implements the policies in DoD Directive 8500.1. It references Division E of the Clinger-Cohen Act and DoD Instruction 5200.40 DITSCAP and OMB Circular A-30.

DoD Instruction 5200.40 DITSCAP references OMB Circular No. A-130, "management of Federal Information Resources, Feb 8, 1996. OMB Circular A-130 focuses heavily on capital planning and IT security processes. Since the 1997 release of DITSCAP, there has been a revision to circular A-130. In 2000 A-130 was revised. The addition to the circular is the inclusion of the Clinger-Cohen Act of 1996. A-130 now reflects Clinger-Cohen and the role of the CIO (CCA Overview). It also emphasizes the tie between capital planning and the development of an enterprise IT architecture, a plan for how technology is going to help an agency accomplish its mission (Frank).

How Clinger-Cohen applies to C&A

The Clinger-Cohen Act (CCA) of 1996 (40 U.S.C. 1401(3)), also known as the Information Technology Management Reform Act, was intended, among its many other purposes, to "reform acquisition laws and information technology management of the Federal Government" (What is Electronic and IT). CCA is a law that codifies best practices for the Program Management of IT Programs, and applies to all IT systems including National Security Systems (NSS) (CCA Overview). CCA is designed to improve the way the Federal Government acquires and manages information technology. One of the key words, in the above statement, regarding C&A process is "manage". If the federal government is to manage Information technology successfully the C&A process must be applied in a consistent manner, emphasizing risk and cost. It requires the Department and individual programs to use performance based management principles for acquiring information technology (IT), including National Security Systems (NSS) (CCA Overview). NIST 800-37 emphasizes risk-base policy for cost-based security (800-37,4).

Changes Since 1997 DITSCAP Release

DOD Instruction 5200.40 DITSCAP was released in 1997. Since that time, changes abound pertaining to Information Assurance (IA) and C&A. There is a successor DIACAP, but to date has not been released to the public. There have been countless legislative mandates, guidelines, directives and instructions created, cancelled or revised effecting IA and C&A. Below is a table that outlines many of the major changes that relate to DITSCAP and C&A.

Title	Release DATE	Reason	Purpose
Federal Information Security Management Act FISMA	2002	Replace GISRA	Provide a framework for enhancing the effectiveness of information security in the federal government. Part of E-Government Act of 2002 (Public Law 107-347), replacing the Government Information Security Reform Act (GISRA).
Cyber Security Research and Development Act of 2002	2002	New	Cyber Security Research and Development Act of 2002 (15 U.S.C.A. 7410) was established to strengthen Internet Security
Homeland Security Presidential Directive #7	Dec-03	New	This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
DOD Acquisition Guidebook	Oct-04	New Release	Guidebook for the Defense Acquisition System. It can be used as a reference tool/source. Chapters contain non-mandatory staff expectations for satisfying the mandatory requirements in DoD Instruction 5000.2. Chapter 7 of the Guidebook discusses Information Technology and Security Systems.
DoD Directive 8500.1, "Information Assurance (IA)"	Oct-02	New Release	This directive establishes policy and assigns responsibilities to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare. According to DoD Directive 8500.1, all acquisitions of Automated Information Systems (AISs) with connections to the Global Information Grid (GIG) must be certified and accredited according to DoD Instruction 5200.40, DITSCAP. Supersedes DoD Directive 5200.28, DoD 5200.28-M, DoD 5200.28-STD
DoD Instruction 8500.2, "Information Assurance (IA) Implementation"	Feb-04	New Release	This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.1.
DoD Directive 5000.1The Defense Acquisition System	May-04	Reissue	This directive provides management principles and mandatory policies and procedures for managing all acquisition programs.
DoD Instruction 5000.2, "Operation of the Defense Acquisition System,"	May-04	Reissue Implements new 5000.1 policies	This instruction implements policy, assigns responsibilities, and prescribes procedures and Establishes a simplified and flexible management framework for translating mission needs and technology opportunities, based on approved mission needs and requirements, into stable, affordable, and well-managed acquisition programs that include weapon systems and automated information systems (AISs).
NSTISSI No. 1000 National Information Assurance Certification and Accreditation Process	Apr-00		This instruction defines the National information Assurance Certification and Accreditation Process.

D0D Instruction 8580.1"Information Assurance (IA) in the Defense Acquisition System":	Jul-04	New Release	This instruction implements policy, assigns responsibilities, and prescribes procedures necessary to integrate information assurance (IA) into the Defense Acquisition System; describes required and recommended levels of IA activities relative to the acquisition of systems and services; describes the essential elements of an Acquisition IA Strategy, its applicability, and prescribes an Acquisition IA Strategy submission and review process.

