January, 2022 Volume 13, **Issue 1**

Risk Management Framework Today… *and Tomorrow*

In this issue:

DoD Transition to NIST SP 800-53 … Why is it Taking so Long? ……1

The Pedagogy of RMF Training ……2

FedRAMP Turns 10! ……3

Ask Dr. RMF ……4

Classroom RMF, eMASS, SCI/SCA, and STIG Training is Back! ……6

Training for Today… and Tomorrow ……7

Find us on LinkedIn

BAI Information Security Consulting & Training

DoD Transition to NIST SP 800-53 Rev 5 … Why is it Taking so Long?

By Lon J. Berman, CISSP, RDRP

Welcome to 2022! It's now been well over a year since the release of NIST SP 800-53 Rev 5, yet Rev 4 remains the DoD standard. When DoD first adopted RMF … back in 2014! … they expressed their commitment to "keeping up" with the NIST publications. So why the long delay in this case? When can we expect DoD to finally adopt Rev 5?

In a previous edition of *RMF Today … and Tomorrow* we provided a summary of the new and revised material in Rev 5, and also listed out the many "moving parts" that will need to change in order to accommodate the transition from Rev 4 to Rev 5. Prime among these is the publication of a revised CNSSI 1253, which is the governing document for selection of security controls and CCIs based on the system categorization. Until the Committee on National Security Systems (CNSS) releases a revised 1253 document, DoD will be unable to proceed with adoption of NIST SP 800-53 Rev 5. So, at least for the time being, DoD can "hide behind" CNSS as the reason for the delay.

Allegedly work is "underway" on the 1253 revision, but, again, no idea when this will actually happen. Unlike NIST, which regularly releases publication schedules and draft documents for public comment, DoD and CNSS tend to do their document development "in the dark", so to speak, before finally lobbing new publications "over the wall" and making them official. In other works, it could happen tomorrow, or it could happen in twelve months … or something in between.

Even after a new CNSSI 1253 is available, there are still numerous obstacles to overcome. First and foremost, eMASS needs to be revised to include the Rev 5 security controls and CCIs. This is a major undertaking that will involve extensive development and quality assurance work. Changes to controls and CCIs may also entail corresponding changes to DISA STIGs. The RMF Knowledge Service content will also need to be revised, particularly the Security Controls Explorer.

Finally, a "transition plan" will need to be worked out. It's clearly unrealistic to expect every DoD system to transition "overnight" to the Rev 5 control set, so some sort of phased approach will be needed. The most reasonable assumption is that each system will be expected to make the transition on its next "ATO cycle". So if your system just got its new three year ATO, you would not be expected to make the transition for another three years. So far so good. If your ATO expires in six or nine months, you would need to get cracking on making the transition ASAP. Well, OK. But, what about a system whose ATO expires in three or four months? The system owner is probably already deep in the throes of working the new ATO. What will they be expected to do? As usual, the devil is in the details, and all of this will need to be worked out before DoD can officially begin the transition.

All that said, I believe it's reasonable to expect some sort of movement on the part of DoD this year. My recommendation is to get yourself as ready as you can. Get yourself a copy of NIST SP 800-53 Rev 5 and start reading!

Risk Management Framework Today…

and Tomorrow

"In order to provide the highest training quality, we have no intentions of deviating from this educational delivery approach as we believe it is the most efficient way for our students to gain a strong understanding of RMF and the ability to work the RMF process."

Find us on LinkedIn

BAI Information Security Consulting & Training

The Pedagogy of RMF Training

By Philip D. Schall, Ph.D., CISSP, RDRP

"By far one of the best courses I have taken in a long time. I just finished up a 10-week graduate course on RMF, and I learned more in this 4-day class from Linda than I did the entire 10 weeks, best money I have ever spent!!"

- BAI RMF for DoD IT student testimonial

BAI's Mission:

To provide exceptional Risk Management Framework (RMF) training by building student confidence in their abilities to operationally engage in the RMF process as efficiently and effectively as possible.

