



# DIACAP Dimensions

November  
2009

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

Online registration is available for all upcoming DIACAP classes! Please visit [www.diacap.net/registration.asp](http://www.diacap.net/registration.asp).

## DIACAP Training Continues in 2010

By Lon J. Berman

The DIACAP Resource Center is pleased to continue our popular DIACAP Training program in 2010. Once again, we will be offering our one-day *DIACAP Fundamentals* and three-day *DIACAP In Depth* classes at our training sites in the National Capital Region, Colorado Springs, Huntsville, San Antonio and Tampa. Training dates have now been published for the first half of 2010.

We are also proud of the continued relationships with our training site partners: Intelligent Decisions, Inc. (National Capital Region); Integral Systems, Inc. (Colorado Springs); Cobham Analytic Solutions (Huntsville); ManTech International (San Antonio); and FishNet Security (Tampa).

Registration for training at all sites is available on our website, [www.diacap.net/registration.asp](http://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.

Please see *2010 Training* on page 2

### INSIDE THIS ISSUE

- 1 DIACAP Training Continues in 2010
- 1 Annual IA Review
- 2 Top Ten List – DIACAP Documentation Hints
- 3 IA Control Spotlight – Physical Security
- 4 2010 DIACAP Training Schedule

## Annual IA Review

By Lon J. Berman

The Federal Information Security Management Act (FISMA) mandates an annual review of the security compliance status of all federal information systems. This Annual IA Review is an integral part of DIACAP Activity 4 - Maintain Accreditation and Conduct Reviews.

The annual review mandate is also included in DoD Instruction 8500.2 in the form of IA Control DCAR-1, which states: “An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.”

Unlike the initial certification, the Annual IA Review can be a *Self-Assessment*; an independent “certification agent” is not required. The Information Assurance Manager (IAM) and Program Manager/System

---

“...the Annual IA Review  
can be a Self-  
Assessment...”

---

Please see *Annual Review* on page 3

## Top Ten List – DIACAP Documentation Hints

By Jeffrey H. Widom

The DIACAP Comprehensive Package consists of the following documents: System Identification Profile (SIP); DIACAP Implementation Plan (DIP); DIACAP Scorecard; Plan of Action and Milestones (POA&M); plus supporting documentation (artifacts). Here is our “top ten list” for DIACAP documentation development and maintenance:

10. *Use a document management system, if available.* Documentation maintenance will be much easier with a document management system that includes checkin/checkout and version control.

9. *Use approved templates where available.* Some components and commands use standardized templates for certain DIACAP documents. Be sure to coordinate with your CA and/or DAA to obtain templates for documents such as the SIP and POA&M.

8. *Keep documents updated regularly throughout the development process.* The DIACAP package should be the “one stop shop” for the latest information on implementation of security features.

7. *Use the DIP as a tracking tool.* Review the DIP at regular DIACAP team meetings to monitor progress.

6. *Update the POA&M quarterly.* POA&Ms should be updated quarterly and submitted to the component IA program for review.

5. *Keep the Contact List current in the SIP.* The Contact List should include key individuals beyond the “mandatory” DIACAP team members (e.g., engineers involved in system implementation efforts).

4. *List Responsible Individual(s) by name in the DIP.* The DIP will serve as a much more effective tracking tool if responsible parties are specifically identified by name, rather than simply listing titles or organization names. Resist the

Please see *Top Ten* page 4

### **2010 Training from page 1**

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](mailto:diacap@diacap.net), to discuss partnering opportunities.

---

*“Keep documents updated regularly throughout the development process ...”*

---

## IA Control Spotlight – Physical Security

By Jeffrey H. Widom

There are numerous IA Controls in the *Physical and Environmental* category. These controls deal primarily with safeguards that are provided by the *facility* in which the system resides. Examples are temperature/humidity control, voltage control, fire protection/suppression, physical access control and visitor control. In most cases, application owners will *inherit* these controls from the hosting enclave.