CANCELED DoD Directive 5200.28 Security Requirements for Automated Systems, March 21, 1988 Superseded by DoD Directive 8500.1 Information Assurance

REVISED Office of Management and Budget (OMB) Circular No. A-130,1996 Revised in 2000.

PROCESS COMPARISON: NIST 800-37 Compared to DITSCAP

This section will compare each phase of NIST 800-37 with phases of DITSCAP. Both SP 800-37 process and the DITSCAP have four main phases. At first glance, the two appear to be almost identical. However, taking a more detailed look at the tasks and activities reveals some subtle differences.

NIST SP 800-37 C&A process consists of the following four phases:

- Initiation Phase
- Security Certification Phase
- Security Accreditation Phase
- Continuous Monitoring Phase

DITSCAP consists of the following four phases:

- Definition
- Verification
- Validation
- Post Accreditation

Phase one: Initiation Phase Vs Definition Phase:

Initiation Phase consists of three tasks: (i) preparation: (ii) notification and resource identification: and (iii) system security plan analysis, update and acceptance (SP 800-37, 26). The purpose of this phase ensures that the authorizing official and senior agency information security officer are in agreement with the contents of the system security plan including requirements (SP 800-37, 2)

DITSCAP Definition Phase contains three activities: (i) Preparation: Registration: and (iii) Negotiation. The purpose of this phase is to collect documentation associated with the system, begin vulnerability assessment, prepare and accurate description of the system, and establish an agreement on the level of effort.

The majority of the tasks within the two phases seem to resemble each other but SP 800-37 Initiation phase contains more emphasis on risk in the preparation task than DITSCAP does in the Definition Phase. DITSCAP contains emphasis on documenting the requirements, determining the scope and schedule, and planning for certification activities. 800-37 Initiation Phase requires consistency with the system security plan and the initial risk assessment. DITSCAP begins to identify vulnerabilities at this point while 800-37 requires a completed initial risk assessment.

A good C&A process contains comprehensive threat assessments, vulnerability assessments, and Risk assessments. SP 800-37 attempts to do this by starting early in the process. These assessments contribute significantly to the success of a IS program. In order to determine the risks, the underlying threats and the vulnerabilities must be known. Threats may be either internal or external to the IS. There are environmental and physical threats that may be either natural or man made. Additionally, an IS invariably has vulnerabilities, most of which are technical. There are network vulnerabilities that may be either internal or external and system vulnerabilities associated with external communications. An important element of a good C&A process is risk management based on a risk assessment. In order to conduct a risk assessment, a threat assessment and vulnerability assessment must first be performed. DITSCAP too conducts threat and vulnerability assessments. However in SP 800-37 threats and vulnerabilities are emphasized early and throughout the entire process. Results of the risk assessment are then used as a basis for identifying security controls or safeguards.

Phase Two SECURITY CERTIFICATION PHASE vs. Verification Phase:

The main focus of the Security Certification Phase is determining if security controls are implemented and operating according to the security requirements. Phase two also concentrates on correcting deficiencies and reducing or eliminating known vulnerabilities.

DITSCAP's Verification phase primarily concentrates on verifying security requirements collecting evidence to support certification and determine if the IS is ready to be evaluated and tested during phase 3, validation phase. Additionally, the IS is analyzed for compliance and evaluated to ensure policies are enforced.

One of the main differences between the Certification Phase and DISTSCAP's Verification Phase is that SP 800-37 emphasizes reuse of previous evaluation/assessment results. One example of such reuse is utilizing countermeasures previously used on other evaluations. Countermeasures

include controls such as physical access restrictions, system access control, encryption of transmissions, Intrusion Detection Systems (IDS) incident response and reporting, environmental protection, personnel segregation of duties, etc. Ultimately security controls are put into place to protect assets. To assist and promote reuse NIST has prepared SP 800-53A, which when completed, will provide standardized methods for assessing security controls. It is hoped it will provide techniques and procedures for effectively assessing security controls. Unfortunately, the current release date has been delayed due to budget cuts. SP 800-53A will be based on the security controls listed in SP 800-53. The security controls are categorized for low, moderate, and high impact information systems based upon the system's FIPS 199 security categorization. Currently SP 800-53 is in its second draft iteration and is expected to be released later in the year.