This short article was created to educate potential BAI students on our training pedagogy.

The Case for the Online Personal Classroom™

It is no secret that the educational landscape has changed dramatically within the past few years due to the COVID-19 pandemic. One of the major changes has been a shift from in-person classroom training to online training. At BAI, we firmly believe that there is no substitute for live instructor-led training conducted by seasoned RMF practitioners. In fact, we have been approached many times about the creation of RMF eLearning courses and other asynchronous RMF training modules, but we stand firm in our belief that in order to fulfill our mission in providing the best RMF training available the ideal delivery platform is live and instructor-led. In order to provide the highest training quality, we have no intentions of deviating from this educational delivery approach as we believe it is the most efficient way for our students to gain a strong understanding of RMF and the ability to work the RMF process.

The Case for In-Person Classes

Although online training is the current trend, as Training Director for BAI, I firmly believe that for some learners, in-person training conducted in a physical classroom setting is the best delivery method for their RMF education needs. Because of this, BAI continues to offer our flagship RMF for DoD IT & Federal Agencies curriculum in physical locations throughout the US with a current rotation between Pensacola, San Diego, Colorado Springs, Washington D.C., and Huntsville. I completely understand the convenience of training remotely, but I believe that nothing can substitute the experience of sitting in a classroom without distractions and learning the RMF process while establishing a face-to-face connection with your RMF instructor. As a cybersecurity educator, I hope in the coming year we see a swing back to traditional in-person classroom training.

The Case for Intensive Four-Day RMF Training

As the above student testimonial demonstrates, many of our students feel the intensive nature of our four-day RMF for DoD IT & Federal Agencies training curriculum is the most effective approach to being able to work on RMF projects as quickly as possible and maximize return on investment. As a traditional university educator, I believe that some topics are a good fit for a full semester of education or even graduate coursework, but I firmly believe an intensive RMF deep dive is the best way for students to be able return to their office ready to get to work on RMF activities. Our traditional student population consists of students who have likely been tasked with an RMF responsibility or have been made aware of an impending RMF project coming down the pipeline. Not having a full understanding of RMF is very stressful for those with looming deadlines. In our experience, the best way to build the knowledge and confidence needed is in the delivery of intensive full-day RMF training in four consecutive days leveraging group activities and real-world examples of RMF implementation.

See The Pedagogy of RMF, Page 3 for more.

Risk Management Framework Today…

and Tomorrow

"FedRAMP launched the Marketplace which provides government agencies with a one-stop-shop for approved cloud solutions to fit their needs as well as provide a base level of assurance that the provider meets the requirements unique to the federal government."

Find us on LinkedIn

BAI Information Security Consulting & Training

FedRAMP Turns 10!

By Kathryn Daily, CISSP, CAP, RDRP

On December 8, 2021, the FedRAMP program turned 10 years old! Created in 2011, the goal for FedRAMP was to produce a cost-effective, repeatable solution for securing cloud services and cloud service providers. I think we can safely say, mission accomplished. The CGI IAAS Platform was the first CSP to be authorized through the Joint Advisory Board in 2013. FedRAMP currently has 246 (As of Jan 10, 2022) vendors approved with many more on the way! FedRAMP launched the Marketplace which provides government agencies with a one-stop-shop for approved cloud solutions to fit their needs as well as provide a base level of assurance that the provider meets the requirements unique to the federal government. Prior to FedRAMP, each federal agency had to assess cloud services that they wanted to use as apart of their Assessment and Authorization activity. With the advent of FedRAMP, the federal government adopted an assess once, use may times framework that reduced the cost and complexity for federal agencies using cloud services. FedRAMP has developed a template set for vendors to use to go through the FedRAMP approval process in an effort to streamline the documentation process, something that RMF could benefit from in my opinion. Additionally, FedRAMP has created an accreditation program for the 3PAOs (Third Party Assessment Organizations) to ensure that assessments are performed uniformly across the board.

