Risk Management Framework Today

Formerly DIACAP Dimensions

... And Tomorrow

March 2012
Issue 1, Volume 2

Find us on Facebook

LinkedIn

In this issue:

DoD C&A Transformation Picture Becomes Clearer

By Lon J. Berman

A recent presentation made public by DoD's Information Assurance Policy and Strategy (IAP&S) Directorate has provided some much-needed clarity on the planned transition from DIACAP to the Risk Management Framework (RMF). In this document, DoD confirms its commitment to transforming its information assurance program to align with Federal government risk management policies and practices in accordance with the work of the Joint Task Force Transformation Initiative Interagency Working Group.

DoD plans to document its implementation of RMF by revision of existing "DoD 8500 Series" publications, including DoDD 8500.01 (IA Policy), DoDI 8500.02 (IA Implementation) and DoDI 8510.01 (DIACAP). The result will be an IA program that embraces standardized terminology used across the Federal government, enables efficient enterprise management of IA, and fully complies with FISMA review and reporting requirements. Most importantly, the DoD security controls and approval process will then mirror those of the intelligence community and "civilian" departments/agencies, thereby fostering interoperability, reciprocity and trust across the federal landscape.

Some of the "highlights" of DoD's implementation plan are as follows:

- Terminology will align with CNSSI 4009 (standard federal glossary of IA terms and acronyms)
- Mission Assurance Category (MAC) and Confidentiality Level (CL) will be replaced by a System Categorization based on impact values (low, moderate, high) for Confidentiality, Integrity and Availability, as documented in Committee on National Security Systems Instruction (CNSSI) 1253
- Existing DoDI 8500.2 IA Controls will

Cont. on page 6

DISA Revamps STIGS and Validation Tools

By Kathryn Farrish

Among its many duties supporting information technology within DoD as well as other government agencies and industry partners, the Defense Information Systems Agency (DISA) is responsible for developing secure configuration guidelines for systems and software, and, where feasible, developing automated validation tools. DISA publishes guidance in the form of Security Technical Information Guides (STIGs) and Security Checklists for popular operating systems (Windows, UNIX), database management systems (Oracle, SQL Server), web servers, network devices, etc. Automated validation tools include the Gold Disk for Windows and Security Readiness Review (SRR) scripts for various versions of UNIX, database systems, etc.

Recently, DISA has revamped its strategy for STIGs and validation tools. STIGs and associated Security Checklists have traditionally been published as PDF documents. DISA is now publishing them in the form of XML documents and style

Cont. on page 2

DISA Revamps STIGS and Validation Tools

(Continued from page 1)

sheets. When opened with an application such as Internet Explorer, these XML files closely resemble the form and content of the legacy PDF STIGs. However, the adoption of XML facilitates the use of the STIG content as input to various automated processes. For example, it is now possible to populate spreadsheets and databases with STIG content in a way not possible with the PDF versions. On the DISA website, each STIG is available as a downloadable ZIP file, which must be completely "un-compressed" in order to access the STIG itself.

Many of the STIGs are now published in two forms. Both are Unclassified, but one of them is publicly available and the other is designated For Official Use Only (FOUO). The FOUO STIG contains additional information on vulnerabilities that are not authorized for public distribution. All users can retrieve the Unclassified STIG, but only those with a DoD Common Access Card (CAC) may retrieve the FOUO versions. For users without CAC, it is important to note that, unlike many DoD sites, DISA has not enabled the use of External Certificate Authority (ECA) credentials to access the FOUO STIGs. Such contractors must rely on their DoD customer to download and provide them with any required FOUO STIGs.

A radical change in DISA's approach to validation tools is also underway. For Windows systems, the Gold Disk has long been the method of choice for compliance validation. The Gold Disk contains a powerful and elegant "scan engine" and reporting mechanism, and is regularly updated with the latest recommended settings for numerous versions of Windows workstations and servers. Probably due more to cost than anything else, DISA has decided to stop further enhancement to the Gold Disk. Gold Disk content for existing versions of Windows will continue to be provided (at least for a while), but the scan engine and reports will not be further enhanced, nor will new versions of Windows be supported. What this means is that the Gold Disk is not, and will not ever be, suitable for scanning Windows Server 2008R2 or Windows 7 systems.