Phase three Security Accreditation Phase Vs. Validation Phase:

During SP 800-37 Security Accreditation Phase the risk level is determined. A decision will be made on whether to accept the risk level, given the known vulnerabilities. If the approving authority determines the risk level is at an acceptable level the IS will be given an approval to operate. This decision will be made based on the results of the certification phase. These results are the vulnerabilities confirmed during the Certification Phase. The vulnerabilities were confirmed by various testing techniques.

DISTCAP Validation Phase validates the IS is operating with an acceptable level of risk. It also includes certification tasks that include certification of software, firmware, hardware, etc. Phase 3 includes tasks to certify the compatibility of the computing environment with the description provided in the SSAA (DITSCAP Manual).

One of the main difference between the two phases is that SP 800-37 relies heavily on the results from the Certification Phase, taking a more cost-effective approach by utilizing the results from the Certification Phase. These results are the confirmed vulnerabilities determined and collected during testing the security controls and verifying the security requirements. DITSCAP conducts testing in its second phase too. However, it also emphasizes additional testing in the Validation Phase. This additional testing is referred to as Security Testing and Evaluation (ST&E).

Phase four Continuous Monitoring Phase Vs. Post Accreditation Phase:

The Continuous Monitoring Phase consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The status reporting includes reporting FISMA requirements.

The Post Accreditation Phase is the final phase of DITSCAP and continues until the IS is removed from service, a major change is planned for the system, or a periodic compliance is required. The main difference between the Continuous Monitoring Phase and the Post Accreditation Phase is that there is no explicit task in DISTCAP that includes reporting FISMA requirements.

A good IS program includes some type of continuous monitoring phase. Whether it is DITSCAP's Post Accreditation Phase or SP 8800-37 Continuous Monitoring phase, the IS program should include an iterative process that must be capable of adjusting as objectives change, as technology evolves, as customer needs evolve, as threats increase or decrease, as new vulnerabilities are exposed, as upgrades and improvements are made, etc. A continuous monitoring phase includes all this and more. Additionally, to meet FISMA requirements, it must also include documenting relevant security aspects and reporting this documentation.

The table below lists all the 800-37 process steps and attempts to map the DITSCAP steps with the associated 800-37 process steps. In most cases there is not a direct mapping but the Phases do seem to align while the tasks do not.

NIST 800-37 Process Steps	NIST 800-37 Task Description	DITSCAP Process Steps
INITIATION PHASE		**DEFINITION PHASE**
TASK 1: PREPARATION	Review system security plan and confirm consistency with an initial assessment of risk.	Activity 1 Preparation. Information and documentation is collected about the system. It includes capabilities and functions, interfaces and data flows. Typically contained in the business case or mission needs statement.
SUBTASK 1.1 INFORMATION SYSTEM DESCRIPTION	Describes: the purpose, functions, and capabilities; the types of information processed, stored, and transmitted; the boundary; the functional requirements; the architecture	Task 1-1; Review Documentation. The objective of this task is to obtain and review documentation relevant to the system. This information includes capabilities and functions the system will perform, operational organizations supported, intended operational environment, and operational threat.

SUBTASK 1.2 SECURITY CATEGORIZATION	Security categorization is documented in the system identification section of the system security plan. FIPS 199 establishes three potential impact levels (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing federal information systems.	Registration Activity Registration initiates the risk management agreement process among the program manager, DAA, Certifier, and user representative. Information is evaluated, applicable IA requirements are determined, risk management and vulnerability assessment actions begin, and the level of effort required for C&A is determined and planned.
THREAT IDENTIFICATION SUBTASK 1.3	Confirm that potential threats that could exploit information system flaws or weaknesses have been identified and documented in the system security plan, risk assessment, or an equivalent document.	Task 1-2; Prepare the System, functional description and system identification. The objective of this task is to prepare an accurate description of the system. It includes system identification, functional description system capabilities, criticality classification and sensitivity of data users and life cycle.
VULNERABILITY IDENTIFICATION SUBTASK 1.4	Document Vulnerabilities. Vulnerability sources include, for example: previous risk assessment documentation; audit reports; system anomaly reports; security reviews; self assessments; results of vulnerability scans and penetration tests;	Task 1-3; Register the System. The objective of this task is to identify the agencies and individuals involved in the C&A process and determine the current status of the system.
SECURITY CONTROL IDENTIFICATION SUBTASK 1.5	Confirm that the security controls (either planned or implemented) for the information system have been identified and documented in the system security plan or an equivalent document.	Task 1-4; Prepare the Environment and Threat Description. The objective of this task is to define the system environment and potential threats to the system. Define the potential threats and single points of failure that can affect the confidentiality, integrity, and availability of the system.
INITIAL RISK DETERMINATION SUBTASK 1.6	Confirm that the risk to agency operations, agency assets, or individuals has been determined	Task 1-5; Determine the System Security Requirements. The objective of this task is to identify the system security requirements. They may include applicable instructions or directives. governing security requisites, data security requirements, and security concept of operations.
TASK 2: NOTIFICATION AND RESOURCE IDENTIFICATION	Provide notification to all concerned agency officials as to the impending security certification and accreditation of the information system; (ii) determine the resources needed to carry out the effort; and (iii) prepare a plan of execution for the certification and accreditation activities	Task 1-6; Prepare the System Architecture Description. The objective of this task is to prepare a high level overview of the types of hardware, software, firmware and associated interfaces envisioned for the completed system. This may include System Hardware software and firmware, interfaces and accreditation boundary.

