CERTIFICATION AND ACCREDITATION - A WORLDWIDE VIEW

Chair: Ms. Penny Klein, DISA, INFOSEC PMO

Panelists: Barry C. Stauffer, CORBETT Technologies, Inc.
LtCol Mark Loepker, National Security Agency
Jack Torok, Central Intelligence Agency
David Murphy, NATO Office of Security
Jack Eller, DISA, INFOSEC PMO

Panel Summary

Ms. Penny Klein, DISA
INFOSEC Program Management Office
701 South Courthouse Rd.
Arlington, VA 22204-4507
(703) 681-7918, kleinp@ncr.disa.mil

On August 19, 1992 the Office of Assistant Secretary of Defense directed the Defense Information Systems Agency (DISA) to formulate a standard DoD process for security certification and accreditation (C&A). DISA formed a working group, consisting of DoD Service and Agency representatives. The working group evaluated ten existing processes, but found none which could be adopted Department of Defense (DoD)-wide. As a result, the working group developed the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). A uniform process across DoD, DITSCAP applies to accreditation of both strategic and tactical systems, as well as stand-alone information systems or networks. DITSCAP capitalized on approved security techniques, software, and procedures to reduce the complexity and overall cost of the accreditation process. The DITSCAP integrates security directly into the system life cycle and is designed so that it can be applied uniformly across DoD. The DITSCAP defines a process which standardizes all activities leading to a successful accreditation, thereby minimizing the risks associated with nonstandard security implementations across shared Defense Information Infrastructure (DII) and end systems. The DITSCAP has been designed to support the requirements of Office of Management and Budget Circular A-130.

C&A is the critical foundation for the “protect” element of the DoD IA model. The concern is both the risk at the system level and the risk to the community at large. In contrast to the previous system based accreditation processes, the DITSCAP is focused on both the system and the infrastructure. The DITSCAP is a network-centric process that views systems and networks as components of the infrastructure to evaluate the impact of the system to infrastructure.

The DITSCAP was signed as the DoD Instruction 5200.40 on December 30, 1997. Since then it has been augmented with the DITSCAP Application Document which is a handbook of step-by-step directions guiding the INFOSEC analyst through the C&A process.

Our panelists today will present:

- An overview of the DITSCAP and the current status,
- Lessons Learned from the use of the DITSCAP with U. S. Federal Agencies,
- A view of the DoD Intelligence Community Accreditation Support Team (DICAST). C&A support and its role with the DITSCAP,
- The National Security Telecommunications and Information Systems Security Committee (NSTISSIC) work on a National C&A standard,
- An overview and status of the NATO approach to a C&A process, and
- Information Assurance ((IA) and C&A tools.

Following these presentations will be a presentation of C&A tools available today and what is needed for the future.

LESSONS LEARNED FROM APPLICATION OF THE DITSCAP WITH U. S. FEDERAL AGENCIES

Barry C. Stauffer
CORBETT Technologies, Inc.
228 N. Saint Asaph Street
Alexandria, VA 22314-2517
(703) 519-8639, staufferbc@aol.com

The DITSCAP establishes a standardized process, set of activities, general task descriptions, and a management structure to verify, validate, implement and maintain the security posture of the enterprise. The DITSCAP is designed to be adaptable to any type of Information Technology (IT) and any computing environment and mission. It can be adapted to include existing system certifications and evaluated products. It can use new security technology or programs, and adjust to the appropriate standards. The process may be aligned with any program acquisition strategy. Its activities can be integrated into the system life cycle to ensure the system meets the accreditation requirements during development and integration and continues to maintain the accredited security posture after fielding. While DITSCAP maps to any system life cycle process, its four phases are independent of the life cycle strategy. The DITSCAP's, four phases, Figure 1, are: Definition, Verification, Validation, and Post Accreditation.

