



Reciprocal: DIACAP Review
infectionvectors.com
July 2006

Overview

Given the widespread interest in the US Department of Defense (DoD) regulations by visitors of the site, the following brief was published on the new DoD Information Assurance Certification and Accreditation Process (DIACAP). This report attempts to identify differences between DIACAP and its predecessor, as well as serve as an introduction to the new process itself.

Although the requirements for the process are in effect only for DoD programs (and many items contained herein will only be relevant to DoD workers), there is a very sound process developed with the DIACAP which may be of benefit to all types of organizations. DIACAP has been in development for many years and has been recently ordered as the replacement to DITSCAP, with transition guidelines coming from the DoD.

DIACAP replaces (but is not a sequel to) the DITSCAP (DoD Information Technology Security Certification and Accreditation Process). As such, the DIACAP (based on DoDI 8510.bb) will cancel DoDI 5200.40 and DoDI 8510.1-M. Existing instructions for implementing high security standards for all systems are still in effect, and in fact can be considered to be reinforced by DIACAP. The table below summarizes the orders affected by DIACAP:

DIACAP will replace:	DIACAP reinforces:
DITSCAP	8500.2 (Information Assurance Implementation, February 2003)
5200.40 (DITSCAP, January 1997)	FISMA (NIST publications 800-53, 59, & 60; FIPS 199 & 200).
8510.1-M (DITSCAP Application Manual, July 2000)	IA requirements of the Global Information Grid (GIG)

The e-Government Act (Title III of which is known as the Federal Information Security Management Act or FISMA) requires that all federal agencies institute IA plans, DIACAP extends the spirit of this into the DoD realm, where the Global Information Grid (GIG) architecture has supported the importance of network security for years.

For those familiar with the phases of the DITSCAP model, the following table compares them with the DIACAP equivalents:

DITSCAP	DIACAP
Definition	Initiate & Plan
Verification	Implement & Validate
Validation	Make C&A Decisions
Post-Accreditation	Maintain ATO/Reviews
	Decommission

Beyond noting the more specific descriptions of each of the phases within DIACAP, one will also notice immediately the explicit “Decommission” phases within the new model. DIACAP requires knowledge of two additional frameworks: the notion of a network-centric environment and the Global Information Grid, or GIG.

Network-centricity, net-centric, and network-centric models are terms that have been tossed around by multiple sources. With respect to DoD systems, net-centric is used to describe the vision for all defense applications. It is based on the development of the GIG and was a major force behind the push for DIACAP. As a result of the numerous changes required by moving from a very segregated, closed set of systems to the globally-interconnected world of the GIG DoD recognized the limits of DITSCAP. Net-centric in the most basic terms is the notion that every system that is connected to the network (or the GIG in this case) is not considered as a standalone entity. The net-centric world requires that systems are capable of sharing data, have appropriate tags for data (making it visible to other network clients), and seamless integration with the GIG. Additional clarification can be found in the DoD “Net-centric” Checklist instruction of 2004¹:

Programs must address the Department of Defense’s Net-Centric Data Strategy for the following:

- Ensuring that data are visible, available, and usable when needed and where needed to accelerate decision-making
- Tagging” of all data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery of data by users
- Posting of all data to shared spaces to provide access to all users except when limited by security, policy, or regulations
- Advancing the Department from defining interoperability through point-to-point interfaces to enabling “many-to-many” exchanges typical of a network environment

To implement the Information Assurance Strategy to transition to a net-centric environment, programs must take advantage of the following:

- An integrated Identity Management, Permissions Management, and Digital Rights Management
- Ensuring that adequate confidentiality, availability, and integrity are provided

GIG standards have been around for some time now, although they have been adopted in different degrees. The core of the GIG is a requirement to provide various platforms a uniform environment. That means similar approaches to implementing technologies, the ability to share guidelines/standards among programs, and maintenance of system flexibility (to allow for new technology).

Application

Two new tools are used in the DIACAP that help share certification data among all interested parties: the Knowledge Service (KS) and the Enterprise Mission Assurance Support Services (eMASS). The KS is a database of guidelines that is reached via the Web. The KS maintains current requirements data, lessons learned documents, best practice resources, and general certification news. The collaborative nature of the site allows for community-wide input and discussion. The eMASS is a web-based set of services that will support program management (producing a set of certification documents, workflow information, etc.), throughout the DIACP system lifecycle. The ability to share such data among various C&A groups around the United States (and the world) should not be undersold – leveraging previous certification work for other programs will have profound effects on future programs.

