Risk Management Framework Today

Formerly DIACAP Dimensions

… and Tomorrow

April, 2017
Volume 7, Issue 2

In this issue:

NIST SP 800-53 Rev 5—Big Changes Coming?	1
BAI Announces eMASS Training Program	2
Top Ten—Things You Should Know about eMASS	3
Security Control Spotlight—"Naming" of Controls, Enhancements and CCIs	4
Training for Today… and Tomorrow	5

NIST SP 800-53 Rev 5—Big Changes Coming?

By Lon J. Berman, CISSP

As you probably know, the "catalog" of security controls used in RMF is derived from NIST Special Publication (SP) 800-53 Rev 4. What you may not know is that NIST is hard at work on SP 800-53 Rev 5.

The reaction to this news on the part of many people involved in the RMF process is likely to be *concern* … or even *fear*! Will extensive re-work need to be done to adapt our RMF packages to the new control set? Will new or revised documentation artifacts … or even system implementation changes … be required in order to comply? The more cynical among us may even be thinking "Just when we're beginning to get our arms around this stuff, they're going to change it and mess us up again!" The bottom line is we won't know for sure until the document is published and we all get a chance to carefully analyze its contents. Until then, however, there are many factors that should lessen our concerns about the potential for major upheaval.

First of all, it's important to understand the NIST publication process, and to do that we need to understand what NIST is all about. A key element of NIST's mission is *private sector outreach*, and part of the way they achieve that mission is by engaging outsiders in the publication process. An Initial Public Draft (IPD) is published, followed by a period during which comments can be submitted, leading to the publication of additional drafts, and, ultimately, a final document. This stands in sharp contrast to most DoD publications that are close-held until final publication, at which time they are "lobbed over the wall" at an unprepared audience.

For NIST publications, it typically takes several months from the IPD to the final document. We have yet not even seen an IPD of SP 800-53 Rev 5. It was originally scheduled for release on 28 March 2017, but, according to a NIST announcement, that has now been delayed due to "internal review" (they hope to publish the IPD "in the very near future"). If we assume the IPD is released in April or May, it is likely the final document will not be published until November or December.

In order to fully utilize this revised SP 800-53, NIST also needs to publish a corresponding revision of SP 800-53A, with assessment procedures matching the new control set. The IPD of this document is currently slated for December of 2017, which would push final publication well into 2018.

Before the new 800-53 and 800-53A can be adopted by DoD, several additional steps must be completed, including:

- Publication of a revised edition of CNSSI 1253. The level of effort for revision of CNSSI 1253 depends on the number of substantive changes to the controls in SP 800-53 Rev 5. Unfortunately there is no visibility into the CNSS publication process; we'll only know the revised document is done when it appears on the CNSS website!

- Incorporation of new/revised controls into the eMASS database. This would be DISA's responsibility and would only occur once the NIST and CNSS documents have been finalized and published.

In other words, we are probably looking at very late 2018, or beyond, before DoD system owners will need to address any of this in their RMF packages.

In their announcement of SP 800-53 Rev 5, NIST gives some insight into the new content we can expect, and much of it will not materially affect the controls.

Here are some examples:

See *Big Changes Coming?*, Page 2

BAI Announces eMASS Training Program

By P. Devon Schall, CISSP

We are pleased to announce that eMASS training will now be available from BAI to complement our *RMF for DoD IT* training program.

Course Content

Our initial course offering, *eMASS eSSENTIALS*, is a one-day session in which we provide "how to" guidance for the most commonly-used eMASS functions, including:

- System Registration
- Security Controls and Test Results
- Artifacts
- Asset Manager
- Plan of Action and Milestones (POA&M)

Who Should Attend

eMASS eSSENTIALS is open to all students with an interest in eMASS, particularly those who have previously completed *RMF for DoD IT Fundamentals* and *RMF for DoD IT In Depth* classes.

Students who have not yet attended RMF training are encouraged to inquire about discounted pricing for a training package that includes *RMF for DoD IT Fundamentals*, *RMF for DoD IT In Depth*, and *eMASS eSSENTIALS*.

eMASS eSSENTIALS includes "simulated live operation" of eMASS, however students are not required to have an eMASS account, or even a DoD Common Access Card (CAC), to attend.

Delivery Methods

eMASS eSSENTIALS will initially be offered as an online, instructor-led class, using our Online Personal Classroom™ technology.

eMASS eSSENTIALS will also be available as a "Friday supplemental class" to organizations wishing to obtain "on site" RMF training for a group of students.

Learn More

For additional information on eMASS training, including initial dates for *eMASS eSSENTIALS*, please call BAI at 1-800-RMF-1903 or visit https://register.rmf.org.

