



DIACAP Dimensions

January
2009

DIACAP Resource Center ▪ www.diacap.net ▪ E-mail: diacap@diacap.net ▪ Phone: 540-808-1050

Online registration is available for all upcoming DIACAP classes! Please visit www.diacap.net/registration.asp.

New Training Sites to Debut in 2009

By Lon J. Berman

INSIDE THIS ISSUE

- 1 New Training Sites to Debut in 2009
- 1 C&A Transformation – the Saga Continues
- 2 Top Ten List – DIACAP “Urban Legends”
- 3 IA Control Spotlight – Inheritance
- 4 2009 DIACAP Training Schedule

Two new DIACAP training sites will begin operation in the first half of 2009! The DIACAP Resource Center has partnered with Sparta, Inc. (www.sparta.com) and ManTech International (www.mantech.com) to begin offering *DIACAP Fundamentals* and *DIACAP In Depth* training in Huntsville and San Antonio, respectively.

The first DIACAP training classes in Huntsville will be held the week of March 23, and in San Antonio the week of April 6.

In addition to these new sites, we continue to offer DIACAP training in the National Capital Region and in Colorado Springs.

Although they have not yet been scheduled, we do expect to offer additional classes in both of these new locations in the second half of the year. These will be announced on the website, www.diacap.net, as soon as they are scheduled and available for registration.

Please see *New Sites* on page 2

C&A Transformation – the Saga Continues

By Lon J. Berman

In the last issue of *DIACAP Dimensions*, we reported on the *Joint Task Force Transformation Initiative Interagency Working Group* and the progress being made toward a unified government-wide C&A process.

NIST Special Publication 800-37, Revision 1, entitled *Guide for Security Authorization of Federal Information Systems - A Security Life Cycle Approach*, describes what may soon become the government-wide standard for C&A. A draft of this document is available from NIST: <http://csrc.nist.gov/publications/drafts/800-37-Rev1/SP800-37-rev1-IPD.pdf>. Once this document is finalized, it is hoped that all three “segments” of the Executive Branch, i.e. DoD, the “civilian” departments/agencies, and the intelligence community, will finally agree upon a single C&A process and a single set of controls (security requirements).

Please see *Transformation* on page 3

“...agree upon a single C&A process and a single set of controls...”

Top Ten List – DIACAP “Urban Legends”

By Jeffrey H. Widom

Even though it is only a couple of years old, DIACAP is already the subject of a multitude of “stories”, some of them true, some of them outright lies, and others somewhere in between. Here are ten of our favorite “myths” surrounding the C&A process in general, and DIACAP in particular.

“C&A is still your responsibility as a program manager...”

10. *I can't get a 3 year accreditation anymore, DIACAP requires my system to be reaccredited annually.* Not true! Under DIACAP, accreditation (ATO) can be issued for any period, up to three years. FISMA requires an annual IA Review, not a reaccreditation.

9. *I don't have to test my system, a trained “certifier” will do it for me.* Not true! DIACAP does require trained certifiers to be used, but every program manager should be testing his system well in advance of the certifier's visit.

8. *I don't need to worry about C&A for my system, my hosting site will take care of it as part of their accreditation.* Not true! You may inherit many controls from your hosting provider, but C&A is still your responsibility as a program manager.

7. *I don't need accreditation for my system; it is a tactical system using “embedded” processors rather than conventional servers, desktops or laptops.* Not true! If your system connects to any government network, it is considered as a “Platform IT Interconnection” and requires C&A just like any other system.

6. *I don't need to go through C&A on my system; I can just ask the vendor I am buying it from to provide their “DIACAP Certificate”.* Not true! Commercial vendors do not hold DIACAP Certificates! You can and should ask your suppliers for support, but the C&A process is still your responsibility.

5. *All the security requirements for my system are listed in DoDI 8500.2.* Not

Please see *Top Ten* page 4



Our San Antonio area training site partner (www.mantech.com)

New Sites from page 1

Training at several additional sites is in the planning stages. New classes will be announced on the website as soon as the dates and locations are finalized.

DIACAP Resource Center is actively seeking partner companies in other major markets. If your company is in the information technology or information assurance business and you have a suitable classroom facility at your office location, we would like to speak with you regarding partnering opportunities. We would like to find partners 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, to discuss partnering opportunities.

IA Control Spotlight – Inheritance

By Jeffrey H. Widom

According to DoDI 8510.01, the DIACAP instruction, Inheritance refers to situations where IA controls, along with their validation results and compliance status, are shared by two or more systems for the purpose of C&A. Inheritance eliminates the need for redundant testing and documentation of inherited IA controls.

