

Certification and Accreditation: Navigating the Jungle

By Karen Olk, MCP, CCNT
kolk@icscorp.com

Our world is quickly developing into a complex array of highly interactive environments made up of powerful systems and devices that interconnect by means of global networks. The complexity of today's information and communication systems presents a great security challenge for both producers and consumers of information technology. Technological advances of the last decade have fueled threats that necessitate drastic changes in the way we think about protecting our communications systems. With little skill or sophistication required, powerful attacks can be initiated via tools that are now available to the Internet-ready masses. It's a jungle out there!

Since Federal agencies routinely interact with industry, private citizens, state and local governments, as well as the foreign governments, a means of ensuring confidence in the security of each system is crucial. As mandated by the king of the proverbial jungle, the Office of Management and Budget (OMB), all agencies must implement and maintain a program to assure that adequate security is provided. This mandate applies for all agency information collected, processed, transmitted, stored, or distributed by general support systems as well as by major applications. Security controls must be in place to systemize the managerial, operational, and technical safeguards for all information systems that adequately protect the confidentiality, integrity, and availability of the system's information. "Adequate security" is defined by OMB A-130 as security in proportion to the risk and magnitude of the potential harm resulting from the loss, misuse, unauthorized access to, or modification of information.

Beyond operational effectiveness, "adequate security" assures that systems and applications provide appropriate confidentiality, integrity, and availability of a system and its resources. OMB A-130 appendix III details the requirements for the System Security Plan (SSP) and specifies individual responsibilities for planning system security controls. A SSP is a fundamental ingredient of obtaining system Certification and Accreditation (C&A).

C&A ensures confidence in the security of each system while protecting information systems and working within constrained budgets. C&A brings standards to system security controls, as well as verification procedures that regularly assess the effectiveness of these controls.

To achieve certification, a system must undergo a comprehensive evaluation of its' security features. Certification establishes the extent to which a particular system's design and implementation satisfies security requirements. Vulnerabilities are analyzed and risks are documented as security threats. Accreditation assures that the identified security risks are accepted, mitigated, or transferred. A system is accredited and approved to operate once the Designated Approving Authority (DAA) accepts responsibility via formal declaration.

Currently, each government agency required to seek C&A of their systems does so via different sets of procedures. With no designated C&A standard, and each agency swinging on their own vine, there are sure to

be security inadequacies and inconsistencies. The most popular of C&A procedures are those determined by and/or derived from the Department of Defense (DoD) or National Institute of Standards and Technology (NIST) guidelines. Providing a clear rendition the oftentimes indecipherable jabbering of procedural monkeys, the following comparison of formats may assist in making a sensible selection based on individual agency requirements.

Under the direction of the Office of Assistant Secretary of Defense, the Defense Information Systems Agency (DISA) Center for Information Security Systems (CISS) was charged with the task of formulating a standard DoD process of protective measures for classified and other national defense related computer systems. The resulting process, the Defense Information Technology Certification and Accreditation Process (DITSCAP), is a DoD instruction that defines the policies, responsibilities, and procedures for establishing information systems in a way that emphasizes the secure management of a system throughout its lifetime.

The DITSCAP process was designed to be applicable to all DoD (classified, secret) systems requiring C&A throughout their life cycle, but is also adaptable to any type of system, environment, or mission. Each DITSCAP C&A effort must complete four phases, beginning with Definition and concluding with Post-Accreditation. Each phase is composed of activities that are in turn composed of tasks. Within the certification analysis, tasks are composed of one or more steps, as determined by the level of certification analysis required. While each of the four DITSCAP C&A phases is mandatory, implementation of the activities therein may be tailored and, if applicable, integrated with other acquisition activities and/or documentation. Security levels, ranging from Security Classification Level (SCL)-1 to SCL-4, are assigned to each system. Tasks and activities determining accreditation are based on the assigned security level, with each strata of the jungle requiring more security testing than its predecessor, and level four requiring the most rigorous testing.

A wide variety of life subsists in the four different layers, or strata, of a jungle, and each layer plays an integral part in maintaining the equilibrium of the environment as a whole. The living conditions vary in each layer. The jungle begins at the forest floor, and moves up through the understory and canopy layers. Hundreds of feet above the forest floor, the emergent layer tops off the jungle.

The floor of the forest is teeming with animal life, especially insects and arachnids (like tarantulas). The largest animals in the jungle generally live here, including gorillas, anteaters, wild boars, and people.