It is important to understand that inheritance is not a “free pass.” If the hosting enclave is not providing one or more of the required controls, this will also be considered as a finding in the application’s certification, and duly noted on the Plan of Action and Milestones (POA&M). If the application owner’s DAA is not willing to accept this risk, there are several potential alternatives:

- The application owner can work with the owner of the enclave to achieve compliance. For example, the application owner might provide some of the funding to enable the enclave to upgrade its infrastructure to address the deficiency.
- The application owner can implement a *compensating control*. For example, the application owner might install his own power conditioner to compensate for the lack of adequate voltage control within the enclave.
- The application owner can find a new hosting provider that is providing fully-compliant physical and environmental protection.

The Service Level Agreement (SLA) between the application owner and hosting provider should explicitly address all physical and environmental controls.

### **Annual Review from page 1**

Manager (PM/SM, sometimes known as System Owner) should work together to ensure the Annual IA Review is completed on or before the anniversary date of the system’s accreditation (ATO).

At a minimum, the Annual IA Review consists of a “tabletop review” of the DIACAP Implementation Plan (DIP). The goal is to examine each of the applicable IA Controls to ensure that it is still in place and operating effectively. Any changes to the security posture should be duly noted in the DIP and recorded as new weaknesses in an updated Plan of Action and Milestones (POA&M). It is highly desirable to augment the tabletop review with some technical testing (e.g., running the Gold Disk on each of the Windows platforms) to ensure continued compliance with applicable Security Technical implementation Guides (STIGs).

The IAM is responsible for reporting the results of the Annual IA Review to the Designated Accrediting Authority (DAA) and the Certifying Authority (CA). If significant weaknesses have been discovered, the DAA and CA may opt to adjust the Authorization Termination date (i.e., shorten the timeframe of the accreditation), downgrade the accreditation (i.e., from ATO to IATO) or even revoke the system’s accreditation altogether. In the absence of any serious weaknesses, the DAA will generally leave the accreditation “as is”.

Each DoD component will have its own unique protocol for reporting the results of the Annual IA Review. PMs should coordinate with their installation IAM to ensure the proper procedures are being followed.

---

“...important to understand that inheritance is not a free pass...”

---

**Top Ten from page 2**

temptation to list the PM/SM as “responsible for everything” even though he/she technically *is*.

3. *Describe weaknesses carefully in the POA&M.* The POA&M is a management-level document. Make sure weaknesses are described in sufficient detail so that management can clearly understand the “get well plan”, but do not overdo the detail (e.g., by including IP addresses) thus unnecessarily increasing the sensitivity of the document.

2. *Make sure the documents are “traceable”.* The

## DIACAP Training Schedule

By Lon J. Berman

The DIACAP Resource Center offers *DIACAP Fundamentals* (one day) and *DIACAP In Depth* (three day) on a regularly-scheduled basis in the National Capital Region, Colorado Springs, Huntsville, San Antonio, and Tampa.

Regularly-scheduled classes for the First half of calendar year 2010 are as follows:

DIACAP Fundamentals (one day)	DIACAP In Depth (three days)
7 Dec 2009 (NCR)	8-10 Dec 2009 (NCR)
1 Feb (NCR)	2-4 Feb (NCR)
TBD (T)	TBD (T)
8 Mar (NCR)	9-11 Mar (NCR)
15 Mar (CS)	16-18 Mar (CS)
29 Mar (SA)	30 Mar - 1 Apr (SA)
12 Apr (NCR)	13-15 Apr (NCR)
19 Apr (H)	20-22 Apr (H)
10 May (NCR)	11-13 May (NCR)
7 Jun (NCR)	8-10 Jun (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

documentation package should tell a consistent “story”. For example, a weakness identified on the POA&M should be traceable to one or more “non compliant” controls on the Scorecard and DIP.

**1. Make sure the documents are honest and accurate.** The DIACAP package is a “living” set of documents that will accompany the system throughout its life cycle. Accurate, honest documentation is the cornerstone of a strong security program and ensures you will be prepared in the event your system is audited.

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](mailto: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](http://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](http://www.fedca.org).