One additional supplement to the existing tool base is the Vulnerability Assessment Management Service (VAMS). VAMS is a database of system information that is intended to produce a standardized report of a particular platforms security posture. The tool will continue to rely upon the current testers/analysts and existing test tools to populate its database.²

Highlights of the DIACAP that should appear as sound IA practices to all organizations:

- Review of System Security at Least Every Year
- Enterprise (central) IA Decision Making
- Fosters Inter-agency Information Sharing
- Configuration Management Requirements

Periodic review is a goal for most enterprises, governmental or commercial, however, implementation of the review process is often met with resistance as budgets and operational restraints prevent adequate auditing. In addition, there is little enforcement for non-compliant projects/divisions. An initial concern of the DIACAP model, much like DITSCAP, is to identify a party responsible for accepting the risks of a respective system and who also has the ability to reject a system for incurring too much risk to the overall network. Under the DITSCAP/DIACAP model that person is the Designated Approval Authority (DAA). There are two new roles with oversight requirements, the Principal Accrediting Authority (PAA), who is given oversight responsibility for mission areas (Component Head) and the Senior Information Assurance Officer (SIAO), responsible for ensuring baseline requirements are met within each area. These roles have not been discussed a great deal outside of early process documents, and they will likely have little impact on routine DIACAP functions for the majority of C&A activities.

In theory, the DAA has identified the acceptable level of risk for the enterprise prior to making a determination on any specific platform. This is a time-consuming exercise in itself for large organizations. It requires evaluating such things as:

- Risk Tolerance
- System Criticality
- Data Valuation
- Network-wide Protection Mechanisms
- Enterprise Policies

This effort is a good barometer of the maturity of an information assurance (IA) program, as established, successful organizations have likely had to perform such valuations numerous times in the past. The Information Assurance Manager (IAM) and/or Certification Authority (CA) are responsible for making the recommendation to the DAA. That involves managing the technical and non-technical review of the complete system and crafting the related documentation. Most tests (especially those in the technical realm) fall under the jurisdiction of the validation tester(s). These positions, although they always have the goals/interests of the enterprise in mind, are ostensibly objective reviewers. The system advocates take the form of a Program Manager (PM, or possibly Project Manager in the commercial world) and their team – those that are charged with producing the hardware/software components. Initial evaluations begin with the project team itself (PM). The PM specifies the Mission Assurance Category (MAC) and Confidentiality Level (CL) required for their platform.

Requirement	Description	Focus
MAC	Criticality of Component Availability to Organization/Business Goal	Availability/Integrity
CL	Criticality of Data Privacy to Organization/Business Goal	Confidentiality

These may seem to have relevance only to military projects, however, requiring an advocate to identify what level of protection their system will need helps align their notions of how much security engineering with realistic goals and the enterprise philosophy.

MAC	Availability	Integrity
I	High	High
II	Medium	High
III	Basic	Basic

CL	Confidentiality
Classified	High
Sensitive	Medium
Public	Basic

For DIACAP reviews, the MAC and CL are used to determine a precise minimum score - correlating to the number of controls a system must implement to ensure that a proper IA plan has been constructed. For example, a system at MAC Level II requiring a CL of Sensitive would require a High level of Integrity, Medium level of Availability, and Medium level of Confidentiality. The generic guidance from this exercise translates into the number of protection mechanisms that need to exist for the given platform:

MAC	CL	Required Minimum for:			
		Confidentiality	Integrity	Availability	Total
I	Classified	45	32	38	115
II	Classified	45	32	38	115
III	Classified	45	27	37	109
I	Sensitive	37	32	38	107
II	Sensitive	37	32	38	107
III	Sensitive	37	27	37	101
I	Public	11	32	38	81
II	Public	11	32	38	81
III	Public	11	27	37	75

The controls themselves are the DODI 8500 requirements (divided into groups based on applicability to Confidentiality, Integrity, and Availability) that are familiar to most Certification and Accreditation (C&A) personnel. In commercial applications, the criteria could be best practices from internal IA teams, external groups like SANS, or from automated vulnerability scanners. The scorecard then becomes a piece of the DIACAP package.