The understory is a dark, cool environment that is under the leaves but over the ground. Most of the understory receives so little light that plant growth is limited. There are some short, leafy, mostly non-flowering shrubs, small trees, ferns, and vines that have adapted to filtered light and poor soil. Animals in the understory include insects, snakes, lizards, and

small mammals that live on and in tree bark. Some birds live and nest within tree recesses and eat the abundant insects. Some larger animals, like jaguars, spend a lot of time on branches in the understory, surveying the area, looking for prey.

The canopy is the name given to the upper parts of the trees. This leafy environment is full of life: insects, arachnids, many birds, mammals, and reptiles. Plants in the canopy include thick, snake-like vines and epiphytes ("air plants") like mosses, lichens, and orchids.

The emergents consist of the tops of the tallest trees, which are much higher than the average canopy. This layer houses many birds, insects, and more.

Much like the jungle strata, DITSCAP and NIST procedures are made up of four integral layers. These interdependent "Phases", as they are called, act as guidelines to satisfy the C&A and security needs of information systems.

DITSCAP Phase 1, Definition, includes documentation of the system mission, environment and architecture. Threats to the system are identified in this phase, as are the certification authority (CA) and the DAA. Phase 2, Verification, can begin only after a documented agreement between the program manager, the DAA, the CA, and a system representative has been established.

The Verification phase serves to confirm compliance of the system with the agreed security requirements. A corresponding set of security actions verifies that the security requirements and evaluated vulnerabilities have been addressed.

Phase 3, Validation, evaluates the system when fully integrated. This phase recognizes levels of acceptable residual risk in a specified environment and, if successful, culminates in an approval to operate.

The final phase, Post-Accreditation, acts as an umbrella over all preceding phases. Much like the emergent strata of the jungle, the Post-Accreditation phase ensures the established environment remains secure. Post-Accreditation includes monitoring system management and operation, ensuring that an acceptable level of risk is maintained and the approved information system, as well as system components, continue to operate in the established accredited environment. Security and change management, as well as periodic compliance validation reviews, are conducted as the system grows or incurs other major changes.

In April 2000, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) introduced the National Information Assurance Certification and Accreditation Process (NIACAP) to establish a standard national process and a management structure to maintain, certify, and accredit non-DoD systems. Much like DITSCAP, the key to NIACAP is the agreement between the information security program manager, DAA, certification agent, and user representative. These individuals are responsible for resolving critical schedule, budgetary, security, functionality, and performance issues. These NIACAP agreements are formally documented as the System Security Authorization Agreement (SSAA), which is used both as a guide to the C&A and as an evolving yet binding agreement on the level of security required. In essence, the SSAA is the vehicle that guides the implementation of information security requirements and the resulting certification and accreditation actions (after accreditation, the SSAA becomes the accepted baseline security configuration for the system).

The NIACAP is composed of four phases: Definition, Verification, Validation, and Post Accreditation. Much like DITSCAP, Phase 1 Definition focuses on an analysis of the systems' environment and architecture to determine the security requirements and level of effort necessary to achieve certification and accreditation. The objective of this phase is to establish agreement on the security requirements, C&A boundary, schedule, level of effort, and resources required.

Verification, Phase 2, substantiates that changes to the system have not evolved beyond compliance with the information in the SSAA. The objective of Phase 2 is to ensure that the now fully integrated system will be ready for certification testing. Phase 2 activities might include software, hardware, and firmware analysis as well as vulnerability assessments. When the Phase 2 initial certification analysis task is completed, the system should have documented security specifications, comprehensive test procedures, and written assurance that all network security requirements have been implemented.

In Phase 3, Validation, evidence must be produced and presented to the DAA so that an informed decision can be made as to whether or not to grant approval of system operation. At this time, the system may receive either full accreditation or an "Interim Approval to Operate" (IATO). An IATO will be awarded if the system fails to meet the requirements as stated in the SSAA but mission criticality demands the system become (or remain) operational. The IATO is a temporary approval that may be issued for no more than a one-year period.

NIACAP Phase 4, as with DITSCAP Phase 4, is referred to as Post-Accreditation. This phase can begin only after the system has been certified and accredited for operation. Phase 4 includes all activities necessary for maintaining the accredited system in the environment in which it was analyzed. Just as in every jungle, some rain must fall; no information system will ever be completely secure. The object of Phase 4 is to ensure that secure system management and continuing operations are preserved within an acceptable level of residual risk. Residual risk acceptability is determined based upon the relationship of the threat to the system as well as the system's mission, environment, architecture, confidentiality, integrity availability, and accountability objectives.

