



DIACAP Dimensions

April, 2007

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

Welcome to our Newsletter

By Lon J. Berman

This newsletter, *DIACAP Dimensions*, is our latest project here at the DIACAP Resource Center. We hope to be able to provide you with information that will help you along as you proceed in your DIACAP efforts.

Some of the things we have in mind are:

- News about DIACAP policies and process from DoD, and the various DoD components
- News about our DIACAP training courses
- What's new on the DIACAP Knowledge Service and updates on *eMass* availability
- Advice and "helpful hints" on implementing and validating the IA controls, preparing the DIACAP documentation package, etc.

Please see *Welcome* on page 2

INSIDE THIS ISSUE

- 1 Welcome to our Newsletter
- 1 Training Schedule and New Site
- 2 Keys to a Smooth Transition
- 3 IA Control Spotlight
- 4 DIACAP Training Comes to You!

Training Schedule and New Site

By Lon J. Berman

The DIACAP Resource Center is proud to announce the DIACAP Training schedule for the remainder of 2007. We will continue to offer both of our courses, *DIACAP Fundamentals* (one day) and *DIACAP In Depth* (three days) on a monthly basis in the National Capital Region.

We have entered into a "partnership" with Intelligent Decisions (ID), a leading supplier of information technology security products and services. Beginning in April, 2007, our monthly training courses in the National Capital Region will be conducted at ID's beautiful facility in Ashburn, Virginia.

The new training site is larger and more comfortable, yet still within minutes of Washington Dulles International Airport. In spite of the additional space, we will continue to keep our classes small, so they

Please see *Training Schedule* on page 3

"The new training site is larger and more comfortable, yet still within minutes of Washington Dulles International Airport."

Keys to a Smooth Transition

By Jeffrey H. Widom

Whether you're responsible for a single system or an entire organization, transitioning from DITSCAP to DIACAP doesn't have to be a nightmare. With apologies to a well-known late night TV host, here is my personal "Top Ten List" of keys to a smooth transition.

"... transitioning from DITSCAP to DIACAP doesn't have to be a nightmare."

10. "Understand the Concept" - Training is a cost effective method of improving an organization's ability to comply with DIACAP.

9. Artifacts - DIACAP has streamlined the reporting requirements for Certification and Accreditation. Documentation (Appendices) originally required by DITSCAP are now considered artifacts and must be developed to comply with specific DoD 8500.2 security requirements.

8. Identify Security Policies - Although DIACAP has established a minimum set of security requirements, DoD Component and local level security policies must be addressed in the DIACAP Implementation Plan and Scorecard.

7. Accurate POA&M - Developing an accurate Plan of Action and Milestones (POA&M) early in DIACAP will improve traceability and help you to accurately track the status of security relevant issues throughout the system life cycle.

6. Security Budget - Financing of security functionality must be included in the system life cycle and accurately documented in the POA&M when applicable.

5. Annual Review - DIACAP requires an annual review of the security controls, which should be scheduled well in advance to ensure maximum participation.

4. Effective Kick-off meeting - Establishing an effective kick-off meeting agenda will improve the ability to complete the System Identification Profile (SIP), assign roles and responsibilities, and schedule future activities.

3. Identify the Certifier - Unlike DITSCAP, DIACAP has "formalized" the role of

Please see *Smooth Transition* page 4



Welcome from page 1

We would also like to include short articles from you, our readers, recounting your DIACAP experiences, "what to do", "what not to do", etc. Please contact us with your ideas. We'd love to talk to you.

If you have friends and colleagues you think would benefit from receiving *DIACAP Dimensions*, please send us their e-mail addresses and we'll be happy to include them on our subscription list.

Conversely, if you no longer wish to receive *DIACAP Dimensions*, please let us know and we will promptly remove you from our list. We certainly don't want you to think of us as one of those annoying "spammers". ☺

Finally, if there is anything else we can do to make this newsletter better, please don't keep it to yourself. Let us know and we will make every effort to address your suggestions.

IA Control Spotlight

By Jeffrey H. Widom

One of the most complex and easily misunderstood IA Controls in DoDI 8500.2 is IAIA-1, entitled “Individual Identification and Authentication.”

