

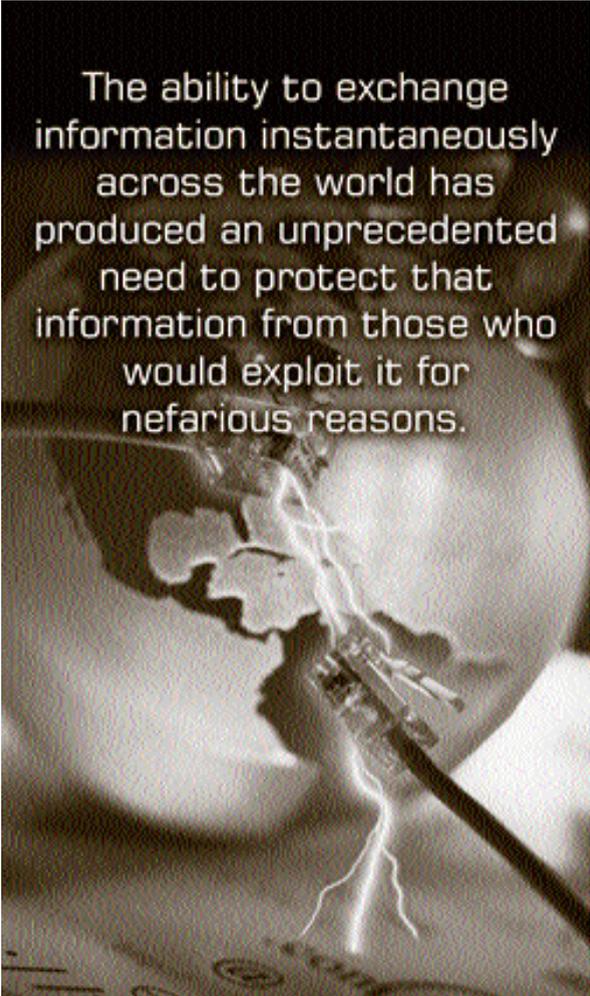
DoD's Information Assurance Certification & Accreditation Process

Peter Williams ■ Tiffani Steward

Global connectivity, real-time collaboration, and rapid and continuous information exchange have become a reality, and this reality is called net-centricity. In a net-centric environment, enterprise applications exchange data, share tasks, and automate processes over interconnected networks and the Internet. Connections between Services are dynamic and ad hoc, which implies a paradigm shift from the past. Users and applications have greater accessibility to data and can utilize data without lag time. This ability to exchange information instantaneously across the world has produced an unprecedented need to protect that information from those who would exploit it for nefarious reasons. The protection of data on information systems by ensuring the information's availability, integrity, authentication, confidentiality, and non-repudiation is called Information Assurance (IA)

and the process for managing and maintaining the system's IA posture is called Certification and Accreditation (C&A).

When communicating between different information systems, it is the responsibility of both parties to ensure the security of that communication. This is done through the



The ability to exchange information instantaneously across the world has produced an unprecedented need to protect that information from those who would exploit it for nefarious reasons.

inclusion of IA security requirements in the development of the information system or the application of those requirements later in its life cycle.

An IA C&A process represents a standard approach for identifying information security requirements, providing security solutions, and managing the security of information systems. It describes a set of requirements and capabilities and provides evidence of compliance through documentation and test results. It is the mechanism for communicating acceptance and trust between information systems.

The C&A process is designed to certify that an information system meets documented security requirements and will continue to maintain the accredited security posture throughout its life cycle. Security accreditation is the official management decision given by a senior official of an organization to authorize the operation of the system and to explicitly accept the risk to operations and assets of the organization based upon implementation of an agreed-upon set of security controls. Accreditation provides a form of quality control and challenges managers and technical staffs to implement the most effective IA security controls possible, given the technical, operational, cost, and schedule constraints.

Williams has been an associate with Booz Allen Hamilton since 2002, focusing on information assurance and certification and accreditation policy issues for the DoD, the Committee for National Security Systems (CNSS), and other Federal agencies. Steward joined Booz Allen Hamilton in 2006 and currently supports the Naval Observatory. She has also worked as system administrator and security specialist and a security engineer for the Army and federal agencies.