Regarding scope and intent, NIACAP is virtually identical to DITSCAP, but appeals to a broader audience of agencies. Where DITSCAP often deals with information classified as secret and is thereby more demanding from a security robustness perspective, security analysts often perceive NIACAP as a "DITSCAP light".

NIST is also an important technical contributor to the nation's standards infrastructure. NIST, an agency of the U.S. Commerce Department's Technology Administration, is responsible for developing accurate ways to measure length, time, mass, temperature, and the other physical quantities fundamental to all aspects of technology. Standards in measurement are integral to both product and process, and NIST documentation specifies standards involving everything from the diameter of optical fibers to the content of C&A proceedings.

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce is to approve standards and guidelines that are developed by NIST for Federal systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. The FIPS series of NIST standards is the official series of publications relating to standards and guidelines adopted under the provisions of the Federal Information Security Management Act (FISMA) of 2002.

NIST develops FIPS when there are compelling Federal government requirements for security and interoperability and there are no acceptable industry standards or solutions. Advanced Encryption Standard (AES), for example, is a new FIPS publication that specifies a cryptographic algorithm for use by the US government to protect sensitive but unclassified information. NIST predicts that the standard also will be widely used by organizations outside of the Federal government.

Marianne Swanson, co-author of the NIST SP 800-37, suggests that many agencies outside of DoD feel that the DITSCAP/NIACAP approach to

the C&A process borders on overkill. Civilian agencies dealing with unclassified or sensitive information are more likely to use the NIST process and take advantage of its adaptability. Since NIST encourages the SSP to be established in OMB approved format, change processes can often be streamlined.

Title III of the E-Government act of 2002 (public Law 107-347) assigned NIST to develop standards and guidelines to provide categorization of each information system of all Federal agencies. NIST SP800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, is a recent release that delineates NIST C&A guidelines.

Another major difference between the DITSCAP and NIST C&A process is the designation of levels. Where DITSCAP assigns security levels to each system, which in turn determine the severity of the security testing it will endure, NIST SP800-37 treats all systems equally as far as security testing is concerned. It defines a standardized set of security controls and prioritizes systems based on the potential impact of its loss.

According to Ron Ross, co-author of the NIST SP 800-37, NIST has fashioned four key documents that comprise a comprehensive map of the C&A jungle; NIST SP 800-37, SP 800-53, SP 800-60, and FIPS 199.

FIPS 199 addressed the first task cited by the *E-Government act of 2002* by developing a new standard for categorizing information and information systems that provides a common foundation for system security while promoting effective management of information for the Federal government. To help keep agencies from getting caught in the daunting forest floor quicksand of C&A documentation, FIPS 199 also encourages consistent reporting to the Office of Management and Budget (OMB) and Congress on the operational feasibility, adequacy, and effectiveness of information security policies, procedures, and practices. FIPS 199 categorizes information systems according to the potential impact of their loss and the net effect on the mission/jungle if a system were to be rendered unavailable; systems are categorized as either "low", "moderate", or "high" impact. Additionally, NIST SP 800-60 standardizes details specifying categorical placement and has recently been released in draft form.

Much like DITSCAP and NIACAP, the C&A process according to SP800-37 is comprised of four distinct phases. The NIST phases include Initiation, Security Certification, Security Accreditation, and Continuous Monitoring. Each phase consists of well-defined tasks to be carried out by the authorizing official, their designated representative, the system owner, the system security officer, the certification agent, and the user representative. Each task has associated subtasks and milestones that must be satisfied before moving on to subsequent phases.

Acting as the forest floor, the Initiation Phase of the development life cycle determines and establishes system requirements. The Initiation Phase consists of three tasks: preparation, notification and resource identification, and SSP analysis, update, and acceptance. The purpose of this phase is to ensure that the authorizing official and senior agency information security officer are in agreement with the contents of the SSP before the assessment of security controls can begin.

During the task of preparation, it is often found that a significant portion of the information needed for the Initiation Phase has been previously generated. For this task, the system owner prepares the initial risk assessment, the development of the SSP, and any previous assessments such as Security Testing and Evaluation (ST&E), and/or independent audits. In most cases, risk assessments and Sap's have been previously reviewed and approved by agency officials, but for new information systems or systems undergoing major upgrades, this information is typically produced during the Initiation Phase of the system.

The object of the second task associated with the Initiation phase, notification and resource identification, is to acquaint all concerned agency officials with the impending C&A process and determine the resources needed to carry out the effort. A plan of execution for the C&A activities is generated and will indicate the proposed schedule as well as important milestones.