Under the new approach, DISA is publishing "automated benchmarks" for each of the Windows versions, including Server 2008R2 and Windows 7. These benchmarks are XML files that are designed to be run through commercially available scan engines, such as eEye Retina, McAfee Policy Auditor, or Tenable Security Center. We expect the UNIX and database SRR scripts to eventually be replaced by XML benchmarks as well.

DISA STIGs, checklists, and validation tools are available at https://iase.disa.mil.

Information Security Certifications Get Easier

By Betsy Taylor

Professional certifications have become a key element in the government's effort to improve the quality of its information assurance workforce. Through regulations like DoDI 8570.1, government agencies have imposed significant requirements for training and certification upon any staff member with information assurance responsibility, *including both government employees and contractors*. Two of the most sought-after certifications are sponsored and administered by the International Information Systems Security Certification Consortium (ISC2):

Certified Information System Security Professional (CISSP). CISSP is a broad-based program covering 10 "bodies of knowledge" that run the gamut of security principles and practice, from risk management to cryptography and everything in between. It has long been considered the "gold standard" of certifications for information assurance professionals. The CISSP exam is a six-hour "marathon" consisting of 250 questions.

Certified Authorization Professional (CAP). This certification, formerly known as Certification and Accreditation Professional, is a more specialized program covering the theory and practice of information system security assessment and authorization using NIST RMF methodology. The CAP exam is a three-hour, 125 question test.

Until recently, these exams were administered periodically in various cities around the nation and the world. Many of the exams were scheduled on weekends – good for some people and not good for others. Candidates were required to schedule their exam date well in advance and arrange travel to the selected testing site. The stress of travel and the "ambience" of the testing center (scores of people taking the exam in one large room) merely added to the "intimidation factor" of the material itself.

In recent months, ISC2 has taken steps to make the testing process much more convenient and much less stressful. The "paper-based classroom" is giving way to modern computer-based testing centers. ISC2 is partnered with Pearson Vue, a leading testing provider, so candidates can now schedule ISC2 exams at a local testing center (there are more than 4,000 of them) on any day/time the center is open. Computer-based testing is currently available for the CAP, with the CISSP expected to come on board this June. The number of questions and time limit for these exams remains the same (i.e., 6 hours, 250 multiple-choice questions for the CISSP; 3 hours, 125 multiple-choice questions for the CAP).

While the knowledge level required to achieve these certifications has not changed, the new testing methodology is bound to make for a more pleasant (or, at least, less unpleasant) experience! Additional information about the certification examinations is available from directly from ISC2 on their website http://www.isc2.org.

Many information security and IT professionals opt for classroom training as a key part of their preparation for these certification exams.

Continued on page 6

IA Control Spotlight—Comparing DoD and NIST Controls

By Robert E. Lee, Jr.

A key element (some would say *the* key element) of DoD's "C&A transformation" process is the adoption of security controls derived from NIST SP 800-53 in place of the existing DoDI 8500.2 IA controls.

One of the first things you'll notice is that the number of controls in 800-53 is vastly larger than what is in 8500.2. The NIST controls work very similarly to the DoD controls in that only a portion of them are applicable to any one system. In DIACAP the selection is based on MAC and CL, while in NIST the *security baseline* is selected by a somewhat more complex process of analyzing the "level of concern" (High, Moderate or Low) for Confidentiality, Integrity and Availability. The typical unclassified DoD system might have a MAC level of II and Confidentiality Level of Sensitive; 106 IA controls would be applicable to such a system. Based on the NIST methodology, such a system would likely be assigned a Moderate security baseline, and approximately 170 security controls would be applicable.

Does this mean there are a 60-odd new security features that need to be built into your system (or its environment and documentation)? Should you panic now? The short answer is NO. There are many reasons why the sheer number of NIST controls is larger, and many of them have little to do with additional requirements being imposed. For one thing, the NIST controls are written in a much more granular fashion. The same concept that is covered in a single DoD control may actually encompass several NIST controls. Secondly, the NIST controls provide additional, more detailed, requirements in areas that are covered more broadly in the DoD policy. Thirdly, the NIST controls cover other DoD policies and guidance contained in other DoD documents that are not explicitly stated in 8500.2. All that said, however, there are *some* NIST controls that cover areas previously absent from DoD policy and guidance, so these may potentially need to be addressed by implementation of additional security features.