If you examine this IA Control carefully, you’ll find it can be separated into as many as 15 unique “requirements”. These include technical requirements, such as password complexity and automatic expiration, as well as procedural requirements such as in-person registration and password-sharing prohibition.

Implementing (or validating) IAIA-1 is made even more complex by the fact that many of these requirements may be implemented differently across various components of the system. For example, the typical web-based system will have an application interface where ordinary users log in, as well as numerous other components (e.g., databases, operating systems) where privileged users log in to perform their duties. Technical and procedural requirements of IAIA-1 must be implemented and validated for each of these “instances”.

Further complexity is introduced by various DoD component-level security policies that are more stringent than some of the provisions of IAIA-1. As an example, the Army requires passwords to be a minimum of 10 characters long, rather than 8 as stipulated in IAIA-1.

The lessons here are: a) read each of the IA Controls carefully; and b) give serious thought to the applicability of the IA Control before jumping to any conclusion as to whether or not it has been fully implemented.

“IAIA-1 ... can be separated into as many as 15 unique requirements.”

Training Schedule from page 1

remain “informal” and encourage interaction among our students.

Students who bring their laptops to DIACAP class will enjoy wireless internet access from the training room, so they can easily keep up with e-mail and other business on the home front.

The training schedule for the remainder of 2007 is as follows:

DIACAP Fundamentals (Monday)	DIACAP In Depth (Tuesday - Thursday)
May 7	May 8-10
June 4	June 5-7
July 9	July 10-12
August 6	August 7-9
September 10	September 11-13
October 1	October 2-4
November 5	November 6-8
December 3	December 4-6



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

Smooth Transition from page 2

Certification Authority. Early in the process, you should contact the Senior IA Official (SIAO) of your DoD component to arrange for a person or organization to perform the certification testing of your system.

2. Security Requirements Review - Establish a recurring schedule to review the Implementation Plan and POA&M for accuracy. Review may include internal testing using approved automated tools such as password checks and vulnerability scanners.

1. Assign Responsibility - It is important to ensure the proper resources are allocated for each security control listed in the Implementation Plan. Assigning responsibility early in DIACAP will improve the ability for the organization to properly document the status of each requirement.

Following these guidelines will help you spend more of your evenings watching those late-night talk shows and less time “burning the midnight oil” on yet another DIACAP deadline!

DIACAP Training Comes to You!

By Lon J. Berman

Technical training is essential in today’s world, but, like so many valuable things, it is expensive. There are three components that contribute to the cost of training to your organization:

- **Training fees.** This is the easy part. All training providers publish their schedule of fees. Sometimes discounts are offered if you send a group of trainees to the same class.
- **Travel expenses.** If your staff requires “out of town” training, the cost of air travel, hotels, meals, etc., often represents a significant portion of the total expense.
- **Hidden cost.** You can’t afford to ignore the cost of having your staff away for training days. If training is in a distant location, they may “lose” extra days for travel. If this wasn’t factored into your project plan, you may find yourself temporarily behind schedule. Hopefully, knowledge gained by your staff from their training experience will help “make up” for the lost time.

Here at the DIACAP Resource Center, we’re trying to “do our part” to help ease the training expense burden. One of the best “tools” we can offer is to bring our DIACAP training classes to you! **With a minimum commitment of 8 to 10 students, we will arrange to send an instructor to your site to deliver one or both of our classes: *DIACAP Fundamentals* and/or *DIACAP In Depth*.** All you need to provide is a suitable classroom facility, preferably including a projector and screen.

With an “on site” class, travel expenses are effectively eliminated, as are extra “lost days”. Our pricing structure offers very favorable “per student” rates as well, especially with “larger” class sizes.

Arranging an “on site” DIACAP class is easy! Call us at 540-808-1050 and ask for a Request For Quotation (RFQ). It should take only minutes to complete. Send us your completed RFQ and we will respond promptly with a quote.

To make things as simple as possible for you, our quoted prices include all instruction fees, training materials, and instructor travel.

To ensure the best choice of available dates, please contact us as soon as possible. Let us show you how an “on site” DIACAP training program can work for you!

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