



DIACAP Dimensions

June
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.

DIACAP Training Expansion Continues

By Lon J. Berman

The DIACAP Resource Center will be opening a new training site in Tampa, Florida during the second half of 2009. We have partnered with FishNet Security (www.fishnetsecurity.com) to begin offering DIACAP training in Tampa, with the first classes scheduled for the week of September 14, 2009. The new site is conveniently located just minutes from the Tampa International Airport; please visit www.diacap.net to download a map of the site, including airport and hotel information.

The initial course offering in Tampa will include *DIACAP Fundamentals* (one-day class) on Monday, September 14, following by *DIACAP In Depth* (three-day class) on Tuesday through Thursday, September 15-17.

With the opening of the Tampa site, we now have a total of *five* DIACAP training sites in operation, including the National Capital Region (our flagship site), Colorado Springs, Huntsville, San Antonio, and Tampa.

Please see *Training Expansion* on page 2

INSIDE THIS ISSUE

- 1 DIACAP Training Expansion Continues
- 1 Risk Management Framework (RMF)
- 2 Top Ten List – Maintaining your ATO
- 3 IA Control Spotlight – “IA and IA-enabled”
- 4 2009 DIACAP Training Schedule

“...Risk Management framework will form the basis of the unified process...”

Risk Management Framework (RMF)

By Lon J. Berman

This is the latest in a series of *DIACAP Dimensions* articles discussing the ongoing transformation to a unified C&A process covering the Department of Defense (DoD), the Intelligence Community (IC), and the federal “civilian” departments/agencies, e.g., Dept. of State, Dept. of Homeland Security, Dept. of Treasury, etc.

The National Institute of Standards and Technology (NIST) has recently begun publishing a series of documents describing a *Risk Management Framework* (RMF) that will form the basis of the unified process.

The RMF is comprised of six major steps:

Step 1: **Categorize** the information system and the information resident in the system based on impact.

Please see *RMF* on page 3

Top Ten List – Maintaining your ATO

By Jeffrey H. Widom

DIACAP activities do not end when the DAA signs an Authority To Operate (ATO). Once your system is fully accredited, there are numerous steps you'll need to be taking *on a continual basis* to maintain that accreditation. Here is our “top ten list” for ATO maintenance

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

10. *Make sure your system is regularly scanned for vulnerabilities.* Your installation Information Assurance Manager (IAM) should have an established vulnerability management program, but you need to make sure your systems are included in any regularly-scheduled scanning activities.

9. *Subscribe to the IAVA mailing list.* Be sure you are receiving the latest Information Assurance Vulnerability Alerts (IAVAs) from DoD or your component IA program.

8. *Keep all commercial software up-to-date with the latest patches.* Keeping current with vendor-released patches is the best way to ensure you are “ahead of the curve” when IAVAs are released.

7. *Report your IAVA compliance.* Work with your installation IAM to ensure your compliance with IAVAs is promptly reported to your component IA program.

6. *Plan ahead for Annual IA Review.* Annual IA Review planning should start 90 days before the anniversary date of your ATO. This will give you plenty of time to ensure the appropriate resources are available for things like Contingency Plan and Incident Response Plan testing.

5. *Plan ahead for reaccreditation.* Reaccreditation planning should start 180 days before the Authorization Termination Date (ATD) of your ATO. This will give you sufficient time to engage all members of the DIACAP team (e.g., DAA and CA), ensure that the DIACAP package is updated, and a certifier is engaged to test the system.



Our Tampa area training site partner (www.fishnetsecurity.com)

Please see *Top Ten* page 4

Training Expansion from page 1

Registration for training at all sites is available on our website, www.diacap.net/registration.asp.

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.

We continue to seek partner companies in other locations around the country, particularly those in close proximity to major military installations. If your company is in the information technology or information assurance business and you have a suitable classroom or conference facility available 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 – “IA and IA-enabled”

By Jeffrey H. Widom

The terms “IA and IA-enabled products” are used several times in the DoDI 8500.2 baseline IA controls. It’s important to have a clear understanding of these terms in order to ensure compliance.

