

## **WHITE PAPER**

*PRESENTED BY :*



### **CERTIFICATION AND ACCREDITATION:**

**HOW CERTIFICATION AND ACCREDITATION CONTRIBUTES TO THE  
SECURITY AND FUNCTIONALITY OF AN INFORMATION TECHNOLOGY  
SYSTEM**

James D. Heimberg, ABC, Ph.D., ISSO

July 30, 2007

## INTRODUCTION

Leverage's Information Security (INFOSEC) Services practice is pleased to present this white paper that describes how Certification and Accreditation (C&A), and its predecessor in determining the ability to operate a system, Security Test and Evaluation (ST&E), function as a process that contributes to the security and overall functionality of an Information Technology (IT) system whether it is a Major Application (MA) or a General Support System (GSS). The requirements for certifying and accrediting Government IT systems come directly from the Information Technology Management Reform Act (ITMRA), also known as the Klinger-Cohen Act of 1996. ST&E has been around for much longer and is as applicable to commercial systems as it is to Government systems.

The original requirements for certifying and accrediting systems resulted from two issues.

- The first issue, which is more commonly known, is describing a system in detail as part of the lifecycle development process, which allows for decision making about the system so that future changes can be determined through a rational, well-thought-out process. As such, C&A may be considered the natural outcome of performing ST&E, a documented record of the system and what was tested and evaluated.
- The second, which is less frequently envisioned, is that the process for certifying and accrediting a system tends to describe, in a straightforward manner, the infrastructure including strengths and weaknesses of the system when the effort is undertaken, a knowledgeable snapshot of a complex system. It is this second issue that becomes the main topic of this white paper.

Many organizations have determined that the process is one of ensuring that certain descriptions of the system are created and thus, that a shortcut method can be implemented to ensure that the 'checkmark boxes' (also known as compliance issues) have been checked. This is somewhat of a shortsighted approach that misses the second reason for performing the C&A effort. The key tool to ensure that the process is being followed correctly is the System Security Plan (SSP), the documentation about the system used throughout the Federal government. There are other names for this document (i.e., also known as the System Security Authorization Agreement [SSAA] when prepared under the former Department of Defense (DoD) Information Technology Certification and Accreditation Program [DITSCAP], now the DoD Information Assurance Certification and Accreditation Process [DIACAP]).

According to the National Institute for Standards and Technology (NIST) in Special Publication (SP) 800-18, the Guide for Developing System Security Plans for Information Technology Systems, "The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect (*at a minimum*) input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager." That document goes on to say that the purpose of preparing SSPs is to provide an overview of the security

requirements of the system, to describe the controls in place or planned for meeting those requirements, and to delineate responsibilities and expected behavior of all individuals who access the system.

The National Information Assurance Certification and Accreditation Process (NIACAP) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000 document describes the reason for C&A as the process designed to "...certify that the information system (IS) meets documented security requirements and will continue to maintain the accredited security posture throughout the system lifecycle. The process should be adapted to include existing system certifications and evaluations of products. Users of the process must align the process with their program strategies and integrate the activities into their enterprise system life cycle."

Therefore, there is significant importance for completing the process so that the security state of the system is fully identified and improved (the key) as a result of having completed the process. Describing how that works is the intent of this white paper.

The INFOSEC Services practice prepared this white paper to describe how it can develop and deliver a complete IT security system using certified security professionals, infrastructure consulting and development services that are among the best in the industry, and a full array of IT products that support infrastructure buildup.

## **Certification and Accreditation Methodology**

There are a number of methodologies used to complete the C&A process to the highest level. In order of most restrictive to least restrictive, the major evaluation systems are:

- Director, Central Intelligence Directive (DCID) 6/3, which is used for national security IT systems.
- DIACAP, which is used for DoD when DCID 6/3 is not invoked.
- NIST SP 800-37, which is used for Government systems that are not covered above.