The third task of the Initiation phase, SSP review, analysis, and acceptance, requires an independent review of FIPS 199 and the SSP. This task secures the acceptance of the SSP by authorizing official before assessing the existing security controls. The completion of this task concludes the Initiation Phase of the C&A process.

The Security Certification Phase consists of two tasks: security control assessment and 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, producing the desired result, and meeting the security requirements of the system. Also addressed during this phase are any known vulnerabilities and any specific actions taken, or planned to be taken, to correct deficiencies in the security controls. Upon successful completion of this phase, the authorizing official will have the information necessary to determine the risk to agency operations, assets, and individuals to render an appropriate accreditation decision.

The purpose of the third phase, Security Accreditation, is to ensure that the risk to agency operations, assets, and individuals is acceptable to the authorizing official. This phase requires both security accreditation documentation and an accreditation decision. Upon successful completion of this phase, the system owner will have either full authorization to operate the system, an interim approval to operate under specific terms and conditions, or be denied authorization to operate.

The Continuous Monitoring Phase is the final phase of the NIST C&A process. There are three tasks associated with this Phase, including configuration management and control, security control monitoring, and 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. Since the security of the system may be impacted, the authorizing official must be notified when changes to the system take place. Re-accreditation may be required due to specific changes to the system or because of federal or agency policies requiring periodic reauthorization.

To help further dispel the current jungle attitude of "connect first... ask questions later", the NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Certification Levels*, will designate each set of security controls with a low, moderate, or high, rating to provide threat coverage.

The jungle is ruled by survival of the fittest, and according to NIST, building a fit system requires:

Well-defined system-level security requirements and security specifications

- ▲ Well designed component products
- ▲ Sound systems security engineering practices
- ▲ Competent system security engineers
- ▲ Appropriate metrics for products/system testing, evaluation, and assessment
- ▲ Comprehensive system security planning and life cycle management

The NIST C&A process, designed with civilian agencies in mind, is based on the internationally accepted Common Criteria security standards. This international standard (ISO/IEC Standard 15408) details an approach

for evaluating security features and establishes a common language for communicating security requirements in IT products and systems. NIST and the National Security Agency (NSA) encourage the use of Common Criteria standards within civilian agencies for procuring and developing secure products. In furtherance of its responsibilities under FISMA, NIST continues to develop FIPS and other special publications; each striving to address the gap between the existing state of a system and a guaranteed secure network.


The purpose of NIST SP 800-53 is to provide guidelines for selecting and specifying security controls for information systems. SP 800-53 has been broadly developed from a technical perspective to compliment similar guidelines issued by agencies and offices operating or exercising control over Federal information systems, other than those systems designated as national security systems. The variable section of security control is clearly identified here by the keywords "assignment" or "selection" which indicate the type of operation permitted. Thereby, the comprehensive approach to security represented in SP 800-53 facilitates a more consistent and repeatable approach to selecting security controls for information systems than does the DITSCAP process.

NIST SP 800-53 also provides a foundation for development of techniques to verify security control effectiveness. Promoted here is an extensive and dynamic catalog of possible controls that adhere to the three sets of baseline controls defined for security categories in FIPS 199. Assurance is based on quality of security control design and three levels of security robustness; basic, enhanced, and strong.

Much like the clean water the exotic jungle firefly Okinawa sujibotaru depends on for survival, security standards must be plentiful, precise, and nontoxic in order to remain effective. Where DITSCAP often deals with systems and information classified as secret, the NIST process satisfies the security needs of sensitive and/or unclassified information systems.

ICS Director of Security, Edwin Covert, who has over eleven years of experience in the information security and information arenas, describes the DITSCAP C&A process as "rigid", and NIACAP as "flexible". He adds that NIACAP testing tends to be subjective, due to the availability of many implementations of its' testing. However, since the NIACAP and NIST formats are relatively new, they have not undergone the years of real world testing endured by the DITSCAP process.

Ron Ross maintains that, "it is imperative that both ends of a communication adhere to the same security guidelines. Certification and Accreditation means nothing if it does not provide assurance of due diligence."

It's a jungle out there, but both NIST and DITSCAP are doing their part to help chart a clear path all the way through. 

Karen Olk is an Information Security Specialist with Integrated Communication Solutions (ICS), of Frederick, Maryland, who is responsible for governing Certification and Accreditations of diverse Federal systems. She is a CompTIA Certified Network Technician and Microsoft Certified Professional who has personally participated in the completion of dozens of C&A's. Karen has a substantial information security background and has worked with an array of information technologies including Voice Over IP, network monitoring, web design, and intrusion detection and management. She can be reached at kolk@icscorp.com.