NOTIFICATION SUBTASK 2.1	Inform the senior agency information security officer, authorizing official, certification agent, user representatives, and other interested agency officials that the information system requires security certification and accreditation support.	Task 1-7; Identify the C&A organizations and the resources required. The objective of this task is to identify the organizations and individuals involved in the C&A process.
PLANNING AND RESOURCES SUBTASK 2.2	Determine the level of effort and resources required for the security certification and accreditation of the information system (including organizations involved) and prepare a plan of execution.	Task 1-8; Tailor the DITSCAP and Prepare the DITSCAP Plan. The objective of this task is to tailor the DITSCAP to the system and prepare the DITSCAP plan. This task determines the appropriate certification level and adjusts the DITSCAP activities to the program strategy and system life cycle.
TASK 3: SYSTEM SECURITY PLAN ANALYSIS, UPDATE, AND ACCEPTANCE	Perform an independent review of the FIPS 199 security categorization; (ii) obtain an independent analysis of the system security plan; (iii) update the system security plan as needed based on the results of the independent analysis; and (iv) obtain acceptance of the system security plan by the authorizing official and senior agency information security officer prior to conducting an assessment of the security controls in the information system.	Task 1-9; Draft the SSAA. The objective of this task is to complete and assemble the SSAA document.
SECURITY CATEGORIZATION REVIEW SUBTASK 3.1	Review the FIPS 199 security categorization described in the system security plan to determine if the assigned impact values with respect to the potential loss of confidentiality, integrity, and availability are consistent with agency's actual mission requirements.	Negotiation Activity. During negotiation all the participants involved in the IS's development, acquisition, operation, security certification, and accreditation reach agreement on the implementation strategy to be used to satisfy the security requirements.
SYSTEM SECURITY PLAN ANALYSIS SUBTASK 3.2	Analyze the system security plan to determine if the vulnerabilities in the information system and the resulting risk to agency operations, agency assets, or individuals are actually what the plan would produce, if implemented.	Task 1-10; Conduct Certification Requirements Review. The objective of this task is to conduct a CRR.
SYSTEM SECURITY PLAN UPDATE SUBTASK 3.3	Update the system security plan based on the results of the independent analysis and recommendations of the certification agent, authorizing official, and senior agency information security officer	Task 1-11; Establish Agreement on Level of Effort and schedule the objective of this task is to agree on the C&A level of effort and schedule.
SYSTEM SECURITY PLAN ACCEPTANCE SUBTASK 3.4	Review the system security plan to determine if the risk to agency operations, agency assets, or individuals is acceptable.	Task 1-12; Approve Phase 1 SSAA. The objective of this task is to obtain the DAA's approval on the Phase 1 SSAA.