There are other systems as well, but for the most part, they are special purpose resulting from those listed above. (For example, the intelligence community, which consists of units of DoD and other agencies, uses a system that falls between DCID 6/3 and DIACAP. The Department of Homeland Security [DHS] determined the need to create their own, a system that is more comprehensive than the NIST method, but less restrictive than DIASCAP.) In addition, the requirement to certify and accredit systems is expected to be levied in some form on contractors of Federal programs as well as state and local governments during 2008 and 2009. This is likely to use the NIST methodology for the most part and DIACAP for those contractors responsive to DoD and for the various elements of state National Guard agencies. Additionally, law enforcement may fall under the DHS system.

The similarities between the systems are vast, in that the information needed is relatively the same, a constant that varies depending on the depth of information required. Regardless, there is information of types that is required independent of the depth.

Purpose is another consideration. The NIST document is the most comprehensive in its description of the types of systems to be certified and accredited. It divides IT systems into two groups: MAs and GSSs.

- An MA is an application or group of applications that function in a similar manner, supporting common mission objectives, sharing common data, using similar programming languages and/or architecture, and requiring the same level of security management. Also, an MA includes an application or group of applications that require special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information under the application's direct control.
- On the other hand, a GSS is a combination of applications, hardware, network resources, procedures, and staff that provides common functionality and services to multiple MAs. The GSS components typically fall under the same direct management control and share common functionality. As an example, a Local Area Network (LAN) would be considered a GSS and all of the applications that are part of the productivity suite for that LAN would be part of the GSS along with the policies and procedures that control it and the people associated with it.

Before addressing the systems more specifically, it is critical to understand how the information is used to protect the organization that gathers the information. There are two critical facets to discuss. The first is the data and the second is the authority. Discussions of data can be divided into two groups.

The first group is "data at rest". Data at rest pertains to the status of data that is stored on media of all types with availability for use throughout the confines of the IT system or to other connected systems. Data at rest describes the datastore of an MA or of network-stored data whether the datastore is in a database available for users or applications or in the form of a Storage Area Network (SAN). Data at rest must share properties for it to be available to every user or application that needs to gain access and use the data to process it into meaningful information.

The second group is "data in transit". Data in transit describes how data is handled when it is being moved throughout the system or shared with other systems. This is critical for the protection of the data itself as being in transit always exposes data to greater vulnerabilities. Common sense should result in an understanding that if data is encrypted both at rest and in transit, as might be the case with sensitive data of any type (e.g., national security data, proprietary data, health information data [as protected under the Health Insurance Portability and Accountability Act of 1996 <HIPAA>], financial information [as protected under the Sarbanes-Oxley Act of 2002 <SARBOX>], classified information, etc.), the encryption schemes must be compatible or the data will not be available either by storage location or usability. Tuning

encryption schemes is a complex task and encryption will use overhead from system processing ability.

Authority describes features of the users rather than the data. When addressing authority, consider that authority can be in the form of access (i.e., need-to-know access) or use of data and the implied result of directing actions as a result of using data. For instance in an organization, various levels of management may have differing procurement authority (amounts that can be approved for payment and that make the corporation liable for the actions of the individual expressing the authority). The same applies to controlling or directing the actions of members of the organization whether in a commercial entity or in the form of command and control in a military or paramilitary organization. In that regard, authority can have a significant impact on organizations and people even resulting in life-and-death decisions.

The major sections of any C&A document must include:

- System description
- Key personnel description with contact information
- Description of data being protected
- Description of authorities (both role based and rule based) as used throughout the system
- Description of vulnerabilities
- Assessment of system risk
- Description of protection mechanisms and ST&E used to validate the condition
- Agreement between the system owners, Information Assurance (IA) personnel, and users of the truth of what is contained in the document
- Certification by a vested authority with the right and duty to oversee the system from a management perspective
- Designation of accreditation by a Designated Approval Authority (DAA) under the sole authority of the organization's Chief Information Officer (CIO) in the form of an authority to operate or interim authority to operate

A discussion of each follows.

### ***System Description***

A description of a system starts with a description of ownership of the system and the system's purpose. It then flows to a description of the components that make up the system. Omission of any of the parts will result in an incomplete level of test and evaluation allowing vulnerabilities to be induced as a result. The order of the information provided may vary between C&A systems; however, the need for complete information does not change.

