Risk Management Framework Today…

and Tomorrow

October, 2020 Volume 10, **Issue 4**

Happy Birthday, RMF!

By Lon J. Berman, CISSP, RDRP

This month we will be celebrating our oldest grandson's tenth birthday. It suddenly made me realize that with everything that's been going on in 2020, it appears we missed another significant birthday this year – February marked the tenth birthday of the Risk Management Framework (RMF). You might be thinking, "Wait a minute. It can't be ten years. It seems like we didn't hear *anything* about RMF until four, maybe five years ago." Well, if you're with DoD, you may well be right. DoD did not formally adopt RMF until 2014, and it took another year or two before it even took hold in most of the DoD agencies. The big picture, however, is that RMF was initially published in NIST Special Publication (SP) 800-37 in February, 2010.

RMF is in fact the work of the Joint Task Force Transformation Initiative Interagency Working Group. If you're thinking you saw an organization by that name in a Hollywood action movie starring Morgan Freeman, you're wrong. That's the name of a real organization – you can't make up stuff like that! Let's just call them the Joint Task Force (JTF) for short. The members of JTF include representatives of DoD, the federal civil departments/agencies, and the intelligence community (IC). The purpose of JTF is to create and maintain an information security framework "for the entire federal government". Those are *their* words, but they are a bit of hyperbole. JTF has purview over the entire Executive Branch and *not* the entire federal government. It's in the Constitution, folks! Of course the lion's share of the federal government lies within the executive branch, so we'll forgive JTF for their exaggeration. JTF's mission is to unify the three "sectors" of the executive branch (DoD, civil departments/agencies and the IC) with an overarching methodology for information security management. The intent is to facilitate information sharing, particularly in programs that involve two or more of these "sectors". Working in partnership with the JTF, NIST published several documents that represented the "birth" of RMF. They then left it for the three "sectors" of the executive branch to get on board and transition from their existing Certification and Accreditation (C&A) process to RMF.

The transition was the easiest for the federal civil departments and agencies since most of them were already using a C&A process based on earlier versions of the NIST publications. They were soon followed by the intelligence community, leaving DoD bringing up the rear. Now as we all know, the wheels of change turn very slowly at DoD and there was considerable debate among the various DoD components. It wasn't about *whether* to adopt RMF. By virtue of its membership in the Joint Task Force, DoD was pretty well committed to making the transition. The debate was more about the *how*, the transition timeline, etc. Finally, in March of 2014, the DoD CIO picked up her pen and signed the publications (DoD Instructions 8500.01 and 8510.01) that marked the beginnings of what they called *RMF for DoD IT*. An interesting footnote to that story is that the pen the DoD CIO used to sign those pub-

See Birthday, Page 2 for more.

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

Risk Management Framework Today…

and Tomorrow

"With thousands of assessment procedures, even those with a strong understanding of RMF can get very overwhelmed and confused by what each security control means."

Find us on LinkedIn

BAI Information Security Consulting & Training

Birthday, Page 1

lications must have been a very heavy one – it wore her out so much that she chose to retire from government service less than two months later! The formal adoption of RMF meant DoD would finally get "in sync" with the NIST publications and JTF. It took "years and tears" for many of the DoD components to get there, but now, in 2020, DoD is firmly entrenched in RMF.

Mission accomplished? Well, not quite.

In the intervening years NIST has made some significant upgrades to the key RMF publications, and DoD has yet to get on board with some of those. In particular, the security controls and assessment procedures were significantly upgraded in NIST SP 800-53 Rev 5 and the accompanying SP 800-53A. Even the RMF process itself has been upgraded in NIST 800-37 Rev 2. It remains for DoD to update DoD Instructions 8500.01 and 8510.01 to keep pace. In other words, it's more like mission *ongoing*. Stay tuned!

Having said all of that … Happy (belated) Birthday, RMF.

New Training Opportunity!

Security Controls Implementation Workshop

By P. Devon Schall, PhD, CISSP, RDRP

If you ask an RMF practitioner what the most challenging part of the RMF process is you're likely to hear them reference responding to security controls! With thousands of assessment procedures, even those with a strong understanding of RMF can get very overwhelmed and confused by what each security control means.