3.2 SECURITY CERTIFICATION PHASE	Security control assessment; and (ii) security certification documentation. The purpose of this phase is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. It also addresses specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system. Upon successful completion of this phase, the authorizing official will have the information needed from the security certification to determine the risk to agency operations, agency assets, or individuals—and thus will be able to render an appropriate accreditation decision.	**PHASE 2, VERIFICATION** Phase 2 activities include verifying security requirements during system development or modification, certification analysis, CT&E (type accreditation only), and analysis of the certification results. The SSAA is refined during Phase 2. Phase 2 activities examine the evolving system in a process similar to an Independent Verification and Validation. As the system development activity progresses and details of the system evolve, the certification effort examines the updated system and its design. All the Phase 2 activities are tailored to meet the certification level defined in Phase 1.
TASK 4: SECURITY CONTROL ASSESSMENT	The objective of the security control assessment task is to: (i) prepare for the assessment of the security controls in the information system; (ii) conduct the assessment of the security controls; and (iii) document the results of the assessment.	SSAA Refinement. Phase 2 starts with a review of the SSAA. During the Phase 2 activities, evidence is collected to support the certification.
DOCUMENTATION AND SUPPORTING MATERIALS SUBTASK 4.1	Assemble any documentation and supporting materials necessary for the assessment of the security controls in the information system; if these documents include previous assessments of security controls, review the findings, results, and evidence.	*System Development and Integration.* These activities are required for development or integration of the IS components as defined in the system's functional and security requirements. This activity verifies requirements in the SSAA are met in the evolving system before it is integrated into the operating environment.
METHODS AND PROCEDURES SUBTASK 4.2	Select, or develop when needed, appropriate methods and procedures to assess the management, operational, and technical security controls in the information system. In lieu of developing unique or specialized methods and procedures to assess the security controls in the information system, certification agents should consult NIST Special Publication 800-53A,	*Initial Certification Analysis.* This task determines if the IS is ready to be evaluated and tested during Phase 3, Validation. Phase 2 initial analysis tasks complement the functional testing certification tasks that occur during Phase 3. 1. System Architecture Analysis. 2. Software Design Analysis. 3. Network Connection Rule Compliance Analysis. 4. Integrity Analysis of Integrated Products. 5. Life-Cycle Management Analysis. 6. Security Requirements Validation Procedures Preparation. 7. Vulnerability Assessment.

SECURITY ASSESSMENT SUBTASK 4.3	Assess the management, operational, and technical security controls in the information system using methods and procedures selected or developed.	Task 2-1; System Architecture Analysis. The objective of this task is to ensure that the system architecture complies with the architecture description agreed on in the SSAA.
SECURITY ASSESSMENT REPORT SUBTASK 4.4	Prepare the final security assessment report.	Task 2-2, Software, Hardware, and Firmware Design Anal The objective of this task is to assess the software, hardware, and firmware security architecture to evaluate the compliance of the design with the stated approach in the SSAA and to evaluate compliance with all planned requirements.
TASK 5: SECURITY CERTIFICATION DOCUMENTATION	Provide the certification findings and recommendations to the information system owner; (ii) update the system security plan as needed; (iii) prepare the plan of action and milestones; and (iv) assemble the accreditation package. The information system owner has an opportunity to reduce or eliminate vulnerabilities in the information system prior to the assembly and compilation of the accreditation package and submission to the authorizing official. This is accomplished by implementing corrective actions recommended by the certification agent.	Task 2-3, Network Connection Rule Compliance Analysis. The objective of this task is to evaluate the connections to other systems and/or networks to ensure that network and overall system security policies are enforced.
FINDINGS AND RECOMMENDATIO NS SUBTASK 5.1:	Provide the information system owner with the security assessment report.	
SYSTEM SECURITY PLAN UPDATE SUBTASK 5.2	Update the system security plan (and risk assessment) based on the results of the security assessment and any modifications to the security controls in the information system.	Task 2-5, Life-Cycle Management Analysis. The objective of this task is to evaluate the ability of configuration management (CM) practices to preserve the integrity of the identified security-relevant software and hardware.
PLAN OF ACTION AND MILESTONES PREPARATION SUBTASK 5.3	Prepare the plan of action and milestones based on the results of the security assessment.	Task 2-6, Security Requirements Validation Procedures. The objective of this task is to prepare the written procedures used in Phase 3 to validate compliance with the technical security requirements.
ACCREDITATION PACKAGE ASSEMBLY SUBTASK 5.4	Assemble the final security accreditation package and submit to authorizing official.	Task 2-7, Vulnerability Assessment. The objective of this task is to evaluate security vulnerabilities (confidentiality, integrity, availability, and accountability), evaluate residual risk, and recommend appropriate countermeasures.