### ***Key Personnel Description***

A description of key personnel provides for initial input about who to contact when problems or questions arise. All of the information contained in the certifying and accrediting documents should be contained in the contingency planning and disaster recovery documentation as well.

It is crucial to include as key personnel those with ownership, control, and administrative authority in addition to those responsible for security evaluation of the system.

### ***Description of data being protected***

For reasons of sensitivity, a description of the data being protected may not be required in any more than general terms, but the protection levels for the various types of data being protected need to be described to the fullest. This description will be used not only to certify how the system handles data, but also to determine the relative risk of loss of data or inability to access data during any event other than normal operations. The Government has devised a number of schemes to describe data protection levels. The system used will depend on the C&A methodology being used. Any inability to fully describe data or the data protection levels needed could result in inherent risks within the system and may result in any subsequent C&A effort being invalidated at the final stages.

### ***Description of Authority Levels***

If the point has not been stressed to the clearest, this is a critical, often overlooked facet of C&A. In most systems, the authority is actually more important than the value of the data. For example, the ability to commit resources is more critical than the loss of part of the data being stored or transmitted. A program manager may be dealing with a program valued at \$5 Million annually, but the ability to direct the work effort of the program staff has greater value as it can be used in other places if not used properly and draws from organizational resources rather than just programmatic resources. As another example, a robbery in progress of a liquor store may only have a real value in the hundreds of dollars, but the police response to protect the store owner and employees may cost the city far more than the hundreds of dollars that might be lost and puts everyone at the scene or responding to the alarm into life-threatening experiences. This is an example of when the authority to dispatch personnel in an emergency has greater value than the data and information that is a component of the system used. There is no clear system for describing authority levels that compares them or values them with regard to system operation and the level of protection needed.

### ***Description of Vulnerabilities***

Every Federally owned system is mandated by law to have vulnerability analyses completed at regular intervals with some interval set for third-party testing. Most often, the evaluation must be provided in quarterly reports to a higher-level authority for inclusion in the overall management evaluation of the organization. This is the case when vulnerability test results are reported under the Federal Information System Management Act (FISMA). In the C&A documents, the vulnerabilities should be fully described in a manner that allows translation to the FISMA required reports, such as the Plan of Action and Milestones (POA&M). Thus, vulnerability test and management become key components in building C&A documentation. This is part of the link between C&A documents and ST&E.

## ***Assessment of System Risk***

Once the information about the system, data protection, and vulnerabilities is brought together, an evaluation of risk can be accomplished. Although software systems were used in the past, risk analysis now is performed based on use of mathematical equations that are focused at the confidentiality, integrity, and availability of the system. One of the common faults in performing C&A is to use a system that is subjective to identify inherent risks at the front end of the 'objective' equations and risk assessment process. While it is commonplace to have those most intimately involved with IT systems identify the risks, there are evaluation methods that can be used to compare and rank risks in a manner that makes the risk analysis more objective.

## ***Description of Protection Mechanisms***

To balance out the identified risks and vulnerabilities, C&A documents must contain a measure of the protection mechanisms used to evaluate threats to data and authority. Such tools include antivirus programs, firewalls, intrusion protection systems, password strengths, biometrics, access control lists, and both automated and personnel-directed policies and procedures. Each should be defined not only by the marketing materials of the vendors who provide the tools, but by the sensitivity levels of the tools as well as the expertise of the personnel using the tools in order to understand fully what the hoped-for outcome will be with regard to the system.

## ***Agreement of What is Contained in the Document***

Many documents of various types that address C&A define those responsible for operating the process as a combination of the system owner, a member of the IA or INFOSEC organization assigned to the system, and a liaison representative acting on behalf of the users. The intent is to balance the results between the audiences that have an interest in the protection of the system. This also allows for a complete path that can identify any change to the system during its lifecycle that might result in an update of the C&A documents or reevaluation of any of the analyses (vulnerability or risk) that were performed.