Recognizing this RMF crux, BAI has created a new course titled Security Controls Implementation Workshop. Security Controls Implementation Workshop is an in-depth dive into Step 3 of the Risk Management Framework process "Implement Security Controls". Upon completion of the course, the student can confidently return to their respective organizations and ensure the highest level of success for the most difficult part of the RMF process.

The course will take the student through the entire process concentrating on key areas of the process including:

- In-depth project planning for security controls implementation.
- The concept of traceability.
- The concept of "holistic security"
- How to properly implement security controls.
- In-depth review of the most critical security controls and how to implement them.
- Review and implementation guidance for student-selected security controls.
- Documenting test results the right way.
- The role of STIGs in the process.
- And many more.

Security Controls Implementation Workshop is being offered regularly in an online, instructor-led format through our Online Personal Classroom™ technology. The schedule of classes and registration information can be found on the back page of this newsletter, or at https://register.rmf.org. Additionally, BAI instructors are available to present a private class for your organization, either online or at your site.

Risk Management Framework Today…

and Tomorrow

"If you do not have anyone in your company who is familiar with the RMF security controls or the DISA STIGs, then getting some training in those areas would also be critical."

Find us on LinkedIn

BAI Information Security Consulting & Training

Ask Dr. RMF

Do you have an RMF dilemma that you could use advice on how to handle? If so, Ask Dr. RMF! BAI's Dr. RMF is a Ph.D. researcher with a primary research focus of RMF.

Dr. RMF submissions can be made at https://rmf.org/dr-rmf/.

Tony from OSD asks:
Dr. RMF, I currently assess a boundary that includes all of our desktops, laptops, network printers, and some local printers. There are a number of devices (i.e. desktop/laptops) that don't store Personally Identifiable Information (PII) per se, but will disseminate PII to our records management boundary on a daily basis. So, my interpretation is considering we process PII within this particular boundary we (desktop environment) would require a Privacy Impact Assessment (PIA). Does this sound accurate? Any assistance you may provide would be greatly appreciated.

Dr. RMF responds:
Tony, from your description of this "workflow", Dr. RMF can see that your desktop and laptop users are gathering PII and then sending it across your system boundary into your records management systems. If that is an accurate take on what is happening on a daily basis, then absolutely your "desktop environment" would require a PIA.

Sean from US Navy asks:
Dr. RMF, we are working on an acquisition for several new medical imaging devices in our hospital. Each of these new devices contains an embedded computer running the Linux operating system. A connection to the hospital's data network is used to send imaging data to the main hospital database. Will these systems need their own RMF ATO, or can they be included in the overall system boundary of the hospital and therefore not require a separate ATO? If the new devices require their own ATO, can we add it to the vendor's scope of work or do we have to do it ourselves?

Dr. RMF responds:
Sean, the question of whether to seek a separate ATO for the new imaging devices depends on the hospital's overall Assessment and Authorization (A&A) strategy. Some facilities will lump everything into a single system boundary, while others will maintain an ATO for the network infrastructure and separate ATOs for systems connecting to the network. The best way to make that determination is to approach the Authorizing Official (AO) or his/her designated representative.
As for adding RMF to the vendor's scope of work, you can certainly do that, but keep in mind you'll need to provide more specific guidance than just "do RMF". You'll be far better off with specific tasking to the vendor, such as "evaluate your product against the following STIGs and make appropriate remediations to the system configuration to address non-compliant items".

Daphne in Kansas City asks:
Dr. RMF, we are bidding on a multi-year contract to provide services to a DoD agency. The process is down to the final stage and we are looking good to win the work. Assuming we are awarded the work, the government will be requiring us to maintain a small network of classified computers in our facility. We have a facility clearance and have been working for many years with DSS (now DCSA), but we've never had any in-house classified IT. It is our understanding we will need an ATO for these classified computers. What can you tell us about the effort involved?

Dr. RMF responds:
Daphne, the most important thing you'll need to do is to establish contact with the Information System Security Professional (ISSP) at your local DCSA office. The ISSP is the person who can give you the best advice as to the steps you'll need to take. You'll be building an RMF package in eMASS, so getting some training on that tool will be extremely helpful. If you do not have anyone in your company who is familiar with the RMF security controls or the DISA STIGs, then getting some training in those areas would also be critical. You may wish to engage the service of a consultant to help guide you through the RMF process. Dr. RMF wishes you the best of luck in your RMF journey.

