



# DIACAP Dimensions

January  
2008

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

## INSIDE THIS ISSUE

- 1 DoD Instruction 8510.01 Signed!
- 1 Consulting Services for Product Developers
- 2 Kickoff Meeting – Key to DIACAP Success
- 3 IA Control Spotlight
- 4 DIACAP Training for 2008

## DoD Instruction 8510.01 Signed!

By Lon J. Berman

On November 28, 2007, DoD Instruction 8510.01 was signed by Chief Information Officer John Grimes. This is the long-awaited “official” DIACAP process document. Despite persistent rumors to the contrary, the C&A process, roles, responsibilities, and documentation requirements have remained largely unchanged from the interim guidance. Still, there are numerous clarifications, revisions, and improvements in this new document. Some of the key areas that have changed are:

- More detail has been added to the DIACAP process steps
- Several line items in the System Identification Profile (SIP) document have been changed to remove some of the redundancy
- Explanations for many line items in the SIP have been clarified

Please see *Signed* on page 2

## Consulting Services for Product Developers

By Lon J. Berman

The DIACAP Resource Center is pleased to offer consulting services specifically aimed at product developers and vendors.

Product developers face a unique dilemma when it comes to DIACAP. Federal customers insist that vendors’ products be “DIACAP Certified,” but there is no way for manufacturers to *independently* seek certification of their wares. The truth is that it takes a *team effort* in which both the product developer and federal customer must understand their roles and provide the necessary information and support.

We have designed two flexible types of consulting engagements to address these needs.

In our *DIACAP Readiness* program, we work with vendors to evaluate their products for compliance with applicable IA Controls (security

Please see *Product Developers* on page 3

---

*“Product developers face a unique dilemma when it comes to DIACAP.”*

---

## Preparing for DIACAP Validation

By Jeffrey H. Widom

Good preparation is the key to successful DIACAP validation (aka. Certification testing). Our Top Ten List will help you be ready when the validators arrive at your site to test your system.

10. Be Prepared - Work with the Certification Team and not against the staff assigned to validate the controls. Be prepared to answer basic human wellness questions such as “Where are the bathrooms?”, “Do you have any coffee?”, or “Where can we get some lunch?”

9. Meetings - Establish a schedule (bi-weekly, monthly) to discuss C&A issues with the entire DIACAP team. Ask as many questions as possible!

8. Accuracy vs. Perfection - Especially in the beginning of the C&A process, it is not reasonable to expect every requirement to be perfect. The IAM’s goal should be to ensure the status of each security control is accurately documented.

7. POA&M - Develop a preliminary Plan of Action and Milestones (POA&M) prior to the validation. Verify the risks identified in the POA&M are accurately documented in the Implementation Plan. Ensure the personnel who responsible for correcting the deficiency can clearly explain the methods being developed to correct the deficiency or safeguards being implemented to minimize risk.

6. STIG Exceptions - Establish a process for documenting all exceptions for Security Technical Implementation Guideline (STIG) requirements that cannot be applied and be prepared to explain the reasoning to the Certifier.

5. The Right Tools - Procure the necessary testing tools and frequently verify compliance throughout the system development life cycle. Ask the Certifier for recommendations on various tools/methods for testing custom applications. Accurately document all results.

4. Artifacts - Develop a plan to draft the required DIACAP artifacts and

Please see *Validation* 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](http://www.intelligent.net))

### **Signed from page 1**

- A few revisions have been made to the format and content of the DIACAP Scorecard and POA&M, and additional explanation has been provided
- Specific information has been provided on *Type Accreditation*, *Stand-alone systems*, and *Outsourced IT-based processes*.
- Many of the roles and responsibilities have been clarified.

A copy of DoDI 8510.01 has been posted on our website [www.diacap.net](http://www.diacap.net).

Beginning in January 2008, our DIACAP training curriculum has been updated to include the provisions of this new, “official” document. We at *DIACAP Dimensions* will continue to monitor the DIACAP Knowledge Service and keep you informed of any further changes, revisions, or supplementary guidance that DoD may offer in the future.