Another thing you'll quickly notice is that many of the NIST controls contain "blanks" that need to be filled in. These are called "Organization-defined values" or "Assignments", and they are intended to make the controls adaptable to a wide variety of organizations and circumstances. The Committee on National Security Systems (CNSS) provides recommended values for many of these assignments, and this methodology will be followed by DoD, thus making the NIST controls "their own".

In the next issue of "RMF Today … and Tomorrow" we will thoroughly "dissect" a NIST security control. Meanwhile, if you don't already have one, download yourself a copy of NIST SP 800-53, Rev. 3 (or Rev. 4, which is currently in draft) from the NIST information security website http://csrc.nist.gov.

Top 10—Reasons to Start Preparing for C&A Transformation

By Kathryn Farrish

The lead article in this edition of "RMF Today … and Tomorrow" indicates that revised DoD IA policies and procedures will not be published until the end of 2011 and that there is sure to be a "phase in" period thereafter. Why, then, should DoD system owners be concerned about preparing for the transformation *now*? This edition of the "Top Ten List" addresses the importance of starting "early".

10. Familiarization with NIST and CNSS documentation. System owners and their supporting staff and contractors need time to become familiar with the plethora of RMF documentation available through NIST and CNSS.

9. Learning RMF roles and responsibilities. System owners need time to understand the organizational impact of new and revised roles and responsibilities in RMF.

8. Learning RMF life cycle. System owners need time to understand and plan for implementation of the RMF life cycle (replacing the DIACAP life cycle).

7. Understanding continuous monitoring requirements. System owners need time to understand the RMF requirements for "continuous monitoring" of security posture so they can plan appropriately for implementation.

6. Learning new security categorization methodology. System owners need time to understand and apply the security categorization methodology published by NIST and CNSS, replacing MAC and CL with "impact values" for confidentiality, integrity and availability.

5. Learning the new security controls. System owners need as much time as possible to ensure personnel become familiar with the new NIST security controls and the "delta" between DoD and NIST.

4. Revising documentation. Transformation to RMF will require development of new documentation, such as a System Security Plan (SSP). System owners need as much time as possible to allocate the resources necessary to develop and maintain this new documentation set.

3. Implementing new or revised security functionality. Some of the 800-53 controls address technologies not currently addressed in DoD IA controls and guidance. System owners need as much time as possible to assess the impact of these controls and determine if additional security capabilities need to be integrated, and what resources will be required to do so.

2. Obtaining training. Training will make all the above steps go more smoothly, and serve to minimize errors and false starts. System owners need as much time as possible to determine the types of training needed, the personnel who will need to attend, and the preferred delivery modality (e.g., classroom training at a vendor's training center, "on site" training", web-based training).

1. Funding and management support. Starting <u>now</u> will enable system owners to ensure management "buy in", assess the cost of making the transition, and submit any necessary funding requests. When it comes to funding, earlier is almost always better!

DoD C&A Transformation Picture Becomes Clearer

(Continued from page 1)

be replaced by Security Controls from NIST Special Publication (SP) 800-53 and CNSSI 1253

- Through the DIACAP Knowledge Service, DoD will provide specific assignment values, validation procedures and implementation guidance for these controls.
- DIACAP Certification & Accreditation (C&A) process will be replaced by the Risk Management Framework (RMF) life cycle process.
- DoD enterprise applications such as eMASS and VMS will be aligned to the new system categorization, security controls and life cycle process

So when is all of this expected to take place? According to DoD, Calendar Year 2012 will be spent on drafting documents, soliciting comments and coordinating revisions. Official publication of revised "8500 Series" documents is expected at the end of CY12. It is rumored that DoD will adopt the name DIARMF, a "blended acronym" that reflects the transformation of DIACAP into RMF.

So, now we know a lot more about DoD's plans for C&A transformation. But we still don't know *everything*. DoD still has not given us any hint as to their proposed timeline for the transformation *after* all the publications are released. How long will system owners be given to make the transition to RMF, implement the new security controls and update their system security documentation accordingly?

