



DIACAP Dimensions

Sept. 2007

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

Happy Birthday DIACAP!

By Lon J. Berman

On July 6, 2007, DIACAP celebrated its first birthday. What sort of progress has been made in the past year?

INSIDE THIS ISSUE

- 1 Happy Birthday DIACAP!
- 1 C&A Training Opportunities Expand
- 2 Kickoff Meeting – Key to DIACAP Success
- 3 IA Control Spotlight
- 4 DIACAP for Product Vendors?

- Major DoD components have published DIACAP implementation guidance
- DoD components have put in place (or are in the process of putting in place) new organizational structures (e.g., CA structure) in support of DIACAP
- DoD has updated the DIACAP Knowledge Service website on a quarterly basis
- Hundreds of DoD employees and contractors have completed one or both of our DIACAP training courses

In all major initiatives, there are inevitably a few disappointments to go

Please see *Birthday* on page 2

C&A Training Opportunities Expand

By Lon J. Berman

The DIACAP Resource Center is proud to announce the expansion of federal C&A training opportunities to civilian agencies and the intelligence community. The *Federal C&A Resource Center* now offers training courses specifically geared to the NIST-FISMA (civilian) and DCID 6/3 (intelligence) Certification and Accreditation processes.

Following the successful pattern of our DIACAP training program, we are now offering both one-day (*Federal C&A Fundamentals*) and three-day (*Federal C&A In Depth*) courses focusing on the NIST 800-37 C&A process, sometimes called the “FISMA process.” This is the C&A process that has been adopted by most federal civilian departments and agencies.

Federal C&A Fundamentals and *Federal C&A In Depth* are offered on a regularly-scheduled monthly basis in the National Capital Region. Please

Please see *New Courses* on page 3

“... expansion of training opportunities to civilian agencies and the intelligence community.”

Kickoff Meeting – Key to DIACAP Success

By Jeffrey H. Widom

A quality “kickoff meeting” can be the key to a successful DIACAP effort. Our Top Ten List can help you get your DIACAP projects off to a good start.

10. Establish an agenda and keep the meeting on point.

9. Do not turn the kick-off meeting into a debate. The kickoff meeting is not the time or place to wrangle over the status of specific security requirements. Focus on the System Identification Profile, Security Test and Evaluation Costs and Milestones, and establishing a rapport among the key security personnel.

8. Ask questions! Talk to the Designated Approving Authority Representative and Certifying Authority Representative. For example, ask the Certifier to provide a generic or template Security Test and Evaluation Plan in order to verify the local DIACAP Implementation Plan is accurate. Verify with the Certifier the amount of time and cost to complete the Certification. Finally, determine the time required for the Designated Approving Authority to review the Certification and Accreditation package.

7. Do not schedule the meeting until you are ready, but do not wait too long. There is no ideal date. Instead, the goal is to ensure the meeting is held before a security requirement may impact the development of the system or application being accredited.

6. Invite the right personnel. More people in the room does *not* demonstrate readiness. Completing a draft DIACAP Implementation Plan should provide a level of confidence to the security team.

5. Complete an initial draft of the DIACAP implementation plan. Establish initial responsibilities and resources required to meet each requirement just in case the Certifier or Designated Approving Representative has questions.

Please see *Kickoff* page 4

“Invite the right personnel. More people in the room does not demonstrate readiness.”



Our National Capital Region training
site partner (www.intelligent.net)

Welcome from page 1

along with the progress. DIACAP is no exception:

- The “final” DoDI 8510.bb DIACAP Instruction has yet to be released, so we are still operating under the “Interim Guidance” published in July 2006
- Deployment of eMass (the DoD-wide database and toolset in support of DIACAP) has been very slow at best
- DoD components have yet to publish their own sets of IA Controls to supplement DoDI 8500.2

All in all, it’s been an eventful year, and we look forward to new developments yet to come.

IA Control Spotlight

By Jeffrey H. Widom

IA Control ECSC-1 consists of a single, very short statement: *For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.*

“DoD security configuration or implementation guides” generally refers to the DISA Security Technical Implementation Guides (STIGs) that are available for most major operating systems, databases, etc. A STIG contains detailed guidance and recommendations for configuring a particular product. Many of the STIGs are complemented by a software tool, such as the Windows Gold Disk, that can “automatically” assess compliance with the settings recommended in the STIG.

