2003-04-00

A Program for Education in Certification and Accreditation

Rasmussen, Craig W.

DARPA DISCEX Conference, April 2003

DARPA DISCEX Conference, April 2003

A Program for Education in Certification and Accreditation

Craig Rasmussen, Cynthia E. Irvine, George W. Dinolt, Timothy E. Levin
Naval Postgraduate School, Monterey, California, USA

Abstract: Large complex systems need to be analysed prior to operation so that those depending upon them for the protection of their information have a well defined understanding of the measures that have been taken to achieve security and the residual risk the system owner assumes during its operation. The U.S. military calls this analysis and vetting process *certification and accreditation*. Today there is a large, unsatisfied need for personnel qualified to conduct system certifications. An educational program to address those needs is described.

Key words: Information Assurance, Certification and Accreditation, Graduate Education

1. INTRODUCTION

Computer and network systems process information critical to enterprise security. Should these information systems be vulnerable to security failures or attacks, the consequences could be grave. Although individual components may provide security features and assurance of correct policy enforcement, their encompassing systems and subsystems are frequently large and complex. How can a system owner assess the suitability of a system to operate in a particular environment? Factors that will affect this determination include the sensitivity and criticality of the information to be processed; the physical and cyber context in which the system is expected to operate; the personnel who will administer and use the system; as well as a wide variety of technical factors that affect security.

The process used to assess networks and systems and to then officially authorize their use is known as *accreditation*. As an example, an avionics system might be the subject of an accreditation. In general, accreditation will result in the approval for the system to be operated with defined physical conditions, interconnections, personnel security attributes, and system assurances, in combination with procedural and technical countermeasures to security threats. The accreditation describes the operational objectives of the system, defines the threats to the system and the countermeasures taken to mitigate those threats, and the resulting residual risks. As part of the process it is recognized that a reassessment of system security is required periodically, so the accreditation will have a limited lifetime.

Certification supports the accreditation process by providing analysis of the technical and non-technical aspects of the system. As the system moves through its lifecycle, the certifier works with component designers and integrators to ensure that a specified set of security requirements are met. Certification supports the accreditation process.

System Certification and Accreditation [7] can help to identify and mitigate risk in a wide variety of systems. Consequently, the U.S. Department of Defense (DoD) has stated that all information systems will be certified and accredited to operate at an acceptable level of risk. Given the sheer numbers of systems in operation, from business systems to weapons system, this is a daunting task.

It is clear that a highly skilled cadre of system certifiers is needed, not only to address the current demands of the government but to provide similar support for the complex systems being fielded in the private sector. Yet, there are relatively few analysts with the background, training and education that would qualify to senior leadership for system certifications. To address the gap between requirements and available qualified personnel, we are establishing an educational program for system certifiers.

Herein, we provide a high-level overview of the certification and accreditation process using the U.S. DoD certification and accreditation model as our example. We will then describe the program we are developing to provide certifiers with the education and experience needed to progress from a beginner to an intermediate level.

2. CERTIFICATION AND ACCREDITATION

To ensure that all services perform accreditations to some standard level, the DoD has published an instruction called The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [2]. This instruction process provides a degree of confidence that all accredited systems have undergone an equal and adequate level of analysis and testing. Realistically, however, the outcome of certification and accreditation is dependent on the education and experience of the personnel conducting the exercise. Qualified personnel are in short supply, and the need for individuals to provide technology support for Certification and Accreditation will continue to grow.

The following sections provide a brief summary of the information system certification and accreditation (C&A) process defined in relevant instructions and publications [1, 2, 3, 4, 5, 6]. We have chosen to focus on Navy requirements and our overview is intended to illustrate the complexity of the C&A task, and the fact that the transition from apprentice to journeyman certifier requires training, formal education, and field experience.

2.1 Who is Involved?

There are four principal participants in the C&A process:

Program Manager (PM). According to the DITSCAP, "program manager" might refer to three distinct roles over the life of a system. During system acquisition, the program manager is the individual responsible for system procurement and development. During the operation of the system, the role belongs to the system manager, who is responsible for system operations. When the system undergoes a major change, the role belongs to the maintenance organization's program manager.

Designated Approving Authority (DAA), who is typically the system "owner". It is the DAA who is ultimately in the position of accepting an inevitable compromise between the desire for perfect security, the minimum set of security features required by applicable legal or regulatory constraints, and the needs of the user community to have a functional system that meets its needs. It is the DAA who assumes the risk; only upon accreditation by the DAA does the system become operational and able to run with "live" data.