## ***Certification***

Certification is management's acceptance of the results of the C&A efforts and documents as truthfully representing the state of the system being evaluated. It should be performed by a Certifying Official, who was appointed in writing and who understands the ramifications of C&A. The Certifying Official should be a member of the management team above the system owner and may or may not be under the direct control of the CIO. Regardless of the organizational chain of command, the Certifying Official must have significant background in the understanding of the inner workings of IT systems generally and the one for which they have been appointed specifically. Not having the proper background induces vulnerabilities associated with how valid the certification has been performed.

## **Accreditation**

Accreditation is the process of accepting the certification and determining and documenting that the system can be operated safely and securely. Typically, C&A of a system results in an Authority to Operate (ATO) that is valid for a period of three years; however, that timeframe may be shortened or lengthened at the discretion of the CIO. Under no circumstances, should the period be lengthened beyond five years for a single ATO and more secure systems may be limited to three years maximum. The ATO is unique in that the authority vested to accredit systems has been determined to be a direct responsibility of the CIO responsible for the system in question by the Federal CIO Council. They have expressed opinions that the CIO may be personally liable for any damage that results from unsafe operation. This is the reason that it is in the best interests of a CIO to not vest the authority in anyone else without ascertaining the knowledge level of that person and the trustworthiness of them in acting on the CIO's behalf. If there is a problem, the CIO will be held responsible, not the person assigned to complete the accreditation process!

There are two temporary conditions that may be used during the C&A process. The first is used when determining the certifiability and accreditability of a system that requires testing on the live network and is referred to as an Interim Authority to Test (IATT). An IATT should not be granted for a period longer than 90 days and may be granted for much shorter periods. The second occurs when preliminary information gathered for the final ATO is withheld based on work that must be performed before the final or when there is testing that has not been completed. This is referred to as an Interim ATO (IATO) and should not be granted for periods of longer than six months.

## **Process Components**

Leverage's INFOSEC Services practice uses its proprietary System Security Plan Evaluation Tool<sup>®</sup> as an integral part of the process of compiling data for security plans as well as for evaluating the end result. The tool uses a series of questions about gathered data. The questions were designed to determine the depth of the answers that need to be provided and to allow grading the results in order to determine that a sufficient level of information is provided. The questions can be sorted based on the C&A process being used in order to properly identify the order and paragraph numbers to which they apply. This is what allows use in generating documents as well as evaluating them.

The overall C&A process followed by INFOSEC Services consists of nine steps, which are defined below.

- *Determining the need to perform C&A* – For new systems, there are various Federal mandates about when C&A is required in the lifecycle of an MA or GSS. In every case, C&A must have been started and have made significant progress before any live network testing that requires issuance of an IATT. The initial C&A process must be completed before the issuance of an IATO with the IATO being issued for a period that allows for fulfillment of any issues determined to require change before a ATO can be issued. The C&A process must be fully complete before the ATO can be issued. For existing

systems, the need for C&A will be driven by cyclical review periods or by any change with significance in the result of the change such that a change to the existing documentation may impact the ability to leave the ATO in place as is.

- *C&A type selection and formatting* – Each part of the Federal government is under the control of various requirements for C&A based on the ITMRA.

The broadest scope and authority comes from the documentation requirements produced by NIST. The NIST guidelines are to be applied where there is not a separate type and format methodology specified due to the special purpose of the MAs and GSSs being used. Under the NIST method, the security plan is formalized as an SSP.

DoD has specified that all parts of DoD use the DIACAP documentation format for C&A based on the type of information being handled. Under DIACAP, the depth of response to much the same questions that are part of the NIST documentation is required to be much deeper. The document required for this type of C&A is the SSAA.

For systems that specifically handle national security information, the Central Intelligence Agency has produced guidance under the directive DCID 6/3. During early 2007, a C&A revitalization program was started with the Director of National Intelligence (DNI) under which that role is responsible for a rewrite of DCID 6/3. Again, the depth of information required is much more comprehensive although the breadth of information is nearly the same as the NIST or DIACAP programs. The document required for this type of C&A is referred to as an SSP.

