



DIACAP RESOURCE CENTER

DIACAP CONSULTING SERVICES FOR SERVICE PROVIDERS

“The Department of Defense shall certify and accredit information systems through an enterprise process for identifying, implementing, and managing Information Assurance capabilities and services.”

... John G. Grimes, DoD CIO

DIACAP BACKGROUND

It is DoD policy that all information systems undergo a Certification and Accreditation (C&A) process. *Certification* is a technical analysis of the system’s compliance with an assigned set of Information Assurance (IA) Controls (i.e., security requirements, derived from DoD Instruction 8500.2 and other policies), thereby providing an assessment of the system’s risk level. *Accreditation* is a formal Approval To Operate (ATO), granted by a senior government official, who determines the risk is acceptable on the basis of information collected during the certification.

DIACAP (DoD Information Assurance Certification and Accreditation Process) is the name given to the formal process for certifying and accrediting information systems within the Department of Defense.

THE SERVICE PROVIDER’S DILEMMA

As a commercial service provider offering (or wishing to offer) your service(s) to DoD, you will sooner or later run into the dreaded “D word” (i.e., DIACAP). Potential customers may ask you if your service or system has been “DIACAP approved,” or even ask for a copy of your “certificate.” However, unlike many other government certification programs, you as a vendor cannot independently seek DIACAP approval.

DIACAP is fundamentally a *government* process, carried out by government *people*. DoD refers to the use of commercial services to process DoD data as *Outsourced IT-based Processes*, and requires certification and accreditation just as they do for DoD-owned and operated systems. The question is – what can the government reasonably expect vendors to provide in support of this C&A effort?

First and foremost, the answer is *information* – in the form of documented evidence of compliance with applicable DoD security requirements. Service providers can maximize their “readiness” for DIACAP by:

- thoroughly analyzing their IT environment’s compliance with DoD security requirements
- making improvements to enhance compliance where necessary
- documenting compliance in a manner that is readily *usable* and *understandable* by DoD customers and conducive to a determination of risk acceptability.

Secondly, the answer is *support and teamwork*. Even though DIACAP is DoD’s own process, it is often not well understood by the government people tasked with carrying it out. The best way



to ensure success is for the government and the vendor to work as a team. A knowledgeable vendor can facilitate the process and gain valuable credibility with the DoD customer at the same time.

In response to these needs, the DIACAP Resource Center is pleased to offer the following consulting services geared specifically to address the needs of service providers:

- *DIACAP Compliance Survey* – a “short-turnaround” service to provide you with a basic view of your compliance with applicable DoD security requirements, and a set of practical recommendations for compliance improvement.
- *DIACAP Readiness Assessment* – a much more comprehensive service that includes extensive “hands on” testing to provide a detailed view of your organization and IT infrastructure compliance, detailed technical recommendations, and a set of DIACAP documents formatted according to DoD standards.
- *DIACAP Liaison Consulting Services* – a consulting service designed to help “bridge the gap” between your organization and your current or potential DoD customers.

DIACAP COMPLIANCE SURVEY

Our *DIACAP Compliance Survey* consulting engagement is designed to quickly provide an assessment of your level of compliance with DoD security standards and offer practical recommendations for compliance improvement. A *DIACAP Compliance Survey* can typically be completed in 21 days or less, and includes the following activities:

- Inbrief teleconference. In this meeting, we present a short DIACAP overview, receive an overview from your company, identify key individuals within your organization, and identify documents for review.
- Interview and document review. We will review the documents you have provided, supplemented by discussion with appropriate persons in your organization, in order to gather additional information about your organization and IT environment and begin to evaluate your security functionality against the applicable DoD controls and standards.
- On-site compliance review. We will meet with your team to review the DoD security requirements and assess your level of compliance.
- Written report. We will document the results of these activities in a *DIACAP Compliance Survey Report*, consisting of an executive summary and an evaluation of your compliance, including recommended steps for compliance improvement.

DIACAP READINESS ASSESSMENT

Our *DIACAP Readiness Assessment* consulting engagement offers a much more detailed compliance evaluation, including “hands on” testing of your IT infrastructure. Depending on the complexity of your organization and IT environment, a *DIACAP Readiness Assessment* may take 10-12 weeks, or more, to complete. Typically, the *DIACAP Readiness Assessment* will entail the following activities:

- Inbrief. If you have not already completed a *DIACAP Compliance Survey*, we will conduct an inbrief teleconference as described above.
- Document reviews and discussions. We will review your organization’s documentation at a technical level, and conduct interviews with appropriate personnel within your organization.