What exactly does it mean when we say that a given STIG has “been applied”? Does it mean that every recommended configuration setting has been implemented? The answer is an emphatic *NO*. In most cases, it is not possible to implement 100% of the settings recommended by the STIG because doing so will compromise the functionality of the application or system. The best strategy for “applying” STIGs is:

- Read and understand the STIG
- Analyze the recommended settings and determine which ones are feasible; use a test system to verify.
- Implement all settings that are found to be feasible, and document the justification for those that were not implemented.

New Courses from page 1

contact us at 540-808-1050 for further information and registration.

The *Federal C&A* training schedule for the remainder of 2007 is as follows:

FedC&A Fundamentals (Monday)	FedC&A In Depth (Tuesday - Thursday)
Nov 12	Nov 13-15
Dec 10	Dec 11-13

The *Federal C&A* training schedule for calendar year 2008 will be announced soon.

Federal C&A training can also be arranged “on site” for groups nationwide. Please contact us for further details and to request a quotation.

In addition, we are pleased to announce a three-day “in depth” course focusing on the *DCID 6/3 C&A* process used by the intelligence community and by DoD systems that process Sensitive Compartmented Information (SCI). This course will only be available “on site”, for pre-arranged customer groups. If you are interested in bringing this training to your site, please contact us.

“... it is not possible to implement 100% of the settings recommended by the STIG ...”



Our National Capital Region
instructional services partner
(www.simplexdatasolutions.com)

Kickoff from page 2

4. Complete the System Identification Profile. The profile should have all major areas filled-in including the registration number if available.

3. Be prepared. Have a strong presentation document that provides a description of the C&A project including an overview of the system, names and contact information for the key players, keys to success, C&A overview, and schedule/milestones. The presentation should look professional and demonstrate your ability to produce a quality C&A package.

2. Be confident. The System Owner and Security Officer should demonstrate to the Certification Authority and Designated Approving Authority that they are fully prepared for the C&A.

1. Know the System! Know the Boundary! The C&A kickoff meeting is not the time to engineer the system. The System Owner and Security Officer must have a clear understanding of the system components and be able to delineate the boundary to the Certifier and DAA representatives.

DIACAP for Product Vendors?

By Lon J. Berman

As DIACAP consultants and trainers, we get numerous phone calls and e-mail messages with questions about the DIACAP process. Many of these come from manufacturers and vendors who sell, or wish to sell, their products and services to DoD. Often their question is something like “how do I go about getting my product (or service) DIACAP certified?”

Well, the short answer, Mr. or Ms. Vendor, is “You can’t!”

There are two fundamental reasons:

1. DIACAP is a *system* certification process, not a *product* certification process
2. DIACAP is initiated and carried out by the government customer, not by the vendor

Unlike other government-sponsored certification programs you may have heard of (e.g., Common Criteria, FIPS 140-2), vendors cannot independently seek certification of their products or services under DIACAP. Rather, the intended government end-user is required to

seek DIACAP accreditation of the system or network that is to contain the vendor’s product.

In some cases, this will mean updating the existing accreditation of a system or network to include the new product(s). In other cases, the vendor’s products may be considered as a system unto themselves and an entirely new DIACAP effort must be initiated.

In either event, the new products or services must be assessed for compliance with the applicable IA controls (requirements). The government end-user will need the assistance and support of the vendor in order to do this kind of evaluation, so the slightly longer (and more accurate) answer to the original question is “**You can’t do it alone!**”

As a vendor, you can be prepared for DIACAP in several ways:

- Educate yourself on the process and your role in it (our DIACAP training courses are a good start!)
- Conduct your own evaluation of your product’s compliance with the DoD 8500.2 IA Controls, and document the results. Having this kind of documentation can sometimes be instrumental in making that big government sale!

DIACAP Resource Center can provide consulting services to assist you in evaluating your product’s compliance and in helping you to work effectively with your government customers on IA issues.

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