The most common inheritance situation occurs when an AIS Application, consisting of hardware and software, is hosted within a data center or other hosting enclave. The AIS Application will inherit most of the physical, environmental, and network boundary defense controls from the hosting site.

It is important to recognize that inheritance does not absolve the system owner of the responsibility to comply with all applicable controls. It merely simplifies the process of validating and documenting compliance. If the hosting enclave is not compliant with a particular control, that non-compliance should be reflected on the application's DIACAP Scorecard and POA&M.

Inheritance of IA controls is a topic that should be covered explicitly in Memoranda of Agreement, Service Level Agreements, or other hosting documents. Application owners should be fully informed of exactly which controls are to be provided by the hosting enclave. Hosting enclaves should disclose their DIACAP Scorecard and POA&M to prospective hosting customers so that they will be fully informed of the enclave's ability to comply. Where feasible, application owners may implement additional controls to compensate for non-compliance on the part of the enclave owner.

Transformation from page 1

Another major step forward in this transformation has occurred with the publication of Intelligence Community Directive (ICD) 503. This document orders the intelligence community to immediately replace its existing C&A process (DCID 6/3) with a process based on the NIST Risk Management Framework (i.e., the new NIST 800-37).

Once ICD 503 has been fully implemented within the numerous agencies that comprise the intelligence community, DoD will be left as the only segment of the Executive Branch with its own “proprietary” C&A process. It is inevitable that we will soon begin to see a transition from the existing DIACAP process to something more closely resembling the NIST process.

At this point it is not clear if DoD will opt for a “whole hog” adoption of the NIST process, as the intelligence community has done, or will initiate some sort of evolutionary series of changes to DIACAP to bring it in line with the civilian and intelligence sectors. Regardless of what DoD decides to do, DIACAP Resource Center will be ready with the training and support you need to be successful. Our DIACAP training materials have been frequently updated to keep up with changes, and we will continue to monitor the situation and make further updates as necessary. Our *Federal C&A Resource Center* affiliate already provides training to civilian agencies in the NIST C&A process, so we are “ready to go” in the event DoD mandates a wholesale change in their C&A program.

*“...the MAC level affects
the operational readiness
... and cost...”*



Our Huntsville area training site
partner (www.sparta.com)

Top Ten from page 2

true! DoDI 8500.2 lists the minimum requirements (controls). Other requirements are levied at the component, command, or even local level.

4. *There is no urgency to complete the C&A process. All I have to do is send a memo to the DAA and he/she will issue an IATO.* Not true! DAAs should not be granting IATOs without adequate testing and a POA&M showing a plan to address risks.

3. *I have no money budgeted for C&A, so my system will be fielded without it.* Not true! As a program manager,

budgeting for C&A is your responsibility.

2. *I can wait until my system is ready for fielding to worry about C&A activities.* Not true! DIACAP is a lifecycle activity that must be initiated early to be successful.

1. *There is so much less paperwork with DIACAP. I don't need to worry about Contingency Plans, Incident Response Plans, etc.* Not true! These items are no longer explicit C&A deliverables, but they are still very much required in order to be compliant with the DoDI 8500.2 IA controls.

2009 DIACAP Training Schedule

By Lon J. Berman

In 2009, the DIACAP Resource Center will continue to offer our *DIACAP Fundamentals* (one day) and *DIACAP In Depth* (three day) training courses on a regularly-scheduled basis in the National Capital Region, Colorado Springs, Huntsville, and San Antonio.

Regularly-scheduled classes for the first half of calendar year 2009 are as follows:

DIACAP Fundamentals (one day)	DIACAP In Depth (three days)
2 February (NCR)	3-5 September (NCR)
2 March (NCR)	3-5 March (NCR)
9 March (CS)	10-12 March (CS)
23 March (H)	24-26 March (H)
6 April (NCR and SA)	7-9 April (NCR and SA)
4 May (NCR)	5-7 May (NCR)
1 June (NCR)	2-4 June (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 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 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 e-mail.

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

NIST C&A PROCESS TRAINING

Training is also available in the NIST C&A process for federal “civilian” agencies. This process has now taken on additional importance as it forms the basis of the forthcoming “unified”, government-wide Security Authorization (C&A) process. For information on our *Federal C&A Fundamentals* and *Federal C&A In Depth* classes, please visit www.fedca.org.