An *IA Product* is one whose primary function is to support some aspect of security policy. Examples of IA products are firewalls and intrusion detection systems (IDA). In addition, cross-domain “guards” (devices for connecting systems at different classification levels) are also considered as IA products.

An *IA-enabled Product* is one whose primary function is something other than security, but additionally supports security policy in the course of performing its primary duty. An operating system is the principal example of an IA-enabled product. For example, the principal function of an operating system is to support applications by providing access to the system hardware devices, network, etc. However, in performing said functions, the OS also has a significant IA role. The OS supports Identification and Authentication through its logon functionality, Access Control through its file system and permission structure, and Auditing through its logging capabilities. Likewise, Database Management Systems and Web Servers are also considered as IA-enabled products.

The baseline IA Controls in DoDI 8500.2 levy specific requirements upon IA and IA-enabled products. The two principal requirements are:

- All IA and IA-enabled products must be Common Criteria certified
- A Security Technical Implementation Guide (STIG) or equivalent must be used to configure all IA and IA-enabled products.

RMF from page 1

Step 2: **Select** an initial set of security controls for the system based on the categorization and the minimum security requirements; apply tailoring guidance and supplement the controls as necessary.

Step 3: **Implement** the security controls in the information system.

Step 4: **Assess** the security controls using appropriate methods and procedures.

Step 5: **Authorize** information system operation based on a determination of risk and the decision that the risk is acceptable.

Step 6: **Monitor** and assess security controls in the information system on a continuous basis, and report regularly on the system’s security status.

Numerous NIST Special Publications and Federal Information Processing Standard (FIPS) publications are available to support each of these steps. Of particular note is NIST Special Publication (SP) 800-53, which is currently undergoing revision. The latest draft (Rev. 3) is now available for comment. The goal is to produce a unified “Security Controls Catalog” that can be applied to all systems across the DoD, IC, and civilian agencies. Another very interesting development is the “retirement” of the term “Certification and Accreditation” in the latest round of NIST documents, in favor of the new term “Security Authorization”.

How and when will DIACAP be affected by these changes? Stay tuned!

“An IA-enabled product is one whose primary function is something other than security...”



For the latest publications and news, see the NIST website src.nist.gov

Top Ten from page 2

4. *Evaluate all proposed changes for IA impact.* Make sure to engage the CA and DAA if there is any likelihood that a proposed change might be considered a “major change” requiring reaccreditation.

3. *Use your incident response plan when necessary.* Make sure all security incidents are properly managed and reported.

2. *Review your system audit logs regularly.* Not only is weekly audit review required by DoD, it is also one of the best ways to monitor the “health” of your system

DIACAP Training Schedule

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 basis in the National Capital Region, Colorado Springs, Huntsville, San Antonio, and Tampa.

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

| DIACAP Fundamentals (one day) | DIACAP In Depth (three days) |
|---|---------------------------------|
| 13 July (NCR) | 14-16 July (NCR) |
| 20 July (H) | 21-23 July (H) |
| 10 Aug (NCR) | 11-13 Aug (NCR) |
| 14 Sept (NCR and T) | 15-17 Sept (NCR and T) |
| 21 Sept (SA) | 22-24 Sept (SA) |
| 5 Oct (NCR) | 6-8 Oct (NCR) |
| 2 Nov (NCR) | 3-5 Nov (NCR) |
| 7 Dec (NCR) | 8-10 Dec (NCR) |
| (NCR) = National Capital Region (CS) = Colorado Springs (H) = Huntsville (SA) = San Antonio (T) = Tampa | |

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

and spot problem areas before they become serious incidents.

1. Practice good Configuration Management. Good CM practice is the single most important element in maintaining your accreditation. You should always have up-to-date documentation and control over your hardware and software assets. Remember, all DoD information systems are subject to audit by numerous organizations such as CIO, IG, etc. Good documentation and a solid CM program will help you get through any audit with “flying colors”.

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. Payment arrangements include credit cards, SF182 forms, or Purchase Orders.

NIST C&A PROCESS TRAINING

Training is also available in the NIST 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 (C&A) process. For information on our *Federal C&A Fundamentals* and *Federal C&A In Depth* classes, please visit www.fedca.org.