Risk Management Framework Today…

and Tomorrow

"Remember to follow your data everywhere it goes once it leaves your authorization boundary!"

Find us on LinkedIn

BAI Information Security Consulting & Training

Security Control Spotlight:

AC-20 (Use of External Information Systems)

By Ernest Smith, CISSP, PMP

Requirement (simplified):
Do you have contracts and or service level agreements with the owners of any system outside of your authorization boundary that are processing, storing, and transmitting your information?

Breakdown:
What is an "external information system"?

- Employee personally owned devices (I said it!)
- Systems controlled by non-governmental organizations
- Government organization system who has an ATO signed by an AO other than yours
- Cloud service offerings

Questions:

- Is any of your information being processed, stored and transmitted by any of the above? How do authorized users access your information from this external information system?
- If yes, do you have a contract in place that outlines how your system's information will be protected from unauthorized disclosure, etc.? How detailed is that contract?
- If yes, do these systems have an ATO? Do you have a copy of that ATO?
- Are you using Office 365, Google Business, or other cloud service offering? Do you have a document where the DoD has issued that service a provisional authorization (ATO), or at least FedRamp ATO'd?

Issues:
How close are you watching your employees? What are the possibilities they have your information on their privately-owned devices? How would you know? Remember to follow your data everywhere it goes once it leaves your authorization boundary!

CMMC AB Proposes "Pay to Play" Program

By Kathryn Daily, CISSP, CAP, RDRP

On Saturday, September 12th, the CMMC Accreditation Body (AB) posted a page to their website that advertised for a "Partnership Program" where contracting companies could pay up to $500,000 for a CMMC AB stamp of approval. The proposed program consists of five levels ranging from Bronze ($5,000) to Diamond ($500,000). As the cost goes up, so do the perks. Each level is limited in the number of contracting companies that can partake with Bronze allowing 50 spots, up to Diamond that only allows three.

Almost immediately, this announcement sparked outrage on LinkedIn. If you do a content search for "CMMC Pay to Play" plenty of posts come up with people pointing out the pay to play nature of the program and pointing out the conflict of interest with the CMMC AB taking sponsorship money from the very organizations they are responsible for accrediting.

Following the online outrage, the CMMC AB took the page down. Mark Berman (no relation to BAI's own Lon Berman), the CMMC AB Communications Committee Chair, stated, "We decided to revisit the page before reposting it, as is noted on the page. There is nothing else to share on the matter."

Katie Arrington, DoD's Chief Information Security Officer for acquisition and sustainment, wrote the following in a LinkedIn post, "Although the idea to look for ways to lower the cost for certification training is admirable, we in the DoD can't condone sponsorships for this nonprofit because the cause is so very critical to national security." A DoD spokesperson added the following statement, "The Department of Defense was unaware of the CMMC Accreditation Body's intent and would not embrace any activity that would pose a potential or perceived conflict of interest."

Furthermore, it appears that the full board was not consulted prior to launching the program indicating that there is a serious communication issue amongst the CMMC AB. This is not the first time that financial decisions have been made without full board approval. In April, the CMMC AB put out a request for proposals for a continuous monitoring solution. That proposal had a turn around time of only nine days, which isn't enough time for a company to put together a proposal, leading many to believe that the companies preferred to win the work were notified ahead of time, leaving the others to scramble to put something together in time.

The CMMC AB clearly needs real accountability, transparency, and oversight. We can only hope that will come in the near future.

Risk Management Framework Today…

and Tomorrow

Contact Us!