3.3 SECURITY ACCREDITATION PHASE	The Security Accreditation Phase consists of two tasks: (i) security accreditation decision; and (ii) security accreditation documentation. The purpose of this phase is to determine if the remaining known vulnerabilities in the information system (after the implementation of an agreed-upon set of security controls) pose an acceptable level of risk to agency operations, agency assets, or individuals. Upon successful completion of this phase, the information system owner will have: (i) authorization to operate the information system; (ii) an interim authorization to operate the information system under specific terms and conditions; or (iii) denial of authorization to operate the information system.	**PHASE 3, VALIDATION** Validate that the preceding work has produced an IS that operates in a specified computing environment with an acceptable level of residual risk. This phase includes a review of the SSAA, evaluation of the integrated IS, certification, and accreditation. Phase 3 certification tasks include certification of software, firmware, hardware, and inspections of operational sites to ensure their compliance with physical security, procedural security, TEMPEST and COMSEC requirements, personnel security, and security education, and awareness requirements. It also includes tasks to certify the compatibility of the environment.
TASK 6: SECURITY ACCREDITATION DECISION	The objective of the security accreditation decision task is to: (i) determine the risk to agency operations, agency assets, or individuals; and (ii) determine if the agency-level risk is acceptable. The authorizing official, working with information from the information system owner, information system security officer, and certification agent produced during the previous phase, has independent confirmation of the identified vulnerabilities in the information system and a list of planned or completed corrective actions to reduce or eliminate those vulnerabilities. It is this information that is used to determine the final risk to the agency and the acceptability of that risk.	*SSAA Refinement.* Phase 3 begins with a review of the SSAA to ensure that its requirements and agreements still apply
FINAL RISK DETERMINATION SUBTASK 6.1	Determine the risk to agency operations, agency assets, or individuals based on the vulnerabilities in the information system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities.	*Certification Evaluation of the Integrated System.* This activity certifies that the fully integrated and operational system will comply with the requirements stated in the SSAA and the system will be operated with an acceptable level of residual risk. 1. Security Test and Evaluation 2. Penetration Testing 3. TEMPEST and RED-BLACK Evaluation 4. COMSEC Compliance Evaluation 5. System Management Analysis 6. Site Accreditation Survey 7. Contingency Plan Evaluation 8. Risk Management Review

RISK ACCEPTABILITY SUBTASK 6.2	Determine if the risk to agency operations, agency assets, or individuals is acceptable and prepare the final security accreditation decision letter.	Task 3-1, Security Test and Evaluation (ST&E). The objective of this task is to evaluate the technical implementation of the security design and to ascertain that security software, hardware, and firmware affecting confidentiality, integrity, availability, and accountability have been implemented as documented in the SSAA and that the features perform properly.
TASK 7: SECURITY ACCREDITATION DOCUMENTATION	The objective of the security accreditation documentation task is to: (i) transmit the final security accreditation package to the appropriate individuals and organizations; and (ii) update the system security plan with the latest information from the accreditation decision. The completion of this task concludes the Security Accreditation Phase of the security certification and accreditation process.	Task 3-2, Penetration Testing. The objective of this task is to assess the system's ability to withstand intentional attempts to circumvent security features through exploitation of the technical security vulnerabilities. Task 3-3, TEMPEST and RED-BLACK Verification. The objective of this task is to validate that the equipment and site meet the TEMPEST and RED-BLACK requirements. Task 3-4, COMSEC Compliance Verification.
SECURITY ACCREDITATION PACKAGE TRANSMISSION SUBTASK 7.1	Provide copies of the final security accreditation package including the accreditation decision letter (in either paper or electronic form), to the information system owner and any other agency officials having an interest (i.e., need to know) in the security of the information system.	Task 3-5, System Management Analysis. The objective of this task is to ensure that security management procedures are in place, operational, and effective. This task verifies that configuration management policies and programs consider security implications in all modifications to the accredited system baseline and operational concept.

SYSTEM SECURITY PLAN UPDATE SUBTASK 7.2	Update the system security plan based on the final determination of risk to agency operations, agency assets, or individuals.	Task 3-6, Site Accreditation Survey. The objective of this task is to evaluate the site to ensure that the integration and operation of the system, with its certified design and operational concept, pose an acceptable risk to the information being processed. Task 3-7, Contingency Plan Evaluation. The objective of this task is to ensure that contingency plans are developed and provide reasonable continuity of IS support if events occur that prevent normal operations. Task 3-8, Risk Management Review. The objective of this task is to assess the overall security design and architecture against the concept of operations, operational environment, information security policy requirements, and threats to ensure that risks to confidentiality, integrity, availability, and accountability of the information and system are acceptable.
3.4 CONTINOUS MONITORING PHASE	The Continuous Monitoring Phase consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the information system. Reaccreditation may be required because of specific changes to the information system or because federal or agency policies require periodic reaccreditation of the information system.	**PHASE 4, POST ACCREDITATION** Contains activities required to continue to operate and manage the system so that it will maintain an acceptable level of risk. Post accreditation activities include ongoing maintenance of the SSAA, system operations, security operations, configuration management, and compliance validation. Phase 4 begins after the system has been integrated into the operational computing environment and accredited. Phase 4 continues until the IS is removed from service, a major change is planned for the system, or a periodic compliance validation is required.