System Certifier. Either alone or as a member of a team, the system certifier provides a comprehensive evaluation of the security features, limitations, and vulnerabilities of a target information system. It is the certifier's responsibility to document for the DAA the target systems's level of compliance with security requirements and the level of residual risk present in putting the system in operation

User Representative. This individual requires that the system in question achieve a specified level of functionality.

2.2 Functional Components of Certification & Accreditation Process

This section provides an overview the functional components of the Certification and Accreditation process. By appreciating this process, the role and contribution of the System Certifier can be understood in context. Appendix A provides a glossary of terms.

The DITSCAP process is divided into four major phases: Definition, Certification, Validation, and Post-Accreditation. Table 1 provides a synopsis of the steps that must be accomplished during each phase. The DITSCAP process may be iterative and for large, complex systems it is sometimes necessary to conduct several iterations.

Table 1. Functional Components in the Certification and Accreditation Process

Phase	Step	Description
Definition		
	1	Document Mission Need
	2	Conduct Registration
	3	Perform Negotiation
	4	Prepare System Security Authorization Agreement
Certification		
	5	Support System Development
	6	Perform Certification Analysis
Validation		
	7	Certification Evaluation
	8	Develop Recommendation to Designated Approval Authority
Maintenance		
	9	Compliance Validation
	10	Maintenance of System Security Authorization Agreement

2.2.1 Definition

This phase comprises the first four steps discussed in this document: documentation of mission need, registration, negotiation, and preparation of the System Security Authorization Agreement (SSAA) (this step is often incorporated into the negotiation step).

2.2.1.1 Document Mission Need

This preliminary phase occurs whenever development of a new information system or modification of an existing system is initiated. Planning the certification begins with acquiring a thorough understanding of the system to be certified, the functions that the system must fulfill, and the mission served by the system. This planning also requires a comprehensive understanding of the steps required in all C&A processes. The certifier keeps all concerned personnel fully informed even at this early stage in the process. Of particular importance are the following:

- Proposed system mission.
- Proposed system functions.
- Proposed system interfaces.
- Category and classification of information to be processed.
- Anticipated system lifecycle.
- Characteristics of system users.
- Operating environment.

2.2.1.2 System Registration

The registration phase is the beginning of the dialogue among the key players in the C&A process. The steps vary, depending on whether the subject system has been fielded previously or is under development. The first step in the registration phase is a review of the materials from either a new

Document Mission Need phase or from a previous life cycle iteration. The final step in the registration phase is the development of a draft (or draft update) of the System Security Authorization Agreement (SSAA). In either case, the draft SSAA represents an agreement among the Program Manager, the DAA, the CA, and the user representative, and describes the goals that must be achieved in support of certification as well as the strategy by which those goals are to be met. The following list describes key steps in the process.

- Register the system: Inform key participants (DAA, Certifier, User representative) that the C&A process must be undertaken.
- Prepare mission description and system identification. In the case of a new system, this step relies on the documentation developed in the previous step. In the case of a system that has already been in operation, this step relies on the body of documentation, including the existing SSAA, that should accompany the system throughout its life cycle.
- Describe the system environment and threat description. The system environment has both physical and logical components. For example, a locked cage in a guarded room presents a much different picture from the standpoint of vulnerability than does a desktop in a busy office. Similarly, a stand-alone system presents a much more difficult target than, for example, a networked system with an Internet connection.
- Describe the system architecture and C&A boundary. This boundary describes precisely which equipment and systems within the domain of the DAA are to be subjected to the C&A process under development.
- Determine the IT security system class and system security requirements. The precise C&A tasks from the DITSCAP are sensitive to this evaluation, in that they must be performed at one of four certification levels, ranging from Level 1 (basic security review) to Level 4 (comprehensive analysis). Minimum security requirements are mandated by the DoD level, and can be strengthened (but not weakened) by the constituent military services.
- Prepare a DITSCAP plan based on the assembled documentation. Based upon the preceding steps, this step tailors the DITSCAP tasks to the system under consideration. For example, execution details of each of the DITSCAP tasks are dependent upon the IT security class determined in the previous step.
- Identify organizations and additional resources required for the C&A process; this step facilitates measurement of the level of effort that will be required.
- Develop the draft SSAA. This document constitutes the basis for the negotiation phase, which follows.