There are other systems considered to be special-purpose systems. For example, the intelligence community uses the NSTISSI methodology with the depth of information as required by the sensitivity of intelligence data. The C&A document is referred to as an SSAA with slightly different format and order to questions. The Department of Homeland Security has its own format requirements, as do some others; however, in each case, the breadth of information required is nearly the same.

- *Information gathering* – Definition of the information required is based from the ST&E report and on the methodology being used. As the information is gathered, it should be shared with those responsible in the C&A process so that it can be verified and validated. Review of drafts should be completed at every critical stage until the document is finalized.

As a best practice methodology for ST&E, INFOSEC Services recommends use of the NIST Special Publication 800-53A (recently published as the 3<sup>rd</sup> public draft). Use of this methodology will ensure a focus on management, operational, and technical controls that need to be described in the C&A documents.

- *Vulnerability and risk assessment* – Vulnerabilities are assessed through the use of automated tools, some of which provide reporting capabilities based on Federal

requirements. INFOSEC Services can use the tools specified by the customer; however when no tool is specified, we recommend the use of Lockdown Networks products as they are the only tools on the market that provide for direct reporting of vulnerabilities on POA&Ms under FISMA. For risk assessment, INFOSEC Services recommends use of a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis as the process for determining the key threats that are then evaluated under the Federally mandated risk assessment guidelines. A separate white paper has been produced and is available from Leverage via our Webpage (Universal Resource Locator [URL]: [www.leverageis.com](http://www.leverageis.com)) detailing how the SWOT analysis is used in the risk assessment process.

Once assessment has been performed, the gathered data is analyzed and the information is available for the next stage of C&A.

- *Documentation* – At this point in the process, sufficient information has been gathered to allow for compilation in the form of the C&A document required under the appropriate methodology. INFOSEC Services strictly adheres to the format guides that apply and additionally uses the proprietary System Security Plan Evaluation Tool to validate throughout the process that sufficient depth is documented in order to ensure that the C&A process actually assists in system management to a greater extent than the efforts involved in the C&A process.
- *Review and coordination* – When the documentation is brought to a final draft status, the document is shared with all critical partnering organizations as well as impacted organizations. The ultimate goal is to provide a Memorandum of Agreement (MOA) between the system owner, IA, and user representative(s) that the document represents an accurate description of the MA or GSS in its current configuration and operational status.
- *Certification* – When ready, the document is forwarded to the Certifying Official to ensure that sufficient management depth conducts a review of the system and its operation. At this point, the Certifying Official may want to use the Leverage tool to fully evaluate how well the document meets the intent of the process effort and compliance requirements before attaching a letter certifying that the information is accurate and that the system is ready for accreditation.
- *Accreditation* – Once certified, the document can be forwarded to the CIO for accreditation, which includes the issuance of an IATO or ATO that allows the system to work on a live network.
- *Periodic evaluation* – Depending on the nature of the accreditation and the length of the accrediting period as well as the status of the ATO (either interim or full), scheduled reviews are planned. During the period between scheduled reviews, any change that might invoke a change in the vulnerability or risk assessment outcomes or the infrastructure of the MA or GSS should result in a review of the system and security plan documentation.

Leverage's INFOSEC Services practice specializes in providing Information System Security Officers (ISSOs) and Information System Security Engineers (ISSEs) to perform this work and to ensure that related systems (e.g., business workflow processes, configuration management, disaster recovery planning, and training [specifically with regard to annual awareness training]) are integrated seamlessly into strategic planning, architecture, vulnerability and risk management, solutions management, incident response and forensics, and audit and survey management as they apply to INFOSEC.

## **Summary**

The key to a successful IT security program lies in how well systems are documented and evaluated with regard to security issues. Leverage's INFOSEC Services practice provides a holistic approach to INFOSEC in general for all customers and specifically to C&A efforts for Government and Federally mandated programs for ensure IT systems can be operated safely and securely. In addition, INFOSEC Services provides services that offer Return-On-Investment (ROI) features to increase safe, secure operations of IT systems and to provide for better system protection throughout the life cycle of the system.

**For more information, refer to the contact information provided on our Website:**  
[www.leverageis.com](http://www.leverageis.com) and a representative will be happy to provide more information.