## IA Control Spotlight

By Jeffrey H. Widom

IA Control DCAS-1 (Acquisition Standards) consists of several statements. For this discussion, we will focus on one part: *“The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources—the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program.”*

First of all, what exactly is an IA product, or IA-enabled product? An IA product is one whose primary function is to support security. Examples include firewalls, intrusion detection systems, etc. An IA-enabled product’s primary function is something other than IA, but the product also plays a significant role in security-policy enforcement. Prime examples are operating systems and database management systems, both of which provide security functionality in the areas of identification and authentication (I&A), access control, and audit.

What this control is saying, essentially, is that any system component (hardware or software) that provides security functionality must have been evaluated in accordance with the Common Criteria, NIAP, or FIPS validation programs. The FIPS validation program is concerned specifically with encryption products for sensitive, unclassified data. The Common Criteria/NIAP evaluation programs cover all other security-related products.

For more information, please refer to [www.nsa.gov/ia/industry/niap.cfm](http://www.nsa.gov/ia/industry/niap.cfm) for the Common Criteria/NIAP program, or [csrc.nist.gov/groups/STM/cmvp/index.html](http://csrc.nist.gov/groups/STM/cmvp/index.html) for the FIPS validation program.

### ***Product Developers from page 1***

requirements) and recommend steps for compliance improvement. We also help vendors develop a documentation package that can effectively provide evidence of compliance to current and potential DoD customers.

In some cases, our recommendations will include development of additional documentation (such as configuration management plans or standard operating procedures), or even the addition of new technical security measures (such as firewalls or encryption) to existing products. In these situations we can provide the expertise to support or carry out the recommended security improvements in a timely and cost-effective fashion.

In our *DIACAP Liaison* consulting program, we provide the IA expertise to facilitate the relationship between product vendors and DoD customers. We can assist by attending meetings, helping vendors respond to IA-related questions from customers or prospects, or helping vendors to develop appropriate security-related portions of proposals, marketing materials, operating manuals, etc.

Both the *DIACAP Readiness* and *DIACAP Liaison* programs can be “customized” to meet the needs of specific vendors and product lines.

For further information on consulting services for product developers, please contact us at 540-808-1050.

---

*“...any system component that provides security functionality must have been evaluated ...”*

---



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

**Validation from page 2**

accurately document the location of the artifacts prior to the testing. The Certifier should appreciate you being extremely well prepared to provide the supporting written evidence of compliance without having to search for policies.

3. Certifier's Test Plan - Request a copy of the Certifier's test plan prior to the validation. The test plan can be a basic template or a sanitized version of an existing document. Use the Certifier's test plan to review the status of each security control.

**DIACAP Training for 2008**

By Lon J. Berman

I want to personally thank everyone who helped make 2007 a successfully year for the DIACAP Resource Center. In our first full year of operation, we trained literally *hundreds* of DoD employees and contractors, both in our regularly-scheduled classes and at customer sites throughout the nation.

In 2008, we will continue to offer our *DIACAP Fundamentals* (one day) and *DIACAP In Depth* (three day) training courses on a regularly-scheduled, monthly basis in the National Capital Region (Northern Virginia).

In addition to these regularly-scheduled classes, we can also provide "on site" training at *your* location. All you need is a group of students (normally 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. Additionally, you will save on the travel expenses and logistical issues associated with sending your people to training away from the office. Please

2. Be Honest - Do not list a security requirement as "Implemented" if supporting evidence of compliance is not available.

1. Review, Review, Review - Take the necessary time to thoroughly review and accurately document the status of all security controls prior to the validation testing.

contact the DIACAP Resource Center at 540-808-1050 for further information on our "on site" training program.

Regularly-scheduled classes in the National Capital Region for the first half of 2008 are as follows:

DIACAP Fundamentals (one day)	DIACAP In Depth (three days)
7 January	8-10 January
4 February	5-7 February
3 March	4-6 March
7 April	8-10 April
5 May	6-8 May
2 June	3-5 June

For course content, cost, and registration, please visit our website [www.diacap.net](http://www.diacap.net), or call us at 540-808-1050.

**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)