2.2.1.3 Perform Negotiation

In the negotiation phase all parties have an opportunity to express their needs and agree on their respective responsibilities. The Certifier, must exercise skills whose relevance to the C&A process might be surprising. These include listening skills, written and oral communication skills, and the power to persuade. In principle, the idea is not that the key players lock themselves in a room until they agree on what must be done, in that compliance with statutory constraints is mandatory. Instead the principals agree on strategy, resources, roles, timeline, etc. In reality, the certifier might have to, for example, convince a user representative that allowing users to hold administrative privileges is unacceptable, or persuade a DAA the level of residual risk claimed by the certifier. The draft System Security Authorization Agreement (SSAA) resulting from the registration phase provides a framework for the negotiations. The DITSCAP identifies three key negotiation tasks:

- Review the draft SSAA for accuracy and completeness, updating as necessary.
- Conduct a review of the certification requirements, modifying the SSAA as necessary.
- Approve the final SSAA, which constitutes the blueprint for the balance of the certification process. Here “final” is a relative term, in that the SSAA is under perpetual scrutiny and, as a living document, is subject to update as required.

2.2.1.4 Prepare the System Security Authorization Agreement (SSAA)

The SSAA encompasses in a single document all essential security-related information about a system. The "final" SSAA is the product of the activities performed in the first three steps, i.e., documentation, registration, and negotiation. As a living document, the SSAA is still subject to updates at every subsequent step prior to accreditation. The principal components of the SSAA are:

- Mission Description and System Identification. Much of this can come from the mission needs statement. Of interest are the system name and identification, the physical and functional descriptions of the system, and a summary of the system concept of operations.
- Description of System Operating Environment. This encompasses technical and non-technical context in which the system will be operated, software, and maintenance environments, as well as a threat description.
- Description of System Architecture. This comprises hardware, software, firmware, interfaces, information flow, and accreditation boundary.
- IT Security System Class. There are four levels of certification effort specified in the DITSCAP. Level 1 consists of a basic review of security features. Level 2 adds to the Level 1 effort some minimal analysis. Level 3 requires detailed analysis, and Level 4 requires comprehensive analysis. Determination of system class is simplified by a checklist-based scoring system applied to a profile of the target system. There are overlaps between adjacent levels, so the Certifier plays a role in ensuring that the appropriate level of effort is adopted.
- System Security Requirements. These, including national and DoD/DoN requirements, data security requirements, security concept of operations, network connection rules, configuration and change management requirements, and reaccreditation requirements.
- Organizations and Resources Required for the C&A Effort. This item identifies the principals (PM, DAA, Certifier, User Representative) and sponsoring organization, enumerates staffing and funding requirements, certification team training requirements, describes roles and responsibilities, and identifies any additional organizations or groups whose participation is required.
- The DITSCAP Plan (tailored as necessary). This includes tailoring specifics, tasks/milestones, the schedule of work, level of effort, and specification of roles and responsibilities.
- Appendices containing supporting and/or amplifying documentation are also prepared.

2.2.2 Certification

This phase comprises the next two steps: support of system development and certification analysis.

2.2.2.1 Supporting Systems Development

This is the first step in the Certification Phase of the DITSCAP, concerned with verification that a system that is in development system remains compliant with the security specifications of the SSAA. This requires more or less continuous oversight on the part of the Certifier as system development and/or integration progresses. The precise details are determined by a number of factors, including the certification level specified in the SSAA and the position of the system in its lifecycle, e.g., new system development or system maintenance. Education in the area of computer and network security is essential in this part of the certification process. The NSTISSI certifier training document (#4015) identifies the following performance items associated with this step:

- Coordination with Related Disciplines. This involves coordination with various security disciplines for expert assistance. For example, it might be necessary to call in experts on physical security, or emanation security, or cryptography. The certifier needs to justify to the DAA the need for such coordination, and to ensure that the coordinated effort is successfully accomplished.

