



# DIACAP Dimensions

September  
2008

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

Please visit us at the Federal Information Assurance Conference (FIAC), Washington, DC, 27-28 Oct., Booth #213.

## DIACAP Training Comes to Colorado

By Lon J. Berman

A new DIACAP training site is now open! The DIACAP Resource Center has partnered with Integral Systems, Inc. (ISI) to begin offering *DIACAP Fundamentals* and *DIACAP In Depth* training in Colorado Springs. This move represents the first step in what we hope will be an ever-expanding array of training sites.

Until the opening of this new site, DIACAP training was only available *on a regularly-scheduled basis* in the National Capital Region. Training at other sites was limited to pre-arranged groups of at least ten trainees, usually from a single company or agency. Now, individual students can register for training in Colorado Springs just like they do for our National Capital Region classes.

The first DIACAP training classes in Colorado Springs will be held the week of September 8. Future classes have not yet been scheduled but will be announced on the website, [www.diacap.net](http://www.diacap.net), when they become

Please see *Colorado* on page 2

### INSIDE THIS ISSUE

- 1 DIACAP Training Comes to Colorado
- 1 The End of C&A?
- 2 Top Ten List – C&A Pitfalls
- 3 IA Control Spotlight – Continuity
- 4 DIACAP Training FY2009

## The End of C&A?

By Lon J. Berman

It has been said that the only thing that is constant in this world is change. Soon that old adage may well apply to DIACAP, as the government moves forward in its effort to adopt a single certification and accreditation process.

At the present time there are *three* predominant C&A processes in use - DIACAP in DoD, NIST in federal “civilian” departments, and DCID 6/3 in the intelligence community. While they all follow the same basic principles, they differ rather significantly in the process steps and documentation products they entail. Each has its own unique set of security controls (requirements), making it problematic for one government segment to “trust” the accreditation of systems owned by another segment.

---

*“...initial public draft of what may soon become the government-wide standard for C&A...”*

---

Please see *End of C&A* on page 3

## Top Ten List – Selecting a “Certifier”

By Jeffrey H. Widom

Depending on your individual component or organization’s policies, you may need to select a “certifier” (usually from an approved list) to perform the formal DIACAP validation of your system. Here is our Top Ten List of things to consider in making this selection.

---

*“Make sure you understand the services a potential certifier will provide...”*

---

10. Cost - The system owner (program/system manager) must plan and budget for the cost of validation. However, try not to let cost be the sole determinant of which “certifier” you choose. Also, be sure that each of the potential “certifiers” gives you a full cost proposal that includes all costs (e.g., travel, materials). Like everything else in the DIACAP process, you do not want any “surprises” here.

9. Location - Consider choosing a “certifier” that located as close as possible to your site. Potentially this can simplify logistics and save money.

8. Prior experience - If your system is “unusual” in any way (e.g., tactical systems or platform IT), be sure to discuss this with any potential “certifier”. Generally speaking, choosing a “certifier” with prior experience in testing similar systems will be more economical and provide a higher quality assessment of your system security posture.

7. Schedule - Make sure any potential “certifier” can meet your schedule expectations. Not only should they provide an estimate of when they can come on site to do your testing, but also how long it will take them after that to create the test report, DIACAP scorecard, etc.

6. Services - Make sure you understand the services that a potential “certifier” will provide, and the deliverables you will receive. In addition to the DIACAP scorecard, they should provide you with a full report of their test results.

5. References - Ask any potential “certifier” to provide references from previous

Please see *Top Ten* page 4



Our Colorado  
Springs Training  
Site Partner  
[www.integ.com](http://www.integ.com)

### **Colorado from page 1**

available. One more series of classes (*DIACAP Fundamentals* and *DIACAP in Depth*) in Colorado is anticipated in 2008.

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 classroom facility at your office location, we would like to speak with you regarding partnering opportunities. We are actively seeking 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).