TASK 8: CONFIGURATION MANAGEMENT AND CONTROL	The objective of the configuration management and control task is to: (i) document the proposed or actual changes to the information system; and (ii) determine the impact of proposed or actual changes on the security of the system. An information system will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the system environment. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.	*System and Security Operation Activity*. The system operation activity include the secure operations of the IS and the associated computing environment. System maintenance tasks ensure that the IS continues to operate within the stated parameters of the accreditation. 1. SSAA Maintenance 2. Physical, Personnel, and Management Control Review 3. TEMPEST Evaluation 4. COMSEC Compliance Evaluation 5. Contingency Plan Maintenance 6. Configuration Management 7. System Security Management 8. Risk Management Review
DOCUMENTATION OF INFORMATION SYSTEM CHANGES SUBTASK 8.1	Using established agency configuration management and control procedures, document proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment).	*Compliance Validation*. Periodic review of the operational system andits computing environment must occur at predefined intervals, as defined in the SSAA The purpose of this activity is to ensure the system continues to comply with the security requirements, current threat assessment, and concept of operations. 1. Site and Physical Security Validation 2. Security Procedures Validation 3. System Changes and Related Impact Validation 4. System Architecture and System Interfaces Validation 5. Management Procedures Validation 6. Risk Decisions Validation
SECURITY IMPACT ANALYSIS SUBTASK 8.2	Analyze the proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment) to determine the security impact of such changes.	Task 4-1, SSAA Maintenance. The objective of this task is to update the SSAA whenever necessary to ensure it reflects the current operating system mission, environment and architecture.
TASK 9: SECURITY CONTROL MONITORING	The objective of the security control monitoring task is to: (i) select an appropriate set of security controls in the information system to be monitored; and (ii) assess the designated controls using methods and procedures selected by the information system owner. The continuous monitoring of security controls helps to identify potential security-related problems in the information system that are not identified during the security impact analysis conducted as part of the configuration management and control process.	Task 4-2, Physical, Personnel, and Management Control Review. The objective of this task is to evaluate the deployment environment of a previously accredited system to ensure compliance with the SSAA.

SECURITY CONTROL SELECTION SUBTASK 9.1	Select the security controls in the information system to be monitored on a continuous basis. The objective of this task is to validate that appropriate COMSEC approval has been granted and continues to support the requirements and agreements in the SSAA.	Task 4-3, TEMPEST Evaluation. The objective of this task is to validate that the equipment and site continue to meet TEMPEST and RED-BLACK requirements, as appropriate. Task 4-4, COMSEC Compliance Evaluation.
SELECTED SECURITY CONTROL ASSESSMENT SUBTASK 9.2	Assess an agreed-upon set of security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	Task 4-5, Contingency Plan Maintenance. Periodically review the contingency plan and related procedures to ensure they remain current. This plan should cover emergency response, back-up operations, and post-disaster recovery. The plan should consider natural disasters, enemy actions, or malicious attacks.
TASK 10: STATUS REPORTING AND DOCUMENTATION	The objective of the status reporting and documentation task is to: (i) update the system security plan to reflect the proposed or actual changes to the information system; (ii) update the plan of action and milestones based on the activities carried out during the continuous monitoring phase; and (iii) report the security status of the information system to the authorizing official and senior agency information security officer. The information in the security status report should be used to determine the need for reaccreditation and to satisfy FISMA reporting requirements.	Task 4-6, Configuration Management. The objective of this task is to continually assess proposed changes to the system to determine if they will impact the security posture of the accredited system.
SYSTEM SECURITY PLAN UPDATE SUBTASK 10.1	Update the system security plan based on the documented changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.	Task 4-7, Risk Management Review. The objective of this task is to assess the overall system security design, architecture, and other SSAA requirements against the concept of operations, operational environment, and threats to ensure that risk to confidentiality, integrity, availability, or accountability of the information and system remains acceptable. Known threats, as well as any new threats, must be analyzed to determine if the system still adequately protects against all them.
PLAN OF ACTION AND MILESTONES UPDATE SUBTASK 10.2	Update the plan of action and milestones based on the documented changes to the information system and the results of the continuous monitoring process.	Task 4-8, Compliance Validation. The objective of the task is to ensure that the IS complies with the requirements, current threat assessment, and concept of operations.

STATUS REPORTING SUBTASK 10.3	Report the security status of the information system to the authorizing official and senior agency information security officer.	

CONCLUSION

DITSCAP is the DOD process for C&A, and while it doesn't explicitly follow the SP 800-37, the majority of the tasks follow NIST guidance. With some revisions and updates DITSCAP has a working process that is ahead of some other agencies struggling to prepare a C&A program. Both SP 800-37 and DITSCAP can be tailored based on the level of the IS. This is an important element of emphasizing a cost effective approach.

