



# DIACAP Dimensions

May  
2008

DIACAP Resource Center ▪ [www.diacap.net](http://www.diacap.net) ▪ E-mail: [diacap@diacap.net](mailto:diacap@diacap.net) ▪ Phone: 540-808-1050

## INSIDE THIS ISSUE

- 1 Putting DIACAP in its Place!
- 1 Inside the DIACAP Knowledge Service
- 2 Top Ten List – C&A Pitfalls
- 3 IA Control Spotlight – Configuration Management
- 4 DIACAP Training for 2008

## Putting DIACAP “in its Place”

By Lon J. Berman

To fully understand DIACAP it takes more than a knowledge of roles, responsibilities, activities, and IA controls. Rather, it requires an understanding of government organization and policy at the highest level.

If you remember your Civics class from eighth grade, you’ll recall there are three branches of government - executive, legislative, and judicial. The legislative branch consists principally of the two houses of Congress and a handful of ancillary organizations such as GAO, Library of Congress, etc. The judicial branch is essentially the federal courts system, including the Supreme Court, US District Court, Court of Appeals, Bankruptcy Court, etc. *The executive branch is everything else...* DoD, the “civilian” departments (Agriculture, State, Homeland Security, etc.), and the intelligence agencies (CIA, NSA, etc.).

At the very top of the executive branch organization chart sits the White

Please see *In its Place* on page 2

## Inside the DIACAP Knowledge Service

By Lon J. Berman

The DIACAP Knowledge Service is DoD’s official website for the DIACAP program. The site contains a wide variety of information, ranging from IA controls and validation procedures to DIACAP documentation templates and examples.

The DIACAP Knowledge Service is hosted on a Navy site, but it is designed for use by all DoD personnel and contractors. The URL is:

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

The primary means of access is by DoD PKI, i.e., the Common Access Card (CAC). If you are a contractor and do not hold a CAC, do not despair, you can still get access to the DIACAP Knowledge Service. You will need a software digital certificate on your PC and the endorsement of a DoD employee. The URL above contains full instructions for both DoD

Please see *Knowledge Service* on page 3

---

*“The News page is updated each time there are changes to the site....”*

---

## Top Ten List – C&A Pitfalls

By Jeffrey H. Widom

Numerous pitfalls can derail your C&A project, or lead to less-than-spectacular results. Here is our Top Ten List of C&A “mistakes.”

10. Fear of reprisal - C&A team members and system supporting personnel should not be afraid to identify risks for fear of reprisal.

9. Failure to accept responsibility - Successful Certification and Accreditation (C&A) projects are not always easy to complete. All members of the C&A team must fully accept responsibility for their assigned C&A positions.

8. Inadequate budget - Funding for C&A must start at the beginning of the system life-cycle. For example, the System Owner may be responsible for funding a certification agent to execute the Security Test and Evaluation (ST&E), automated tools verify to security controls, and contractor support to develop the C&A package.

7. Insufficient time - Successfully completing a C&A takes time. Determining the total amount of time requires the input of multiple C&A team members including the System Owner, IAO, CA, and/or DAA.

6. Failure to involve required resources - It is extremely difficult for a single person to successfully complete a C&A. Physical Security Officers, Personnel Security Officers, System Administrators and other staff play a vital role in the success of the C&A process and must be identified early in the project.

5. Lack of training - Personnel assigned to primary C&A roles (such as the IAO) should be fully trained and understand their responsibilities. Holding a “generic” information security certification does not necessarily guarantee that a person has the necessary DIACAP knowledge.

4. Lack of traceability - C&A documents should be related. For example, the MAC and CL on the System Identification Profile relate directly the requirements

Please see *Top Ten* page 4

---

*“Personnel ... should be fully trained and understand their responsibilities...”*

---



Our National Capital Region training  
site partner ([www.intelligent.net](http://www.intelligent.net))

### ***In its Place*** from page 1

House (i.e., the office of the President). It is from the White House Office of Management and Budget (OMB) that one of the fundamental information security policy documents originates. This is OMB Circular A-130, entitled *Management of Federal Information Resources*. Appendix III of OMB A-130 deals specifically with security, and mandates the *certification* (compliance validation) and *accreditation* (formal approval to operate) of all federal information systems.

Each department and agency in the Executive Branch is required to implement the provisions of OMB A-130. The C&A requirement has been implemented in three different ways. The civilian federal departments have standardized on the C&A process developed by NIST, the National Institute of Standards and Technology. The intelligence community has standardized on a process called DCID 6/3. The Department of Defense has standardized on a process called DIACAP, the *DoD Information Assurance Certification and Accreditation Process*. **All three C&A processes meet the high-level requirements set forth in OMB A-130.**

## IA Control Spotlight – Configuration Mgmt.

By Jeffrey H. Widom

DCCB-1 and DCPR-1 are the fundamental Configuration Management (CM) requirements in DoDI 8500.2. Essentially, they require a chartered Configuration Control Board (CCB) and a fully-functional CM program that includes: formally-documented roles, responsibilities and procedures; security review and approval of proposed system changes and interconnections; testing of proposed changes prior to implementation; a verification process to ensure proper functioning of the CM program and to prevent unauthorized changes outside of CM control.