Our best advice to DoD staff and contractors is the begin preparing for transformation now. Our *FISMA RMF Fundamentals* and *FISMA RMF In Depth* courses will give you the RMF life cycle skills and NIST/CNSS security control knowledge you will need to effectively address your organization's needs now and in the future.

Information Security Certifications Get Easier

(Continued from page 3)

DID YOU KNOW? Our *FISMA RMF Fundamentals* and *FISMA RMF In Depth* courses cover all seven domains that comprise the CAP Common Body of Knowledge (CBK):

- Understanding the Security Authorization of Information Systems
- Categorize Information Systems
- Establish the Security Control Baseline
- Apply Security Controls
- Assess Security Controls
- Authorize Information System
- Monitor Security Controls

In addition to preparing you for the CAP exam, our courses will give you the practical knowledge that will help you implement these processes successfully in your organization. A full schedule of FISMA RMF courses is on the last page of this newsletter. Registration is available at http://www.fisma1.net/registration.asp.

Contact Us!

RMF Today … and Tomorrow is a publication of BAI DIACAP/RMF/FISMA Resource Center, Fairlawn, Virginia.

Phone: (540) 808-1050
Fax: (540) 808-1051
Email: RMF@RMF.ORG

Training for Today … and Tomorrow

Our FISMA RMF training program is suitable for Federal "civilian" agencies as well as DoD personnel looking for insight into the future of "C&A" within their programs.

Since DoD is just at the early stages of its C&A transformation, we are continuing to offer our "traditional" DIACAP training program, which has recently been enhanced to include information on the RMF transition.

Each of our training programs consists of a one-day Fundamentals class, followed by a three-day In Depth class. The cost of training is $650 for the one-day class, $1,500 for the three-day class, or $1,935 for the full four-day program (both classes).

DIACAP Fundamentals (One-day)	DIACAP In-Depth (Three-day)
23 Apr 2012 (NCR)	24-26 Apr 2012 (NCR)
7 May 2012 (SD)	8-10 May 2012 (SD)
4 Jun 2012 (H)	5-7 June 2012 (CS)
11 Jun 2012 (SD)	12-14 Jun 2012 (SD)
18 Jun 2012 (H)	19-21 Jun 2012 (H)
25 Jun 2012 (NCR)	26-28 Jun 2012 (NCR)
16 Jul 2012 (SD)	17-19 Jul 2012 (SD)
20 Aug 2012 (NCR)	21-23 Aug 2012 (NCR)
10 Sep 2012 (CS)	11-13 Sep 2012 (CS)
24 Sep 2012 (H)	25-27 Sep 2012 (H)

FISMA RMF Fundamentals (One-Day)	FISMA RMF In-Depth (Three-Day)
16 Apr 2012 (CS)	17-19 Apr 2012 (CS)
30 Apr 2012 (H)	1-3 May 2012 (H)
21 May 2012 (DC)	22-24 May 2012 (DC)
23 Jul 2012 (DC)	24-26 Jul 2012 (DC)
30 Jul 2012 (CS)	31 Jul-2 Aug 2012 (CS)
13 Aug 2012 (H)	14-16 Aug 2012 (H)
17 Sep 2012 (DC)	18-20 Sep 2012 (DC)

(H) - Huntsville, AL (CS) - Colorado Springs, CO
(NCR) - National Capital Region (Ashburn, VA)
(SD) - San Diego, CA (DC) - Washington DC

On-line registration and payment for all scheduled classes is available at www.diacap.net (for DIACAP classes) or www.fisma1.net (for FISMA RMF classes). Registration can also be done by downloading a registration form and submitting the completed form by FAX or email.

Payment arrangements include credit cards, SF182 forms, or purchase orders.

Please visit www.diacap.net or www.fisma1.net for the latest training schedule, including any new dates or locations.

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 (normally 8-10 or more) and a suitable classroom facility. We offer a substantial discount over the normal "per student" registration cost; the discount grows larger as the 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 associated with sending your people to training away from the office. Please contact us to request an on-site training quotation.