- Configuration Control. The certifier must evaluate configuration and change control with regard to consistency with requirements, recommending changes and/or reporting deficiencies as necessary. Included in this step is verification of associated activities, such as audits, component inventories, etc.
- Information Security Policy. The certifier must identify all applicable information systems security policies, keeping the development team fully informed in order to enable system compliance. The certifier must also monitor development to ensure compliance.
- Life-Cycle System Security Planning. The certifier must evaluate the life-cycle security plan adopted by the development team. If the plan is deficient, the certifier must become an active participant in life-cycle security planning to ensure the desired outcome.
- Principles and Practices of Information Security. The certifier must understand the principles and practices of information security and the way in which those principles apply to the certification effort in question. The certifier must also adhere to these principles and, if necessary, explain these principles to the development team.
- Network Vulnerabilities. The certifier must perform system analysis to identify potential network vulnerabilities for the development team, evaluate the potential impact of such vulnerabilities, and suggest corrective measures.

2.2.2.2 Perform Certification Analysis

The certification analysis step determines whether the system in question is ready to advance to the evaluation and testing that precede a recommendation to accredit. The DITSCAP specifies the following component tasks:

- System Architecture Analysis. This task provides documented assurance that
  - The system architecture is consistent with the architecture specified in the SSAA.
  - Security architecture is consistent with specified security policy and requirements.
  - Interfaces between the subject system and other systems are identified and evaluated in terms of supporting the required system security posture.
- Software Design Analysis. The output of this step documents that security features required of the Trusted Computing Base (TCB), such as authentication, access control, and auditing, are implemented as specified.
- Network Connection Rule Compliance Analysis. This step provides assurance that neither the network nor the subject system will have undesired effects on the other's security posture.
- Integrity Analysis of Integrated Products. The subject system might integrate software, hardware, and firmware from a number of sources, e.g. commercial-off-the-shelf, government-off-the-shelf, specialized, etc. This step provides assurance that:
  - Interaction of integrated components does not result in degradation of the integrity of individual components.
  - The result of this integration is compliant with the specified system security architecture.
  - Application of components must be consistent with their intended use.

  The complexity of this step can be considerable, depending upon the level of certification required. For example, it might be necessary to verify the security features of individual components.
- Life Cycle Management Analysis. This step provides documented assurance that the security posture of the system will be preserved by the implemented change control and configuration management practices.
- Vulnerability Assessment. This step verifies satisfactory progress in implementation of the security requirements of the SSAA, by evaluating vulnerabilities and recommending countermeasures. Any vulnerability identified during certification analysis must be analyzed in terms of susceptibility to (and likelihood of) exploitation, and of the associated threat. The output of this process is a statement enumerating and evaluating residual risks and estimating the

operational impact of accepting or rejecting them. Residual risk cannot exceed the level of acceptable risk determined by the DAA.

2.2.3 Validation Phase

Like the Certification Phase, the Validation Phase also comprises two steps: certification evaluation and development of the recommendation to the DAA culminating in accreditation.

2.2.3.1 Certification Evaluation

The objective of this step is to ensure that the system, configured for deployment, complies with the security specifications as given in the SSAA. Certification evaluation is applied to hardware, software, firmware, and additionally includes site inspection. Main functional items are listed below and definitions, where definitions of terms may be found in the glossary:

- Security Test and Evaluation
- Penetration Testing
- TEMPEST and Red-Black verification
- Validation of COMSEC compliance
- System management analysis
- Site accreditation survey
- Contingency plan evaluation
- Risk-based management review

2.2.3.2 Develop Recommendation to DAA

In this activity the Certification Authority (i.e., the manger of the certification process) submits to the Designated Approving Authority a report detailing all findings from the certification process. If the process has been successful, the DAA formally accepts the (positive) recommendation and the outcome is accreditation. If change is required, an Interim Approval to Operate may be granted and, all or part of the certification effort is revisited. The following elements are identified:

- Access Control Policies. Access control policies implemented in the system to be certified must be explained to the DAA. Included in this explanation are descriptions of who makes authorization decisions and on what basis as well as the effectiveness of the implementation from the standpoint of the requirements. The certifier recommends changes, if necessary.
- Administrative Security Policies and Procedures. The certifier must consider not only those policies and procedures required by law, but also those additional policies and procedures that might be required by agency instruction or other organizational mechanism. The certifier must document to the DAA all applicable policies and procedures and the degree to which the system is in compliance, recommending countermeasures as needed to address any deficiencies.
- Certification. This is a conditional recommendation, outlining (if necessary) conditions that must be met before a decision to accredit is recommended.
- Presentation of Security Test and Evaluation Results. This might require translation, depending on the audience, however, the objective is to communicate the results to management and technical personnel.
- Identification of Potential Corrective Approaches
- Determination of Residual Risk

2.2.4 Post-Accreditation

Finally, the Post-Accreditation Phase corresponds to ongoing maintenance of the SSAA.