Our Colorado Springs training site partner, Integral Systems, Inc., is at [www.integ.com](http://www.integ.com).

## IA Control Spotlight – Continuity

By Jeffrey H. Widom

The *Continuity* subject area deals with issues that affect the ability of the system to function in the event of an emergency. Data backup, alternate processing site, and contingency planning are the principal areas of concern.

This subject area contains the most striking example of the effect of the Mission Assurance Category (MAC) level on the security requirements. As you probably know, the MAC level is a measure of system criticality that ranges from MAC I for mission critical systems to MAC III for office systems. Here is how this plays out in the requirements for disaster recovery:

- MAC III systems - IA Control CODP-1 applies, stating that “a disaster plan exists that provides for the partial resumption of mission or business essential functions within 5 days of activation.” IA
- MAC II systems - IA Control CODP-2 applies, requiring that the disaster plan provide for “resumption of mission or business essential functions within 24 hours activation.”
- MAC I systems - IA Control CODP-3 applies, requiring a disaster plan that provides for “smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity.”

From this set of controls alone, it is very clear how the MAC level affects the operational readiness ... *and cost* ... of the system.

### End of C&A from page 1

Seamless cooperation among government entities is vital to our national security. While the existence of multiple C&A processes is far from the most pressing problem they face, it certainly does not help matters.

The *Joint Task Force Transformation Initiative* Interagency Working Group was formed to address this issue and come up with a single, unified process for Security Authorization (i.e., C&A) of federal information systems. Under the leadership of NIST, the first published document reflecting the work of the Joint Task Force was recently released in draft form.

NIST Special Publication 800-37, Revision 1, is entitled *Guide for Security Authorization of Federal Information Systems - A Security Life Cycle Approach*. This is the initial public draft of what may soon become the government-wide standard for C&A. A copy of this draft is available from NIST: <http://csrc.nist.gov/publications/drafts/800-37-Rev1/SP800-37-rev1-IPD.pdf>. It is currently in the public comment period; NIST welcomes your comments and suggestions for improvement.

One noteworthy change that is apparent in this draft is the “retirement” of the term “C&A” in favor of “Security Authorization”.

When and how will this new process be adopted (or adapted) by DoD? Can “*DIACAP II - The Sequel*” be far away? Stay tuned!

---

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

---



Our National Capital Region  
instructional services partner  
([www.simplexdatasolutions.com](http://www.simplexdatasolutions.com))

**Top Ten from page 2**

engagements. Call these customers and talk to them about their experience.

4. Test Plan - Make sure any potential “certifier” will provide you with their test plan well in advance of their site visit.

3. Testing tools - Ask any potential “certifier” what automated tools they will be using. If you don’t currently own these tools, ask if they can they provide you with “loaner” tools so that you can pre-test your system.

2. Documentation - Make sure you provide any potential “certifier” with all available system documentation, especially diagrams and inventories. This will help them properly estimate the level of effort needed to test your system, and avoid any unpleasant “surprises” (i.e., additional charges) down the road.

1. Communication - Make sure any potential “certifier” is ready and willing to communicate with your DIACAP team, both before and after the site visit.

**DIACAP Training in FY 2009**

By Lon J. Berman

In FY09, 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, and, hopefully, other locations as well.

Regularly-scheduled classes for the remainder of calendar year 2008 are as follows:

DIACAP Fundamentals (one day)	DIACAP In Depth (three days)
8 September (NCR)	9-11 September (NCR)
8 September (CS)	9-11 September (CS)
6 October (NCR)	7-9 October (NCR)
3 November (NCR)	4-6 November (NCR)
TBD November (CS)	TBD November (CS)
8 December (NCR)	9-11 December (NCR)
(NCR) = National Capital Region (CS) = Colorado Springs	

The schedule of classes for the first half of calendar year 2009 will be announced in October.

For customers in other locations, 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). Optionally, you may also download a registration form for submission 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](mailto: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](http://www.fedca.org).