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

Phone: 1-800-RMF-1903
Fax: 540-518-9089
Email: rmf@rmf.org

Registration for all classes is available at

https://register.rmf.org

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

Find us on LinkedIn

BAI Information Security Consulting & Training

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, and security controls.
- **RMF Supplement for DCSA Cleared Contractors** – This one-day course covers the specifics of RMF as it applies to cleared contractor companies under the purview of the Defense Counterintelligence and Security Agency (DCSA). Companies holding a Facility Clearance who also maintain "on premise" information technology (such as standalone computers and small networks) will benefit from this training.
- **CMMC Readiness Workshop**—prepares DoD contractors for the impending mandatory Cybersecurity Maturity Model Certification.
- **eMASS eSSENTIALS** – provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is utilized.
- **STIG 101** – is designed to answer core questions and provide guidance on the implementation of DISA Security Technical Implementation Guides (STIGs) utilizing a virtual online lab environment.
- **Security Controls Implementation Workshop** – provides an in-depth look into Step 3 of the Risk Management Framework process Implement Security Controls. Upon completion of the course the student can confidently return to their respective organizations and ensure the highest level of success for the most difficult part of the RMF process.
- **Security Controls Assessment Workshop** – provides a current approach to evaluation and testing of security controls to prove they are functioning correctly in today's IT systems.
- **Continuous Monitoring Overview** – equips learners with knowledge of theory and policy background underlying continuous monitoring and practical knowledge needed for implementation.
- **RMF in the Cloud** – provides students the knowledge needed to begin shifting their RMF efforts to a cloud environment.

Our training delivery methods:

- **Traditional classroom**
- **Online Personal Classroom™ (live instructor-led)**
- **Private group classes for your organization (on-site or online instructor-led)**

Regularly-scheduled classes through March, 2021:

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

- **Online Personal Classroom™ ▪ 19 - 22 OCT ▪ 26 - 29 OCT ▪ 2 - 5 NOV ▪ 16 -19 NOV ▪ 7 - 10 DEC ▪ 14 - 17 DEC ▪ 11 - 14 JAN ▪ 25 - 28 JAN ▪ 1 - 4 FEB ▪ 8 - 11 FEB ▪ 22 - 25 FEB ▪ 1 - 4 MAR ▪ 15 - 18 MAR ▪ 29 MAR - 1 APR**
- **San Diego ▪ 22 - 25 FEB**
- **Pensacola ▪ 8 - 11 MAR**
- **Colorado Springs ▪ 15 - 18 MAR**
- **Virginia Beach ▪ 29 MAR - 1 APR**

RMF Supplement for DCSA Cleared Contractors—1 day program

- **Online Personal Classroom™ ▪ 27 OCT ▪ 10 NOV ▪ 19 JAN ▪ 24 MAR**

CMMC Readiness Workshop—3 day program

- **Online Personal Classroom™ ▪ 19 - 21 OCT ▪ 1 - 3 DEC ▪ 15 - 17 DEC ▪ 19 - 21 JAN ▪ 16 - 18 FEB ▪ 22 - 24 MAR**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 23 OCT ▪ 6 NOV ▪ 23 NOV ▪ 18 DEC ▪ 15 JAN ▪ 29 JAN ▪ 5 FEB ▪ 12 FEB ▪ 26 FEB ▪ 5 MAR ▪ 12 MAR ▪ 19 MAR ▪ 2 APR**
- **San Diego ▪ 26 FEB**
- **Pensacola ▪ 12 MAR**
- **Colorado Springs ▪ 19 MAR**
- **Virginia Beach ▪ 2 APR**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 30 OCT ▪ 24 NOV ▪ 11 DEC ▪ 21 JAN ▪ 16 FEB ▪ 19 MAR**

Continuous Monitoring Overview—1 day program

- **Online Personal Classroom™ ▪ 12 NOV ▪ 18 FEB**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 9 NOV ▪ 22 JAN ▪ 26 MAR**

Security Controls Implementation & Assessment Workshop—4 day program

- **Online Personal Classroom™ ▪ 25 - 28 JAN ▪ 22 - 25 MAR**

Security Controls Implementation Workshop—2 day program

- **Online Personal Classroom™ ▪ 25 - 26 JAN ▪ 22 - 23 MAR**

Security Controls Assessment Workshop—2 day program

- **Online Personal Classroom™ ▪ 9 - 10 NOV ▪ 8 - 9 DEC ▪ 27 - 28 JAN ▪ 24 - 25 MAR**

CAP Exam Preparation—1 day program

- **Online Personal Classroom™ ▪ 20 NOV ▪ 26 MAR**

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

- **Online Personal Classroom™ ▪ 22 - 25 MAR**