2.2.4.1 Compliance Validation

At intervals specified in the SSAA, the system and its operational environment are subject to review to verify compliance with the SSAA in terms of security specifications and concept of operations, and to verify that the threat assessment described in the SSAA remains accurate. The principal functional components are:

- Physical security analysis
- Review of SSAA with an update to the SSAA as needed
- Risk-based management review
- Procedural analysis
- Compliance re-verification

2.3 Maintenance of the SSAA

While the SSAA is subjected to continuous review and update during system development, the maintenance step outlined here occurs post-accreditation to ensure that the SSAA is not allowed to become stale with respect to the operational system. The principal players are the same as they have been throughout the process. As the operational system undergoes incremental change, the cerrtifier evaluates the impact of these changes on system security features, updating the SSAA, if necessary. Similarly, updates to the SSAA must themselves be evaluated in order to determine whether the Certification process must be repeated. If so, the process reverts back to the appropriate DITSCAP phase. The certifier ensures that the DAA has up to date information, and the DAA will determine whether continued operation of the system is approved. Key components in this step are:

- Control of Configuration Changes
- Maintenance of Configuration Documents
- Periodic Review of System Life-Cycle
- Contingency Planning
- Compliance Validation
- Physical Security
- SSAA Review
- Risk-based Management Review
- Compliance Re-verification

3. CERTIFIER EDUCATION

A considerable amount of technical and non-technical analysis is required to support an accreditation. This process of system certification provides a way by which the technical and non-technical aspects of a system's security can be assessed from inception through retirement. The factors that must be addressed include the sensitivity and criticality of data to be processes, the system's environment, its users, its location, its applications, interconnections, configuration, etc. To achieve these objectives, such activities as security test and evaluation, risk analysis, and a variety of other analyses and evaluations are conducted. The level of technical expertise required for individuals involved in certification is high. Even while focussing on a single security component of the system, the certifier must keep the larger system context in mind and be able to understand the impact and side effects of that component on overall system security. Thus the certifier cannot address his or her task using a check list, and focus on individual pieces, while neglecting the whole.

As is the case with many other aspects of computer science and system development, e.g. construction of operating systems or construction of physical databases, one does not learn everything in books or in a standard classroom. Even laboratory activities can be inadequate unless they are specifically designed to

foster the development of both implicit as well as explicit knowledge. In the case of system certifiers, it has been found that a combination of knowledge and experience are essential for achieving mastery of the profession.

The U.S. Department of Defense has imposed requirements for the certification and accreditation of all information systems to ensure that they are operated at an acceptable level of risk. Given the sheer numbers of systems in operation, from business systems to weapons system, this is a daunting task. The certification and accreditation problem is further compounded by the lack of experienced certifiers able to conduct the required field work. While concentrating on a particular detail, less experienced certifiers may overlook security weaknesses of the system that would be found by their more seasoned colleagues.

To address this problem, we have developed an educational program for certifiers. It is intended to compress the time it takes an apprentice certifier to achieve the experience and expertise to become a journeyman certifier. We believe that master certifiers are those individuals who have considerable experience and have the education, knowledge and fully internalized skills to assess the security properties of highly complex systems. In a sense the activities of the certifier parallel those of a systems integrator. Just as there is no expectation that a highly experienced systems integrator can be created through a set of classroom activities, there is no expectation that a master certifier can be manufactured.

Students in the program will be of two types: short course students and resident graduate students. Short course students will be individuals who may already be working in the area of certification and accreditation or those who are moving into this field. The short Certifier Education program students will spend approximately eight weeks in formal courses over a period of from eighteen months to two years. The courses will be of short duration and high intensity; with eight hours devoted to class and laboratory exercises each day. The intervening periods between visits to school will be spent in the field, where students acquire essential experience. Resident students will include certifier courses as electives as part of their graduate program, which depending upon student background, validation of prerequisites, and other factors can last between 12 and 24 months.

A prerequisite for all students is an undergraduate degree in computer science or closely related engineering field.