- Phase 1, **Definition**, defines the Certification and Accreditation Level of Effort, identifies the Designated Approving Authority, and documents the security requirements necessary for the C&A in a single document, the System Security Authorization Agreement (SSAA). Phase I focuses on understanding the mission, environment, and architecture to determine the security requirements and level of effort necessary to achieve accreditation.
- Phase 2, **Verification**, verifies the evolving, or modified, system's compliance with the agreed upon security requirements.
- Phase 3, **Validation**, validates the fully integrated system's compliance with the security requirements. Phase III concludes with full approval to operate the system, e.g., security accreditation.
- Phase 4, **Post Accreditation**, monitors system management, operation, and maintenance to preserve an acceptable level of residual risk. Phase 4 includes those

activities necessary for the continuing operation of the accredited system, e.g. change management, security management, and periodic compliance validation.

Phases 1, 2, and 3 are the DITSCAP process engine. The DITSCAP methodology permits the forward or backward movement between phases to keep pace with the system development or to resolve problems. Therefore the phases are repeated as often as necessary to produce an accredited system. The objective of these steps is to achieve agreement between the Program Manager, DAA, CA, and the Users Representative at each step of the process.

The DITSCAP has been used as the C&A process in recent government large and small client server environments, network control centers, large computer centers, financial systems, specific purpose workstations, and large scale network backbone environments. This presentation will discuss some of the lessons learned in the application of this new process.

A VIEW OF THE DOD INTELLIGENCE COMMUNITY ACCREDITATION SUPPORT TEAM (DICAST) C&A SUPPORT AND ITS ROLE WITH THE DITSCAP

Jack Torok
Director, Security Policy and Plans
Intelink Management Office
(703) 281-8920 Jacklt@ucia.gov

The DICAST was chartered in September 1997 to facilitate the joint management of risk brought about by interconnecting networks of the Defense and Intelligence Community Component members. The DICAST is neither a certifier or accreditor but a forum positioned to make recommendations that take into account this interconnected environment. This presentation will present some of the work of the DICAST and how it relates to the DITSCAP and the SABI processes.

THE NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE (NSTISSC) WORK ON A NATIONAL C&A STANDARD.

Lt Col Mark Loepker
National Security Agency/V15
9800 Savage Road 6755
Fort Meade, MD 20577-6755
(410) 859-4691, mloepker@radium.ncsc.mil

The National Security Telecommunications and Information Systems Security Committee (NSTISSC) has established a subcommittee to develop a National C&A standard. This committee is currently reviewing existing processes such as the DITSCAP, the NCSC draft Certification and Accreditation Process Handbook for Certifiers, NCSC-TG-031, and the draft

Information Assurance Guide. This presentation will present the strategy for the NSTISSC, the C&A process status toward developing the National C&A guidance in support of NTISSP 6.

AN OVERVIEW AND STATUS OF THE NATO APPROACH TO A C&A PROCESS

David Murphy
NATO Headquarters
Office of Security, Room H318
1110 Brussels Belgium
011 322 707 4592, facsimile 011 322 707 5227

NATO members have developed a NATO approach to the C&A of their information systems. This presentation will include an overview of the NATO approach, the NATO C&A process, the responsibilities of the NATO Office of Security and those of the Security Accreditation Board. A key element in the NATO security accreditation is the trust that each NATO/National Security Accreditation Authority will fulfill its responsibilities in providing statements of compliance with the Security Accreditation Boards requirements. The basis for NATO security accreditation includes:

- Review of the risk assessment process and resultant information.
- Review and approval of the security-related documentation.
- Verification that the security measures have been implemented in accordance with the security requirements.
- Identification of residual risk, and processes for ongoing risk management.

INFORMATION ASSURANCE, C&A AND INFOSEC AWARENESS TOOLS

Mr. Jack Eller, DISA
INFOSEC Program Management Office
701 South Courthouse Rd.
Arlington, VA 22204-4507
(703) 681-7929, ellerj@ncr.disa.mil

The Defense Department, through DISA and NSA, have developed numerous ways to support the DoD Information Assurance program, C&A standardization, the DITSCAP, the SECRET And Below Interoperability (SABI) initiative and INFOSEC Awareness and Training programs. Mr. Eller will discuss the functions and availability of some of these tools, methods, and procedures.