***Big Changes Coming?* from Page 1**

"… we are probably looking at very late 2018, or beyond, before DoD system owners will need to address any of this..." *owners will*

- The phrase "information system" will be replaced by "system" in order to make the document applicable to a wider variety of systems, such as industrial and process control systems, cyber physical systems, weapon systems, and even "Internet of Things" (IoT) devices.
- The wording (but not the intent) of the controls will change to make them more "outcome based". For example, a control such as "The organization will implement multi-factor authentication…" will now be stated-as "Implement multi-factor authentication…".
- The Program Management (PM) family of controls and the Privacy controls will be moved into a single Appendix along with the 17 primary security control families.
- The "federal focus" of the document will be de-emphasized to encourage its use by non-federal organizations such as state and local governments, private industry and academia.

As we learn more about SP 800-53 Rev 5, we will share our insights in future issues of *RMF Today … and Tomorrow*.

Top Ten—Things You Should Know about eMASS

By Lon J. Berman, CISSP

The Enterprise Mission Assurance Support Service, or eMASS, is a web-based Government off-the-shelf (GOTS) solution that automates a broad range of services for comprehensive, fully-integrated cybersecurity management, including controls scorecard measurement, dashboard reporting, and the generation of Risk Management Framework (RMF) package reports.

If you're not yet using eMASS to support your RMF activities, here are 10 things you probably need to know. If you're already using eMASS, please read on; you'll probably learn a few new things!

10. eMASS is not a single, integrated system. There are actually separate eMASS "instances" (i.e., databases) for each DoD component (e.g., Army, Navy, Air Force, DISA, NGB, DHRA, DAU, etc.). There is limited ability for one database to "reach across" to another (e.g., to implement control inheritance).

9. A few DoD components are <u>not</u> currently using eMASS because they have "standardized" on a different tool for RMF support. Even within DoD components that are "standardized" on eMASS, there may be individual commands or programs that are not participating.

8. Each DoD component has its own process for access approval. In most cases, a DD 2875 form is required, along with evidence of completion of DISA eMASS training (see below).

7. DISA provides a short online eMASS training course that is required in order to obtain an account, as well as limited classroom training. Commercial training providers offer various in-depth online and classroom training programs.

6. Access to eMASS requires a DoD Common Access Card (CAC) - *no exceptions*!

5. Most eMASS databases are accessible from NIPRNET only (not internet). This can be problematic for contractors who typically work off-site. In those cases, the DoD customer needs to provide some sort of "remote access" solution (e.g., VPN, Citrix, VDI) that enables off-site contractors to get "virtual" NIPRNET access. A few of the eMASS databases (e.g., Navy, DHRA) are directly accessible to off-site contractors from internet.

4. In addition to the eMASS account itself, users must be assigned to specific "roles" within the various "systems" that give them permission to read and/or write information in the record. In general, an eMASS user can only "see" systems in which he/she has been assigned a role. (Note: at least one of the eMASS "instances" had less restrictive permissions in which all users had read access to all systems; to the best of our knowledge, that is no longer the case.)

3. eMASS now requires all users to log in at least once every 35 days; accounts left "dormant" for more than 35 days are automatically deactivated. If you have an account on more than one eMASS "instance" (e.g., Army and Air Force), you will need to log in at least once every 35 days on *each* instance.

2. eMASS also enforces an "inactivity timeout" for logged-in users. If you do not click on anything or type anything for 30 minutes, your session is terminated and you will have to log into eMASS again in order to continue your work.

1. If you have an eMASS account, you should periodically receive e-mail messages from DISA informing you of planned outages, system upgrades, etc. Please read these carefully. NOTE: Do <u>not</u> access eMASS during any announced outage period; you <u>may</u> be able to successfully log in, but information you enter may not be saved!

Security Control Spotlight— "Naming" of Controls, Enhancements and CCIs

By Kathryn M. Daily, CISSP

After assisting numerous customers with their RMF efforts, we have seen several instances of confusion arise concerning the "naming" or "numbering" of Security Controls, Control Enhancements, and Control Correlation Identifiers (CCIs). We hope this short tutorial will help to clarify things.

Security Controls. Security Controls are organized into 18 primary families. Additionally, there are 8 families of Privacy Controls. Each control family has a unique two letter identifier, such as AC for Access Control, AT for Awareness and Training, etc. Controls within each family are sequentially numbered, thus the Controls in the AC family are named AC-1, AC-2, AC-3, etc. NIST SP 800-53 contains the complete "catalog" of Security and Privacy controls. The System Categorization (Low, Moderate or High for Confidentiality, Integrity and Availability) determines the precise set of controls applicable to a particular information system.

"...within RMF, Control Enhancements are treated as if they are simply additional Security Controls..."

Control Enhancements. Control Enhancements provide additional protection in the same general subject area as the control to which they "belong". The System Categorization determines the precise set of enhancements applicable to the information system. In NIST SP 800-53, the Control Enhancements are presented just below the description of each Control, and are sequentially numbered. Control Enhancements are named with the name of the control, followed by the sequential number in parentheses. For example, the Control Enhancements that "belong" to Security Control AC-2 are named AC-2(1), AC-2(2), AC-2(3), etc. It is important to understand that, within RMF, Control Enhancements are treated as if they are simply additional Security Controls.