It's been so successful, that states have started to imitate what the federal government has accomplished with their own StateRAMP to accomplish the same mission as the federal government but at the state level. While StateRAMP is still in its infancy, it shows great promise to bring the same benefits that the federal government has seen to state government.

Let's see what FedRAMP has in store for the next 10 years!

The Pedagogy of RMF, from Page 1

The Case for RMF Training

In a research study published by *Cyber Security: A Peer-Reviewed Journal* I found a direct relationship between the receipt of formalized RMF training and increased RMF efficiency and reduced overall RMF project costs. Taking this data into consideration, I suggest all parties involved in an RMF project attend live instructor-led RMF training taught by expert RMF practitioners. Through my research, I found that when workers are tasked with an RMF project and attempt to self-educate, RMF efficiency decreases and RMF project timelines and costs increase. RMF is a complicated process best taught by those with an active understanding of the intricacies of the hundreds of government documents and policies which compose RMF. Quite simply, there is no substitute for RMF training delivered by an RMF subject matter expert.

Whether RMF training is delivered in our Online Personal Classroom™ or in a physical classroom, our research and student feedback support our belief that BAI delivers an exceptional RMF training experience.

For the most up to date curriculum and training schedule, please visit www.rmf.org.

Risk Management Framework Today…

and Tomorrow

"So long as the POA&M presents a realistic plan to address the non-compliant controls, the AO should at least be willing to consider an ATO or ATO with Conditions."

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 consists of BAI's senior RMF consultants who have decades of RMF experience as well as peer-reviewed published RMF research. Dr. RMF submissions can be made at https://rmf.org/dr-rmf/.

"Overlay Layover" asks:
I'm a little bit confused about how to find available security controls overlays. According to the RMF policy (DoD Instruction 8510.01) and the RMF Knowledge Service, approved overlays can be found on the CNSS.GOV website. Well, I keep looking there and all I see are the same handful of overlays that have been there for years (classified information overlay, privacy overlay, space platform overlay, etc.) I'm quite sure lots of additional overlays have been developed, but there don't seem to be any new ones showing up. Why is that?

Dr. RMF responds:
Dr. RMF can confirm that there are in fact other overlays out there. It's not altogether clear why they haven't shown up as "official" overlays on the CNSS.GOV site. Dr. RMF suspects the process of gaining approval from CNSS may be sufficiently onerous that the overlay developers just haven't chosen to go that route. Having said that, it is worth noting that many overlays have been developed for specific "communities of interest" and have been shared by some means within the said community. For example, several overlays dealing with classified contractor systems (under DCSA purview) have been made available in "NISP eMASS", which is exclusive to that community.

"In Search of Perfection" writes:
One of my customers was told by their Security Control Assessor (SCA) that they could not get Authorization To Operate (ATO) unless their POA&M had zero open items; in other words, they are expected to be 100% compliant with all the controls in their baseline. What makes this even more ridiculous is that the system in question has no connection to any other system or network – it is literally a standalone system! Does this make any sense to you, Dr. RMF?

Dr. RMF Responds:
The short answer is "No". The decision to issue an ATO … which, by the way, belongs to the Authorizing Official (AO) and not the SCA … should be based on a judgment that the overall system risk is acceptable. Virtually every system will have some non-compliant controls – perfection is a laudable goal but rarely achievable in the real world. So long as the POA&M presents a realistic plan to address the non-compliant controls, the AO should at least be willing to consider an ATO or ATO with Conditions. That way, the system can be put into operation while the remaining non-compliant items are addressed.

Want to see more of Dr. RMF? Watch our Dr. RMF video collection at https://www.youtube.com/c/BAIInformationSecurity.

Risk Management Framework Today…

and Tomorrow

"...the DoD RMF process uses CNSSI 1253 as the process document for system categorization and security control selection. On the other hand, the Treasury RMF process will use CNSS1 1253 for systems designated as National Security Systems (NSS) only…"

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 consists of BAI's senior RMF consultants who have decades of RMF experience as well as peer-reviewed published RMF research. Dr. RMF submissions can be made at https://rmf.org/dr-rmf/.