Revision

Of course, the risk incurred by any individual system cannot be completely captured by a numerical score. The risk assessment is still a vital role of the CA/IAM once testing and documentation of the system is complete. Analyzing the Residual Risk of the system under review is completed by taking the vulnerabilities/threats to system, any mitigation efforts, the value of the information/components, and the network context of the system under consideration. All of these elements should play into a holistic risk assessment. That assessment then becomes the foundation of the Certification and Accreditation decisions.

It is vital to an enterprise-class C&A program that determinations of security posture discrepancies (findings), the threat exposure rankings (or Categorizations), and then the subsequent accreditation decisions are consistent. C&A efforts that are based in subjective criteria and intuition are often described as “moving targets” by the PMs at their mercy. These types of C&A shops act as impediments to new technology and business processes instead of facilitators.

The DIACAP “product” is a set of materials that should fully encapsulate the security posture of the proposed system. A complete DIACAP package contains the following:

- System Identification Profile
- Implementation Plan & DIACAP Strategy Documents
- Support Documentation (Test Reports, Artifacts, etc.)
- Scorecard (and Certification decision)
- Accreditation decision
- Plan of Actions and Milestones (POA&M, if needed based on test reports/accreditation)

The traditional SSAA is no longer required.³ That is tremendous news to many programs that have wrestled with the sometimes overwhelming amount of paperwork required by DITSCAP accreditation cycles.

Additional details for each of these documents as well as the current guidance from DISA for DIACAP programs are available during the transition period.⁴ From that document comes the following breakdown of each phase of the DIACAP process:

PHASE	PROCEDURE	PHASE #
Initiate & Plan	Register System with DoD Component	1
	Assign IA Controls	
	Assemble DIACAP Team	
	Review DIACAP Intent	
	Initiate Implementation Plan	
Implement & Validate	Execute and Update IA Implementation Plan	2
	Conduct Validation Activities	
	Compile Validation Results	
Make C&A Decisions	Analyze Residual Risk	3
	Issue Certification Determination	
	Make Accreditation Decisions	
Maintain ATO/Reviews	Lifecycle Implementation Begins	4
	Plan for IA Controls	
	Maintain Situational Awareness	
	Maintain IA Posture	
Decommission	Disposition of DIACAP Data	5

As can be gleaned from the table above, the iterative nature of the testing and validation process means a system can reside in one of the phases for quite some time. In addition, there may be cycles of each phase, for instance a system may get an unfavorable accreditation decision and return to Phase 2 from Phase 3. A system may remain in Phase 4 for years prior to exiting the DIACAP lifecycle.

As one can see, the keys to DIACAP are the standardization of security posture scores and a flexible (and reusable) set of documentation. As the new process is adopted by programs entering the C&A lifecycle, the success of such tools as the KS and eMASS will be the best barometers of DIACAP's longevity.

References

1. Net-centric Checklist, version 2.1.3. Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 12 May 2004. http://www.dod.gov/nii/org/cio/doc/NetCentric_Checklist_v2-1-3_May12.doc.
2. Additional information on the VAMS as well as a broad array of DIACAP-related initiatives can be found in: IA Newsletter, Net-centric Assured Information Sharing. Volume 8, Number 3, Winter 2005/2006. http://iac.dtic.mil/iatac/download/Vol8_No3.pdf
3. For an excellent overview of the DoD C&A process, standards, and new DIACAP requirements, also see Jenifer M. Wiernum's "Defense Information Assurance Certification and Accreditation Process (DIACAP) and the Global Information Grid (GIG) Information Assurance (IA) Architecture" report published by Cygnacom Solutions for the 10th International Command and Control Research and Technology Symposium The Future of C2 found at: http://www.afei.org/documents/DIACAPandtheGIGCCRTS_371.pdf.
4. Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance, 6 July 2006. <http://iase.disa.mil/ditscap/interim-ca-guidance.pdf>.

Additional Resources

The FISMA documentation:

<http://csrc.nist.gov/policies/FISMA-final.pdf>

DISA documentation DITSCAP-DIACAP

<http://iase.disa.mil/ditscap/>