Control Correlation Identifiers (CCIs). CCIs roughly correspond to Assessment Objectives, as documented in NIST SP 800-53A. Each Control is "broken down" into one or more CCIs; only when all CCIs for a particular control are assessed as compliant will the control as a whole be considered compliant. NIST SP 800-53A names the assessment objectives by the portion of the control text from which they are derived. So, for example, AC-2 has assessment objectives named AC-2(a)[1], AC-2(a)[2], etc.

DoD, specifically eMASS, does not follow the naming convention of NIST SP 800-53A. Instead, assessment objectives (and therefore CCIs) are sequentially numbered for each Control or Control Enhancement. For example:

- Assessment objectives (CCIs) for AC-2 are named AC-2.1, AC-2.2, AC-2.3, etc.
- Assessment objectives (CCIs) for control enhancement AC-2(1) are named AC-2(1).1, AC-2(1).2, etc.

People sometimes get confused between the nomenclature for control enhancements, which use parentheses, e.g., AC-2(1), and the nomenclature for CCIs, which use a period or dot, e.g., AC-2.1. It becomes even more confusing when we are talking about CCIs that belong to a control enhancement, where both nomenclatures are used together, e.g., AC-2(1).1.

Also confusing at times is the notion of overall compliance. Controls and Control Enhancements are treated as completely separate entities when it comes to compliance. A control itself can be compliant, while some enhancements are compliant and some are non-compliant. By contrast, an individual Control or Control Enhancement is only considered as compliant when all of its CCIs are compliant.

Training for Today … and Tomorrow

Our training programs:

- **RMF for DoD IT** – recommended for DoD employees and contractors that require detailed RMF knowledge and skill training; covers the RMF life cycle, documentation, security controls, and transition from DIACAP to RMF. The program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **RMF for Federal Agencies** – recommended for Federal "civil" agency (non-DoD) employees and contractors; covers RMF life cycle, NIST security controls and documentation. Program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **Information Security Continuous Monitoring (ISCM)** – open to all, however prior knowledge of RMF is recommended. This is a three day "In Depth" program.
- **Certified Cloud Security Professional (CCSP)** – recommended for government employees and contractors working (or planning to work) in the cloud environment, this five-day training program will prepare students for the CCSP certification examination given by ISC2
- **eMASS eSSENTIALS** – recommended for government employees and contractors working (or planning to work) in the DoD environment, this one-day training program provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is used to reinforce the practical skills needed to use eMASS.

Our training delivery methods:

- **Traditional classroom** – regularly-scheduled training programs are offered at various locations nationwide, including Colorado Springs, Huntsville, National Capital Region (Pentagon/Crystal City area), Orlando and San Diego.
- **Online Personal Classroom™** – regularly-scheduled training programs are also offered in an online, instructor-led format that enables you to actively participate from the comfort of your home or office
- **On-site training** – our instructors are available to deliver any of our training programs to a group of students from *your* organization at *your* site; please contact BAI at 1-800-RMF-1903 to discuss your requirements

Regularly-scheduled classes through September, 2017:

RMF for DoD IT—4 day program (Fundamentals and In Depth)

- **National Capital Region ▪ 10-13 APR ▪ 10-13 JUL**
- **Huntsville ▪ 8-11 MAY ▪ 7-10 AUG**
- **Colorado Springs ▪ 12-15 JUN ▪ 11-14 SEP**
- **Orlando ▪ 26-29 JUN ▪ 25-28 SEP**
- **San Diego ▪ 19-22 JUN ▪ 18-21 SEP**
- **Online Personal Classroom™ ▪ 17-20 APR ▪ 15-18 MAY ▪ 19-22 JUN ▪ 17-20 JUL ▪ 14-17 AUG ▪ 18-21 SEP**

RMF for Federal Agencies—4 day program (Fundamentals and In Depth)

- **Online Personal Classroom™ ▪ 22-25 MAY ▪ 25-27 JUL**

Information Security Continuous Monitoring—3 day program (In Depth class only)

- **Online Personal Classroom™ ▪ 11-13 APR ▪ 21-24 AUG**

Certified Cloud Security Professional (CCSP)—5 day program

- **National Capital Region ▪ 26-30 JUN ▪ 25-29 SEP**
- **Online Personal Classroom™ ▪ 24-28 JUL**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 31 MAY ▪ 28 JUN ▪ 26 JUL ▪ 30 AUG ▪ 27 SEP**

Registration for all classes is available at https://register.rmf.org

Payment arrangements include credit cards, SF182 forms, and Purchase Orders.

Contact Us!

RMF Today … and Tomorrow is a publication of BAI Information Security, Fairlawn, Virginia.

Phone: 1-800-RMF-1903
Fax: 540-808-1051
Email: rmf@rmf.org