"Identity Crisis" writes:
I am a contractor working on development of a system that is jointly owned by a DoD agency and a federal civil agency (Dept. of Treasury). My company is expected to do most of the "heavy lifting" to develop the RMF package for this system and we are terribly confused as to how we should approach this task. Our boss is not terribly understanding, he seems to think that since DoD and Treasury "both use RMF", there shouldn't be any ambiguity and our path forward is clear. How do we convince him it's harder than he thinks? Beyond that, how do you recommend we approach the RMF tasking?

Dr. RMF responds:
A system under joint ownership needs to have a single designated Authorizing Official (AO). There should be a Memorandum of Agreement (MOA) put in place between the two organizations' AOs that designates one or the other of them as the "lead" AO. This can sometimes be a long and painful process, but, fortunately, as a contractor, it will not involve you or your company!

Among the issues that will need to be "negotiated" are the RMF roles and responsibilities. It's critical that there be agreement on which RMF process and control sets are to be used. DoD RMF and Treasury RMF are certainly very similar, but there are key differences that will have to be worked out. For example, the DoD RMF process uses CNSSI 1253 as the process document for system categorization and security control selection. On the other hand, the Treasury RMF process will use CNSS1 1253 for systems designated as National Security Systems (NSS) only; all other systems will use FIPS 199 for categorization and NIST SP 800-53 for security control selection.

Want to see more of Dr. RMF? Watch our Dr. RMF video collection at https://www.youtube.com/c/BAIInformationSecurity.

Risk Management Framework Today…

and Tomorrow

Find us on LinkedIn

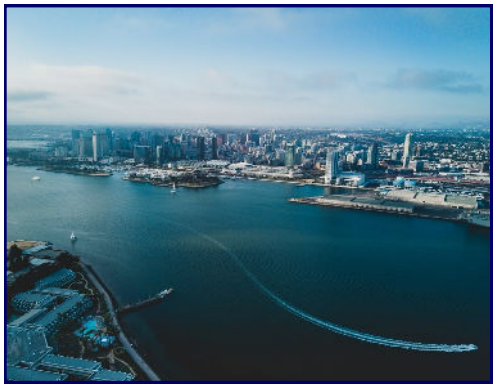
BAI Information Security Consulting & Training

Classroom RMF, eMASS, SCI/SCA, and STIG Training is Back!

BAI RMF Resource Center is pleased to announce the return of RMF, eMASS, Security Controls, and STIG training classrooms with the addition of our new locations in Colorado Springs, Pensacola, San Diego, and San Antonio!

RMF for DoD IT and Federal Agencies & eMASS eSSENTIALS ™

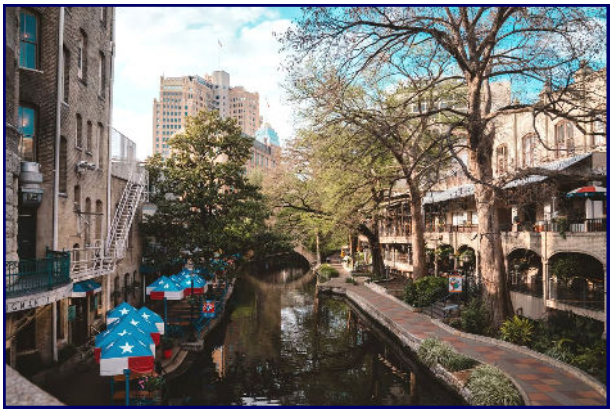
Colorado Springs, CO — February 28th – March 4th and May 23th – 27th
Pensacola, FL — April 25th – 29th
San Diego, CA — March 28th – April 1st and June 27th – July 1st



Enjoy the scenery after class in Colorado Springs (top), Pensacola (bottom left), or San Diego (bottom right)!