The Transition to a New C&A Process

The DoD Information Assurance Certification and Accreditation Process (DIACAP) was developed by DoD to address the paradigm shift in IA security from an individual information system-level approach to a DoD-wide enterprise approach of securing information systems in a net-centric environment and for supporting the implementation of IA security during a system's life cycle. The DIACAP was necessary to respond to changes in information technology, the way DoD acquires IT, and the way DoD operates IT; and to comply with emerging federal requirements and guidelines, such as the Federal Information Security Management Act of 2002, which requires federal departments and agencies to develop, document, and implement an organization-wide program to provide IA. Also, DoD wanted to develop a new C&A process that was less time-consuming, easier to implement, less resource-intensive, presented clear accountability, was paperless, used standardized security, had a security reporting status capability, and incorporated an enterprise perspective. The DIACAP meets those requirements.

The DIACAP is a dynamic IA C&A process that supports and complements the net-centric Global Information Grid environment. In general terms, the DIACAP establishes a standard, required process for identifying, implementing, and validating standardized IA controls; authorizes the operation of DoD information systems; manages the IA posture of an information system throughout its life cycle; and provides the DoD with an enterprise-level methodology for administering and monitoring C&A across the Department. The DIACAP process has replaced the previous information system-specific C&A process, the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

The DIACAP program, consisting of the DIACAP Policy, DIACAP Knowledge Service (KS), and Enterprise Mission Assurance Support Service (eMASS), was developed to meet DoD's current and future C&A requirements. All three elements of the DIACAP were developed concurrently by DoD in order to provide the DoD C&A community with the policy and specific tools designed to support and enhance the implementation of the DIACAP. The DIACAP program includes the elements described below.

DODI 8510.bb Instruction—This provides a new policy and enterprise governance structure that establishes a C&A process to provide management of the implementation of IA and visibility of accreditation decisions authorizing the operation of DoD information systems, to include core enterprise services and Web services-based software systems and applications.

DIACAP KS—DIACAP implementation support is provided through the DoD-owned, Web-based resource, the DIACAP KS. The KS is DoD's official site for DIACAP policy

and guidance and may be accessed at <<https://diacap.iaportal.navy.mil>>. The KS provides:

- A library of tools, diagrams, process maps, artifacts, etc., to support the execution of the DIACAP
- Guidance for identifying which IA controls sets are needed for a given information system, while providing the required validation tests and their expected results
- A collaboration workspace for the DIACAP user community to develop, share, and post lessons learned and best practices.

Enterprise Mission Assurance Support Service (eMASS)

eMASS is a DoD-owned, automated, Web-based suite of integrated services for the management of key activities in the DIACAP process workflow that facilitates the implementation of the DIACAP. eMASS automatically generates the C&A process workflow once a system is registered and personnel are selected for the DIACAP process functions. It also creates the C&A package for the information system. eMASS allows the user to:

- Enter IA system information
- Track the progress of IA activities of systems
- Track current C&A status of systems.

Integration of IA into the Acquisition Process

The DIACAP directly supports the DoD Instruction 8580.1, Information Assurance in the Defense Acquisition System; DoD Directive 5000.1, Defense Acquisition System; and DoD Instruction 5000.2, Operation of the Defense Acquisition System, by providing the capability to introduce IA into any stage of the system life cycle, with an emphasis on building in IA capabilities during the concept refinement and technical development phases and synchronizing the DIACAP activities with the entire life cycle. Early planning and the integration of IA result in lower program risk and support milestone decisions. There is also a significant cost benefit to building in IA during the development phase, as opposed to bolting on IA capabilities after an information system is operational.

Current Status of the Policy

The Interim DoD Information Assurance Certification and Accreditation Process Guidance, as well as the Knowledge Service and eMASS, were released on July 6, 2006, to provide the DoD user community early access to the new process and guidelines for transitioning to the DIACAP. The DITSCAP instruction and manual were replaced at that time by the DIACAP as the only DoD IA C&A process. The final version of the DIACAP is under coordination at the time of writing, and it is anticipated to be signed out during the late summer or early fall of 2007.

The authors welcome comments and questions and can be contacted at williams_peter@bah.com and steward_tiffani@bah.com.