It is important for agencies to understand the driving forces behind the creation of SP 800-37. FISMA is the main driving force for creating SP 800-37. FISMA requires agencies to perform an independent evaluation of the information security program to determine the effectiveness of the program. OMB A-130 requires agencies to follow NIST C&A guidance. By emphasizing reuse and utilizing security tests and techniques that will be incorporated in the SP 800-53A, NIST SP 800-37 is a good starting point for implementing a C&A process.

LIST OF REFERENCES

"CCA Overview, IT & NSS Defined." Oct 27, 2004. Acquisition Community Connection. Jan 10, 2005 <http://acc.dau.mil/simplify/ev.php?ID=22270_201&ID2=DO_TOPIC>

"Defense Acquisition Guidebook." Oct 24, 2004. Defense Acquisition University. Nov 14, 2004 <http://akss.dau.mil/dag/>

Department of Defense. "DoD Directive 5000.1 The Defense Acquisition System." May 12, 2003. Jan 10, 2005 <http://www.dtic.mil/whs/directives/corres/html/50001.htm>

Department of Defense. "DoD Instruction 5000.2, Operation of the Defense Acquisition System." May 5 2003. Jan 10, 2005 <http://www.dtic.mil/whs/directives/corres/html/50002.htm>

Department of Defense " DoD Instruction 5200.40 DoD Information Technology Security Certification and Accreditation Process (DITSCAP)". December 30, 1997. Jan 10, 2005 < http://www.dtic.mil/whs/directives/corres/html/520040.htm>

Department of Defense. "DoD Directive 8500.1, Information Assurance (IA)." Oct 24, 2002. Jan 10, 2005 http://www.dtic.mil/whs/directives/corres/html/85001.htm

Department of Defense. "DoD Instruction 8500.2, Information Assurance (IA) Implementation." 02/06/2003. Jan 10, 2005 <http://www.dtic.mil/whs/directives/corres/html/85002.htm>

Department of Defense "DoD 8510.1-M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual." July 2000. Jan 10, 2005 <http://www.dtic.mil/whs/directives/corres/html/85101m.htm>

The E-Government Act. Public Law 107-347. Dec 2002.

Federal Information Security Management Act of 2002 Title III of the E-Government Act Public Law 107-347. December 2002.

Moteff, John. "Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives" April 16, 2004. Congressional Research Service. Jan 10, 2005 < http://www.fas.org/irp/crs/RL32357.pdf>

NIST Special Pub 800-37. "National Institute Standard and Technology (NIST), Guide for the Security Certification and Accreditation of Federal Information Systems". May 24, 2004. Jan 10, 2005 <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>

"NIST Background." Aug 2, 2004 FISMA Implementation Project Protecting the Nation's Critical Information Infrastructure. Jan 10.2004 <http://csrc.nist.gov/sec-cert/ca-background.html>

"NIST General Information." Aug 2, 2004. National Institute of Standards and Technology. Jan 10, 2004 <http://www.nist.gov/public_affairs/general2.htm>

NetSec. "Principles and Challenges of the Federal Information Security Management Act." Aug, 2003. NetSec Security Brief Archive. Jan 10, 2004 <http://www1.netsec.net/content/securitybrief/archive/2003-08_FISMA_Principles_Challenges.pdf>

NSTISSI No. 1000. "National Information Assurance Certification and Accreditation Process". April 2000 (Unclassified).Nstissc.gov. Nov 20, 2004 <http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf>

Ross, Ron. "Guide for the Security Certification and Accreditation of Federal Information Systems An Introductory Tutorial." Version1.3 October 28, 2004. FISMA Implementation Project Protecting the Nation's Critical Information Infrastructure. Jan 10, 2005 <http://csrc.nist.gov/sec-cert/PPT/fiac-2004-ca-tutorial-ross.ppt>

symantic. "Understanding and Complying With FISMA." 2003. ses.symantic.com Jan 10, 2005 <http://ses.symantec.com/pdf/FISMA_wp_Feb04.pdf>

United States Government. Office of Management and Budget. "Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources." November 2000. Jan 10, 2005 <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>

Frank, Diane. "OMB finalizes central guidance for IT planning." Dec 11, 2000. FCW.com. Jan 10, 2004 <http://www.fcw.com/fcw/articles/2000/1211/pol-a130-12-11-00.asp>

"What is electronic and information technology?" National Center on Accessible Information Technology in Education Article ID: 106. Jan 10 2005 <http://www.washington.edu/accessit/articles?106>