Security Controls Implementation and Assessment Workshop & STIG 101™

San Antonio, TX — March 21st – 25th



Students can discover and enjoy San Antonio's authentic cuisine and historic River Walk outside of class hours.

To register, contact alice@rmf.org or go to register.rmf.org.

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 for Federal Agencies** – recommended for Federal Agency employees and contractors that require detailed RMF knowledge and skill training; covers the RMF life cycle, documentation, and security controls with an additional emphasis on Federal application.
- **RMF Supplement for DCSA Cleared Contractors** – 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.
- **DFARS Compliance with CMMC/NIST SP 800-171 Readiness Workshop**—provides detailed practical application based DFARS training that will help DoD contractors work through DFARS requirements towards certification in the most efficient means possible.
- **eMASS eSSENTIALS** – provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS is exemplified in our eMASS eXPERIENCE™ simulation environment.
- **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.
- **Information Security Continuous Monitoring** – 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™ (interactive, live, instructor-led)**
- **Private group classes for your organization (on-site or online instructor-led)**

Regularly-scheduled classes through June, 2022:

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

- Online Personal Classroom™ ▪ 10 - 13 JAN ▪ 24 - 27 JAN ▪ 14 - 17 FEB ▪ 28 FEB - 3 MAR ▪ 14- 17 MAR ▪ 28 - 31 MAR ▪ 4 - 7 APR ▪ 25 - 28 APR ▪ 9 - 12 MAY ▪ 23 - 26 MAY ▪ 6 - 9 JUN ▪ 27 - 30 JUN
- Colorado Springs, CO ▪ 28 FEB - 3 MAR ▪ 23 - 26 MAY
- Pensacola, FL ▪ 25 - 28 APR
- San Diego, CA ▪ 28 - 31 MAR ▪ 27 - 30 JUN

eMASS eSSENTIALS—1 day program

- Online Personal Classroom™ ▪ 14 JAN ▪ 28 JAN ▪ 18 FEB ▪ 4 MAR ▪ 18 MAR ▪ 1 APR ▪ 8 APR ▪ 29 APR ▪ 13 MAY ▪ 27 MAY ▪ 10 JUN ▪ 1 JUL
- Colorado Springs, CO ▪ 4 MAR ▪ 27 MAY
- Pensacola, FL ▪ 29 APR
- San Diego, CA ▪ 1 APR ▪ 1 JUL

Security Controls Implementation & Assessment Workshop—4 day program

- Online Personal Classroom™ ▪ 17 - 20 JAN ▪ 7 - 10 FEB ▪ 7 - 10 MAR ▪ 18 - 21 APR ▪ 2 - 5 MAY ▪ 31 - 3 MAY ▪ 13 - 16 JUN
- San Antonio, TX ▪ 21 - 24 MAR

STIG 101—1 day program

- Online Personal Classroom™ ▪ 21 JAN ▪ 11 FEB ▪ 11 MAR ▪ 22 APR ▪ 6 MAY ▪ 17 JUN
- San Antonio, TX ▪ 25 MAR

DFARS Compliance with CMMC/NIST SP 800-171 Readiness Workshop—3 day program

- Online Personal Classroom™ ▪ 22 - 24 FEB ▪ 11 - 13 APR ▪ 21 - 23 JUN

RMF Supplement for DCSA Cleared Contractors—1 day program

- Online Personal Classroom™ ▪ 24 JUN

Information Security Continuous Monitoring—1 day program

- Online Personal Classroom™ ▪ 19 JAN ▪ 9 FEB ▪ 9 MAR ▪ 12 APR ▪ 16 MAY

RMF in the Cloud—1 day program

- Online Personal Classroom™ ▪ 20 JAN ▪ 10 FEB ▪ 10 MAR ▪ 13 APR ▪ 17 MAY ▪ 23 JUN

CAP Exam Prep—1 day program

- Online Personal Classroom™ ▪ 18 MAY