



DIACAP Dimensions

Volume 4 Issue 1 • June 2010

DIACAP Resource Center • www.diacap.net • Email: diacap@diacap.net • Phone: (540) 808-1050 • Fax: (540) 808-1051

C&A Transformation

By Lon Berman

It has been said that the only constant in this world is change. Just when we were finally getting comfortable with DIACAP and the DoD Instruction 8500.2 IA Controls, rumors have begun to circulate about possible “sweeping changes” to the DIACAP. In a previous issue of *DIACAP Dimensions* we even jokingly referred to “DIACAP II – The Sequel”. While it is true there is an ongoing “transformation” underway in the DoD Certification and Accreditation (C&A) program, we believe it is premature to call it a “sweeping” or “radical” change.

First, some background is in order. For as long as many can remember, the government (specifically the executive branch) has labored under the burden of three distinct approaches to C&A. As we all know, DoD C&A is based on the DIACAP process (DoDI

8510.01) and requirements derived from DoDI 8500.2. The “civilian” departments and agencies, (State, Treasury, Homeland Security, Veterans Affairs, etc.) utilize a different process, based on NIST 800-37 and NIST 800-53 requirements. The intelligence community uses yet another process and requirements set, based on DCID 6/3. Many government programs involve players from two or even all three of these “sectors” (DoD, Civilian, Intelligence) and therefore have to deal with C&A processes and requirements sets that are, at best, difficult to align and sometimes even conflicting.

The Joint Transformation Initiative is an ongoing attempt to align the DoD, civilian and intelligence agencies on a common C&A process and requirements set. In the past several months, the Joint Transformation Initiative Task Force has



Lon Berman, Principal Consultant

worked with NIST to publish two documents that show some significant progress in that direction. NIST Special Publication (SP) 800-37, Revision 1, describes a new Risk Manage-

See C&A on page 3

Four Types of Information Systems

By Kathryn Farrish

DoDI 8500.2 defines an information system as a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

The Department of Defense categorizes information sys-

tems into four major categories: AIS Application, Enclave, Outsourced IT-Based Process, and Platform IT Interconnection. DIACAP is implemented for each of these types utilizing a lifecycle centric model.

Automated Information System (AIS) Application: A product or deliverable of an

acquisition program performing clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. AIS applications are deployed to enclaves for operations, and have their operational security needs assumed

See Four Types on page 3

Inside this issue:

<i>C&A Transformation</i>	1
<i>Four Types of Information Systems</i>	1
<i>IA Control Spotlight</i>	2
<i>Top Ten List</i>	2
<i>DIACAP Training Schedule</i>	4



IA Control Spotlight—Configuration, Change and Release Management

By Lon Berman



Spotlight on Configuration, Change and Release Management

“It would be difficult, if not impossible, to maintain an adequate security posture without effective policies and procedures in these areas.”

Configuration, change and release management are essential elements in the life cycle of any system. It would be difficult, if not impossible, to maintain an adequate security posture without effective policies and procedures in these areas. DoD Instruction 8500.2 includes several IA Controls that address this subject.

DCCB-1 establishes the fundamental requirement for a configuration control board (CCB):

“All DoD information systems are under the control of a chartered configuration control board that meets regularly according to DCPR-1.”

DCCB-1 applies to MAC III systems. For the more critical MAC II and MAC I systems, **DCCB-2** includes the additional requirement that the Information Assurance Manager (IAM) be a member of the CCB.

Basic features of a sound configuration management program are spelled out in **DCPR-1**, which applies to systems at all

MAC and Confidentiality levels.

“A configuration management (CM) process is implemented that includes requirements for:

(1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation;

(2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems;

(3) A testing process to verify proposed configuration changes prior to implementation in the operational environment; and

(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.”

DCHW-1 and **DCSW-1** require

baseline hardware and software inventories to be kept under CCB control.

Change and release management are addressed in controls such as DCII-1, Impact Assessment, which states:

“Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.”

and **DCCT-1**, Compliance Testing:

“A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.”

A good source of additional information on these topics is the Capability Maturity Model (CMM) developed by the Carnegie Mellon Software Engineering Institute.

Top Ten List — IA Resources Online

By Jeffrey Widom

Previous issues of *DIACAP Dimensions* have made reference to various online resources for DIACAP and related Information Assurance topics. Here is our “top ten” list of online IA resources. A few of these sites may be “restricted” (i.e., accessible only from .gov/.mil or requiring CAC authentication), but most of them are open to all. Enjoy!

10. DoD IA Training -

<http://iase.disa.mil/eta/index.html#onlinetraining>
Online training provided by the Defense Information Systems Agency; includes a brief DIACAP overview.

9. DSS -

http://www.dss.mil/isp/industrial_sec.html
Defense Security Service web site for the National Industrial Security Program. This information mostly concerns contractors handling

clearances, classified documents, and/or classified computer systems on their premises.

8. DISA (NIPRnet/SIPRnet) -

<http://www.disa.mil/services/data.html>
Defense Information System Agency web site for Secret Internet Protocol Router Network (SIPRNet) and Non-classified Internet Protocol Router Network (NIPRNet) connection approval processes.

7. CNSS -

<http://www.cnss.gov>
Web site for the Committee on National Security Systems, including numerous publications. CNSS Instruction 4009, the National Information Assurance Glossary, was recently revised and is available for download. CNSS Instruction 1253 provides requirements for National Security Systems.



Top Ten IA Websites

C&A (cont. from page 1)

ment Framework (RMF) that includes, among other things, a Security Authorization (aka. C&A) process. NIST SP 800-53 provides an updated “catalog” of controls (aka. security requirements or IA Controls) that address management, operational and technical areas.