Table 2. Courses of the Certifier Education Program

Title	Catalog Description
Introduction to Information Assurance: Computer Security	Provides a comprehensive overview of the terminology, concepts, issues, policies, and technologies associated with the field of Information Assurance. It covers the notions of threats, vulnerabilities, risks and safeguards as they pertain to the desired information security properties of confidentiality, integrity, authenticity and availability for all information that is processed, stored, or transmitted in information systems.
Information Assurance: Secure Management of Systems	Provides students with a security manager's view of the diverse management concerns associated with administering and operating an automated information system facility with minimized risk. Students will examine both the technical and non-technical security issues associated with managing a computer facility, with emphasis on DoD systems and policies. Students will earn CNSS (formerly NSTISSI) certification for: INFOSEC professional, Systems Administrator, and ISSO.
Network Security Threat Analysis	This course is designed to give the student exposure to Internet security threats in a lab environment. Lectures and labs provide the student with a "hands on" experience with current network attacks and vulnerabilities. Foot-printing, scanning, enumeration and escalation are addressed from an attack prospective. Emphasis on detection and protection of critical data and nodes is addressed. A final project that demonstrates skills and knowledge is required.
Introduction to Certification and Accreditation	This course provides an introduction to the Certification and Accreditation (C&A) process as applied to procurement and lifecycle management of DoD and Federal information systems. Topics include: principal roles, functional components, and output documents of the C&A process; and a comparison of the government C&A process specification currently in use (DITSCAP/NIACAP, FIPS, DCID 6/3) with the emerging effort to produce a unified specification.

System Certification Case Studies	This course is part two of the two course (CS4680 and CS4685) Certification and Accreditation course sequence. Students will investigate 2-3 case studies of systems that have been evaluated, and then apply the lessons of CS4680 to make final accreditation decisions. Successful completion of this two course sequence leads to NSTISSI DAA and Certifier certification.

Our educational program is based on courses already in use as well as two new courses specific to the Certification and Accreditation Process. The courses are briefly described in Table 2. The first three courses are intended to provide students with an understanding of the problem domain for system certification. Introduction to Information Assurance is a survey course and provides students with a broad overview of the many aspects of the certification domain. The second course, Secure Management of Systems, leads to and understanding of the administrative, procedural, and personnel issues that might affect the ongoing security of a system. Finally, Network Security Threat Analysis provides students with an appreciation of the techniques and skills that will be brought to bear by adversaries attacking their systems. When combined with their background in computer science the three-course sequence described above prepares students for the two courses specific to certification.

Introduction to Certification and Accreditation is intended to teach students about all aspects of the certification and accreditation process. They are introduced to procedural aspects of the process as well as to the variety of technical issues that might be addressed. A considerable amount of social skill and team building is required for a successful certification, and students learn about the give-and-take required to achieve success. Students must understand when certain security requirements must be adhered to at all cost and when some flexibility may be appropriate.[1]

The capstone course in the sequence centers on a group of case studies. These are taken from real systems and allow students to understand how a certifier can help ensure that the security requirements are met. The cases include not only technical and procedural aspects of the certification, but discussion of the social process required to accomplish the certification.

An unusual aspect of the program is its mentoring process. Students in the program will have the opportunity to interact with instructors and staff who have experience in DITSCAP certification. This mentoring experience will help speed their mastery of the certification process. A member of our educational team with significant experience in certification keeps in touch with short course students while they are in the field gaining on-the-job experience. Students can communicate and commiserate with each other about their challenges and experiences. Because the certifier community is relatively small, it is expected that students will get to know senior certifiers and be able to ask them questions as they progress.

4. SUMMARY

Large complex systems should be analyzed prior to operation so that those depending upon them for the protection of their information will have a well defined understanding of the measures that have been taken to achieve security and the residual risk the system owner assumes during its operation. The U.S. military calls this analysis and vetting process certification and accreditation. Today there is a large, unsatisfied need for personnel qualified to conduct system certifications. An educational program to address those needs has been described.

[1] Long ago, a flag-level officer complained to one of the authors about the inability of a command to deploy a system because, from his perspective, the certifier appeared to be unusually inflexible regarding a particular point. A certifier's communications and interpersonal skills might prevent possible misunderstandings and resulting frustration.

REFERENCES

1. National Training Standard for System Certifiers, NSTISSI Document #4015, December 2000
2. DoD Instruction 5200.40, December 1997 (This instruction established the DITSCAP.)
3. DoN IA Publication 5239-13, Volume I: Introduction to Certification and Accreditation, December 2000.
4. DITSCAP Application Manual, DoD Manual Number 8510-1-M, July 2000
5. DoN IA Publication 5239-13, Volume III: Program of Record Information Systems, June 2000
6. DoN IA Publication 5239-13, Volume II: Site, Installed Program of Record, and Locally Acquired Systems, December 2000
7. DoD, Introduction to Certification and Accreditation, NCSG-TG-029, January 1994.