- Test plan. Based on review of your documentation and follow-up technical discussions, we will develop a comprehensive plan for testing your security functionality and compliance.
- On-site testing. We will spend several days at your facility conducting observations and “hands on” testing (with a variety of security testing tools), along with follow-up discussions, in order to evaluate the technical aspects of your IT security.
- Analysis. Information from document reviews, discussions and on-site testing will be analyzed to produce a detailed assessment of compliance with each of the applicable DoD requirements, and a set of recommendations for compliance improvement and risk mitigation.
- In-process briefing. We will verbally present the “highlights” of our findings and recommendations.
- Development of deliverables. In addition to a comprehensive *DIACAP Compliance Report* and executive summary, we will also provide a set of DIACAP documents (*System Identification Profile (SIP)*, *DIACAP Implementation Plan (DIP)*, *DIACAP Scorecard*, and *Plan of Action and Milestones (POA&M)*), formatted in accordance with DoD standards.
- Outbrief meeting, in which we present our “final” set of findings and recommendations, based on the deliverable documents.

The deliverables from the *DIACAP Readiness Assessment* will play a major role in facilitating certification and accreditation of your service as an “outsourced IT-based process”. Also, they will serve as a powerful weapon in your company’s marketing arsenal. In some cases, this can be the “competitive edge” that separates your service offering from that of your competitors.

DIACAP LIAISON CONSULTING SERVICES

Our *DIACAP Liaison* consulting engagement is designed to assist you in working with your government customers (and potential customers) on security-related matters. Services we can perform in this capacity include, but are not limited to:

- participation in pre- or post-sales meetings with your current or potential DoD customers as an information assurance “subject matter expert”
- assisting your government customers in understanding your organization’s regulatory compliance, or even the DIACAP process itself
- acting as your “in house” security expert during the “full life cycle” of DIACAP evaluation by your current or potential DoD customer
- assisting your staff in drafting appropriate security language for proposals and marketing material
- assisting your staff in drafting security-related language in technical documentation such as installation and operating manuals, etc.

CONTRACTUAL ARRANGEMENTS AND FEES

DIACAP Compliance Survey engagements are typically done on a “firm fixed price” basis.

DIACAP Readiness Assessment engagements may be done on a “firm fixed price” or “time and materials” basis. If a firm fixed price arrangement is desired, the quoted cost will be dependent upon the number and complexity of products to be analyzed, and the breadth of desired services. For “time and materials” engagements, an initial estimated number of hours will be given, and adjusted thereafter based on progress and issues encountered.



DIACAP Liaison consulting engagements are typically done on a “time and materials” basis. We initially recommend a “block” of hours to be allocated in the form of a purchase order. We will then track utilization of these hours and provide a monthly statement along with our invoice.

OTHER CONSULTING SERVICES

Policy and Procedures Development. If the compliance analysis of your service and IT environment recommends development of additional policy and/or procedures documents, it may be worthwhile to consider using outside assistance to prepare them rather than diverting your valuable product development or support resources. Our consultants can develop the required documents at a reasonable cost and with minimal disruption to your staff.

Information Security Engineering. If the compliance analysis of your service and IT environment recommends development of additional technical security safeguards, our consultants can provide the needed engineering support to make such product enhancements efficiently. We are experienced in the implementation and integration of security technologies such as firewalls, intrusion detection systems, encryption devices, etc.

DIACAP TRAINING

The DIACAP Resource Center also offers classroom training to government and industry. We currently offer a one-day *DIACAP Fundamentals* and a three-day *DIACAP In Depth* course. Both courses are presented on a regularly-scheduled basis at selected cities nationwide. If you have a group (normally 8-10 trainees or larger), we can also arrange to bring one of our instructors to your site. A full schedule of class dates and locations, as well as registration for the regularly-scheduled courses is available at www.diacap.net. For an on-site training quotation, please contact us at 540-808-1050.

ABOUT US

The DIACAP Resource Center is an independent consulting organization dedicated to assisting the DoD and its suppliers in understanding and implementing the DIACAP process.

The DIACAP Resource Center is a division of BAI Information Security Consultants. BAI has been a provider of information technology and security consulting services since 1974 and specializes in Certification and Accreditation (C&A) of federal information systems. BAI founder and principal consultant Lon Berman has over 35 years’ experience and is a recognized authority on DIACAP.

CONTACT US

For more information, please contact the DIACAP Resource Center:

Phone: 540-808-1050 FAX: 540-808-1051 E-mail: diacap@diacap.net



**Information Security Consultants
DIACAP Resource Center**

7467 Bluff View Dr • Fairlawn, VA 24141
540-808-1050 • FAX 540-808-1051
diacap@diacap.net • www.diacap.net