A properly functioning CM program ensures compliances with numerous IA Controls beyond the two basic ones above. These include:

- DCCT-1 - Compliance Testing
- DCHW-1 - Hardware Baseline
- DCID-1 - Interconnection Documentation
- DCII-1 - IA Impact Assessment
- DCSW-1 - Software Baseline

As evidence of compliance with the CM requirements, you should include your CM Plan and CCB Charter in your package of DIACAP supporting documentation (artifacts). In addition, you should also include evidence for the validator that your CM program is *actually functioning*, e.g., CCB meeting minutes, change control logs, etc.

A strong CM program alone will not guarantee that your system will be secure, but a weak CM program virtually guarantees security will *not* be maintained.

### **Knowledge Service from page 1**

personnel and non-CAC holders to gain authorization. Note that all DIACAP Knowledge Service users will be required to set up an account on the Navy Enterprise Single Sign-on (NESSO); this is a simple on-line process that takes just a few minutes.

Once you've gained access to the DIACAP Knowledge Service, you'll see a familiar web-based interface. The site is built around Microsoft Sharepoint technology, which means you have the ability to "subscribe" to the site and receive e-mail notifications when selected pages are updated or changed.

Several areas of the site are of particular note:

- The News page is updated each time there are changes to the site, so this is a good place to look whenever you log on.
- The IA Controls section contains the full text of all the DoDI 8500.2 IA Controls, as well as implementation guidance, validation procedures, and impact codes.
- The Contacts page gives the phone number and e-mail address for the DoD-operated DIACAP Help Desk.
- The Message Boards section is your place to post questions and receive answers and suggestions from your peers.

We encourage you to check out the DIACAP Knowledge Service soon.

---

*"...a fully-functional CM program includes formally-documented roles, responsibilities and procedures ..."*

---



Our National Capital Region  
instructional services partner  
([www.simplexdatasolutions.com](http://www.simplexdatasolutions.com))

**Top Ten from page 2**

selected from the Department of Defense (DoD) 8500.2. Security controls listed as In-Place on the DIP should be traceable to a supporting artifact. Additionally, security controls identified on the POA&M should be traceable to a “Planned” requirement on the DIP.

3. Inaccuracy - Accurately reporting compliance is more important than a “perfect score.” Writing precise C&A documentation is not an easy task, but is necessary to demonstrate compliance with IA controls. Concise documentation allows the team to focus their energy on managing risk rather than formatting reports.

## DIACAP Training for 2008

By Lon J. Berman

The DIACAP Resource Center continues to offer our *DIACAP Fundamentals* (one day) and *DIACAP In Depth* (three day) training courses on a regularly-scheduled, monthly basis in the National Capital Region (Northern Virginia).

Regularly-scheduled classes in the National Capital Region for the remainder of 2008 are as follows:

DIACAP Fundamentals (one day)	DIACAP In Depth (three days)
5 May	6-8 May
2 June	3-5 June
7 July	8-10 July
4 August	5-7 August
8 September	9-11 September
6 October	7-9 October
3 November	4-6 November
8 December	9-11 December

**DIACAP Dimensions** is published by the DIACAP Resource Center, a division of BAI Information Security Consultants, 7467 Bluff View Drive, Fairlawn, VA 24141.

**Phone:**  
540-808-1050

**Fax:**  
540-808-1051

**E-mail:**  
diacap@diacap.net

2. Integrity - Personnel associated with the C&A must provide honest answers in order to accurately document the status of each security requirement. Less-than-truthful responses may lead to unforeseen risks being identified during the certification phase of the process.

1. Loss of focus - C&A is not about producing large documents with thousands of pages of description. C&A is not about racing to create POA&Ms to silence OMB. *C&A is all about identifying and reporting risk.*

For customers in other locations, 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 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 and logistical issues 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](mailto:diacap@diacap.net) to request an on-site training quotation.

To register for our regularly-scheduled training in the National Capital Region, please visit our website at [www.diacap.net](http://www.diacap.net) and download a Registration Form. Then, simply e-mail or FAX the completed Registration Form to reserve your seat! *Coming soon ... on-line registration!*

### PARTNERS WANTED

If your company is in the Information Assurance business and you have a classroom facility at your office location, we would like to speak with you regarding partnering opportunities. We are actively seeking partner firms in various locations throughout the country who are interested in hosting DIACAP training as well as our other IA training products. Please contact Training Director Lon Berman at 540-808-1050 or [diacap@diacap.net](mailto:diacap@diacap.net).