APPENDIX A: GLOSSARY

Accreditation: Accreditation is the statement granting approval to operate to a particular information system, with specified security safeguards and at a level of residual risk deemed acceptable. Accreditation is issued by the DAA in the form of the System Security Authorization Agreement (SSAA).

Certification: Certification is the process of evaluating the security features of a given system and the assurance levels achieved. Certification also refers to the documentation that results, specifying the extent to which the system complies with identified security requirements and the level of residual risk inherent in placing the system in operation at that level of compliance.

Certification Authority (CA): The individual with responsibility for managing the certification process. The CA determines whether the complexity of a system requires that the System Certifier be an individual or a team, by identifying the types of expertise required for the certification.

Communications Security (COMSEC): The steps taken to ensure security and integrity of information during telecommunications, especially encryption, electromagnetic emissions security, and physical security steps.

Designated Approving Authority (DAA): The DAA is the individual, typically a senior officer, who ultimately accepts the risk inherent in making a system operational. The decision is based on the evaluation of residual risk provided by the Certification Authority, Information System Security Manager, or equivalent. This evaluation is in turn likely to be assisted by the Certification Agent, or ISSO, and the Program Manager. The DoN uses the term DAA to describe two distinct roles. First is the Developmental DAA, who is in the DAA seat during program development. The Developmental DAA issues a type accreditation statement for the system in question prior to deployment. At the time of deployment, control passes to the Operational DAA, who is ultimately responsible for the risk incurred at system startup. The type accreditation statement generated during development is part of the system documentation and is thus available to the Operational DAA.

DITSCAP: The DoD Information Security Certification and Accreditation Process established by DoD Instruction 5200.40. The process formalized by the DITSCAP is fundamentally identical to the process described in this document, although there are superficial differences. The DITSCAP breaks the C&A process into four phases. Phase 1 (Definition) comprises the first four steps discussed in this document: documentation of mission need, registration, and negotiation, and final preparation of the SSAA (this step is incorporated into the negotiation step). Phase 2 (Verification) comprises the next two steps: support of system development and certification analysis. Phase 3 (Validation) also comprises two steps: certification evaluation and development of the recommendation to the DAA culminating in accreditation. Phase 4 (Post-Accreditation) corresponds to the final step in this document, which is maintenance of the SSAA. The DITSCAP was designed to be a flexible standard, readily tailored to support C&A efforts on a variety of systems including program-of-record, legacy, site, installed program-of-record, and locally-obtained systems.

Information System Security Manager (ISSM): The ISSM advises the DAA on Information Assurance issues.

Information System Security Officer (ISSO): The individual responsible for ensuring that the security safeguards of a system are maintained as specified in the accreditation, throughout the system lifecycle.

Interim Approval to Operate (IATO): An IATO can be issued for a number of reasons. For example, it might be that (a) ST&E has not been completed in the operational setting, thereby preventing completion of the C&A process, or (b) the DAA is unwilling to accept the identified level of risk except on a provisional basis.

Program Manager (PM): The individual responsible for system procurement and development, operations, or maintenance, depending upon life cycle stage.

Residual Risk: Amount of risk remaining after security measures have been applied.

Risk: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.

Software Support Activity, System Support Activity (SSA): Individual or organization responsible for life cycle support.

Security Test and Evaluation (ST&E): Testing and evaluation of the security features of a system as applied in an operational setting, to determine compliance with the specifications in the final SSAA.

System Certifier: An individual or member of a team, responsible for conducting a comprehensive analysis of the security features in a given system, and for evaluating the risks inherent in operating the system in question.

System Security Authorization Agreement (SSAA): The SSAA represents an agreement among the principals (PM, DAA, CA, User Representative), and documents the DITSCAP process. The final SSAA documents acceptance by the DAA of the level of risk inherent in making the system operational.

TEMPEST: The DITSCAP describes TEMPEST as the "short name referring to investigation, study, and control of compromising emanation from IS equipment.

Threat: Any circumstance or event with the potential to harm an IS through unauthorized access, destruction, disclosure, modificatioin of data, and/or denial of service

Trusted Computing Base (TCB): The TCB is the suite of security features interacting within a given information system to enforce a specified security posture.