At this point there has been some movement on the part of DoD to begin a transition from the 8500.2 IA Controls to the 800-53 control set. DoD has recently published the first draft of a “mapping” between the two control sets. As of yet

there is no formal DoD policy mandating, or even recommending, this transition, nor have any timelines been established. Still, it is clear the intent is for DoD to eventually make the move. DoDI 8500.2 is more than seven years old (it predates the DIACAP by well over four years!), so it is certainly more than ready for a “facelift”.

By contrast, the DIACAP *process* itself (DoDI 8510.01) is only three years old and just now becoming entrenched within the various DoD components. It does not seem likely

that DoD will be looking to replace it with the RMF anytime soon.

DIACAP Dimensions will continue to track the progress of the transformation and report any significant events. Stay tuned!



Four Types (cont. from page 1)

by the enclave. An AIS application is analogous to a “major Application,” as defined in OMB A-130, however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System (MAIS).

Enclave: A collection of computing environments connected via one or more internal networks, under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes that they support, and derive their security needs from those systems. They provide standard IA capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and email. Examples of

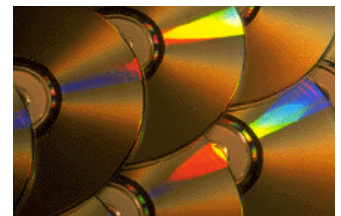
enclaves include local area networks (LANs) and the applications they host, backbone networks, and data processing centers.

Outsourced IT-based Process: A general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Platform IT Interconnection: Refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Platform IT consists of computer resources, both hardware and software,

that are physically part of, dedicated to, or essential in real-time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of Platform IT connections that impose security considerations include: communication interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

“The Department of Defense categorizes information systems into four major categories: AIS Application, Enclave, Outsourced IT-Based Process, and Platform IT Interconnection.”



DIACAP Training Schedule

DIACAP Resource Center offers *DIACAP Fundamentals* (one-day) and *DIACAP In-Depth* (three-day) classes on a regularly scheduled basis in the National Capital Region, Colorado Springs, Huntsville, and San Antonio.

Regularly scheduled classes for the remainder of the calendar year for 2010 are as follows:

DIACAP Fundamentals (One-day)	DIACAP In-Depth (Three-day)
7 June (NCR)	8-10 June (NCR)
12 July (NCR)	13-15 July (NCR)
19 July (H)	20-22 July (H)
16 August (CS)	17-19 August (CS)
13 September (NCR)	14-17 September (NCR)
20 September (SA)	21-23 September (SA)
18 October (NCR)	19-21 October (NCR)
25 October (H)	26-28 October (H)
6 December (NCR)	7-9 December (NCR)

(NCR) = National Capital Region
 (CS) = Colorado Springs (H) = Huntsville
 (SA) = San Antonio

For Customers in other locations or those with specific scheduling requirements, we offer the option of “on-site” training. All you need is a group of students (at least 8-10) and a suitable classroom facility. We offer a discount over the normal “per student” registration cost; the discount grows larger as the class size increases. Our “on-site” training fee includes all instructional services, training materials, and instructor travel expenses. Most importantly, you will avoid the travel expenses associated with sending your people to training away from the office. Please contact the DIACAP Resource Center at (540) 808-1050 or diacap@diacap.net to request an on-site training quotation.

On-line registration and payment for all scheduled classes is available at our website www.diacap.net. Registration can also be done by downloading a registration form and submitting the completed form by FAX or email. Payment arrangements include credit cards, SF182 forms, or purchase orders.

Please visit www.diacap.net for the latest training schedule, including any new dates or locations.

FISMA Risk Management Training

Training is also available in the FISMA (NIST) Risk Management Framework (C&A process) that is used by federal civilian agencies and the intelligence community. This process forms the basis of the forthcoming “unified”, government-wide, Security Authorization process. For information on this training program, please visit www.fisma1.net or www.fedca.org.

Top Ten (cont. from page 2)

6. OMB Memoranda -

http://www.whitehouse.gov/omb/memoranda_default/

Web site for Office of Management and Budget (OMB) Memoranda, including those that address security, privacy and FISMA requirements.

5. STIGs -

<http://iase.disa.mil/stigs/index.html>

Defense Information Systems Agency web site for Security Technical Implementation Guides (STIGs), Security Checklists, and Security Readiness Review (SRR) scripts. STIGs contain detailed configuration guidance for operating systems, databases, web servers, wireless systems, etc., and are mandatory for all DoD information systems. SRR scripts are automated tools that assist in validating STIG compliance.

4. DIACAP Knowledge Service -

<https://diacap.iaportal.navy.mil/>

Official Department of Defense web site for DIACAP. Common Access Card (or commercial certificate and DoD employee sponsor) required for access.

3. DoD Directives - <http://www.dtic.mil/whs/directives/index.html>

Official Department of Defense web site for DoD Issuances including Directives, Instructions, Publications, Administrative Instructions, and Directive-Type Instructions.

2. FIPS - <http://csrc.nist.gov/publications/PubsFIPS.html>

Official NIST web site for Federal Information Processing Standards (FIPS). FIPS Publications are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

1. NIST Special Publications -

<http://csrc.nist.gov/publications/PubsSPs.html>

Official NIST web site for Special Publications. Special Publications in the 800 series present documents of general interest to the computer security community. Special Publications include documentation of the new Risk Management Framework (RMF) that will (hopefully) become the standard for all federal information systems.