Risk Management Framework Today…

*and Tomorrow*

*April, 2022 Volume 13, **Issue 2***

# RMF for DoD IT — What Changes Might Lie Ahead?

*By Lon J. Berman, CISSP, RDRP*

Sometimes I wish I had a crystal ball I could peer into to see what is in store for the future. And nowhere do I wish for this more fervently than in the area of cybersecurity and RMF. It would be lovely to know what is lurking around the next corner, so to speak. Alas, the best we can manage is some intelligent guesswork about what lies ahead. I don't claim to be the most intelligent person around, but I have worked in this field for *decades*, and, hopefully, I've gained a little bit of insight.

Here, then, are some of my views into the future of RMF:

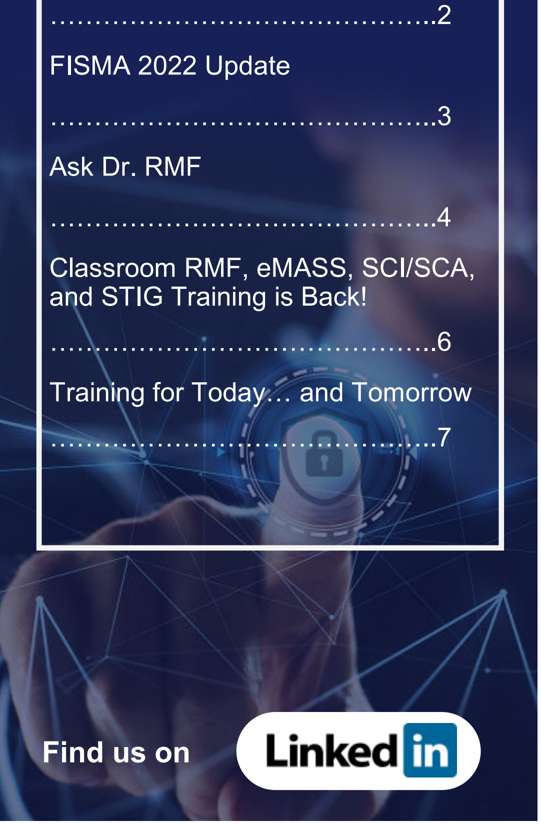
**Likely, and just around the next corner:**
It is highly likely we will be seeing an increased emphasis on Continuous Monitoring, which is Step 6 of RMF. One of the long-standing "missing pieces" in the suite of DoD RMF documentation has been a set of policies and procedures for Continuous Monitoring. DoD has recently released a policy for Ongoing Authorization (aka Continuous ATO). Ongoing Authorization enables the Authorizing Official (AO) to grant ATO "extensions" on a regular basis, as opposed to going through the full "re-authorization" process. Ongoing Authorization requires the system owner to present evidence of a robust Continuous Monitoring program in order to give the AO assurance that the security posture of the system is being maintained at a high level. My speculation is that DoD will finally respond with some meaningful "how to" guidance.

**Somewhat less likely, but still possible:**
Significant changes to eMASS might conceivably be in the cards. It is no secret that there is widespread "discontent" with eMASS, both from the user level (complexity) and at the DoD level (cost). It is *possible* DoD may be looking at wholesale replacement of eMASS with some other tool. Needless to say, that would entail a considerable expenditure and a complex "migration" process. The migration process alone is likely to be daunting to many system owners. I can only hope that DoD really, really thinks this one through before committing to some other tool. The last thing they would want to do is to end up "trading a headache for an upset stomach".

**Extremely unlikely:**
There always seems to be a little bit of "background chatter" in the cybersecurity community to the effect that DoD is looking to replace RMF with "the next big thing". My opinion is that just "ain't gonna happen". The reason is pretty simple – DoD is unable to act unilaterally. As a member of the Joint Task Force Transformation Initiative, DoD is obligated to work in concert with the federal civil agencies and the intelligence community. As difficult as it was to get consensus on RMF, there is virtually no chance that kind of consensus will happen again. Having said that, I feel compelled to add the disclaimer that "nothing is impossible", however I believe it's a fairly safe bet that there will be no wholesale replacement of RMF anytime soon.

I'm pretty confident in these "predictions", but only time will tell if my crystal ball was accurate or not!

**In this issue:**



Find us on LinkedIn

BAI Information Security Consulting & Training

Risk Management Framework Today...

*and Tomorrow*

# Observations from AFCEA West 2022 and Rocky Mountain Cyberspace Symposium 2022

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

As spring arrives, I thought it would be beneficial to share the rumblings and conversations I heard/had at AFCEA West 2022 and Rocky Mountain Cyberspace Symposium 2022 regarding my favorite topic, Risk Management Framework (RMF).

Before I dive into my RMF conference debrief, I am pleased to report that in-person conferences are back in full force!!! After the past few years of hiding in our offices in virtual meetings, the overall atmosphere of these events was very positive and full of energy! I think it is safe to say the DoD government and contractor community are ready to get back to it!

***“...RMF is not a failed framework, but the perception of failure is due to a fundamental misunderstanding of the RMF process which likely starts with Authorizing Officials (AO’s) and government leadership.”***

“Do we really need thousands of RMF controls?” The previous quote was a statement that I overheard at Rocky Mountain Cyberspace Symposium 2022 in a keynote address by a high-ranking government official. For edification, the answer to this question is YES, we really do need all of the RMF controls (if they are applicable to the system in question). The idea that RMF is failing and is inefficient is not a new one. I have previously written on this topic, and it is my belief that RMF is not a failed framework, but the perception of failure is due to a fundamental misunderstanding of the RMF process which likely starts with Authorizing Officials (AO’s) and government leadership. I have been trying for years to put together a half-day training class for AO’s without success or interest due to the busy schedule of those at the AO designation.

Below are the three themes and questions that were constant as well as my general responses.

**Theme 1: RMF has too many controls and we need to figure out a way to make RMF quicker.**

**Response:** RMF is a holistic framework. It does not focus on only technical controls. In fact, if you review most cybersecurity breaches, they often have direct relationships to poor implementation of administrative and operational controls. As an RMF practitioner, I recognize that RMF has A LOT of controls associated with systems, but we simply cannot start ignoring controls because they take too much time to respond to. Instead of trying to skip and cheat on control responses, I suggest we focus on reciprocity and trying to inherit controls from common control providers within our systems. Also, the automation of technical controls via STIG automation is a great idea, but we cannot simply ignore controls that are not technical in nature.

**Theme 2: DoD has issued a statement on continuous authorization. Do you have any information on it?**

**Response:** Yes, we saw that statement too. Unfortunately, until DoD publishes more specific continuous monitoring guidance and continuing authorization guidance in RMF Knowledge Service, we are in a holding pattern. We are very excited about this development too though and plan to create Continuous Authorization training as soon as guidance is available!

*See AFCEA Observations, Page 4 for more.*

Risk Management Framework Today...

*and Tomorrow*

***"To understand the totality of risk within the environment, agencies would be required to inventory their internet-accessible information systems and assets and allow CISA to perform risk assessments of agencies on an ongoing and continuous basis."***

**Find us on** LinkedIn

## FISMA 2022 Update

*By Kathryn Daily, CISSP, CAP, RDRP*

On February 7, 2022, The Office of the Director of National Intelligence (ODNI) released the Annual Threat Assessment of the U.S. Intelligence Community. In its assessment of Russia and their Cyber capabilities, ODNI assessed that Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities, as well as a deterrence and military tool. For a year, lawmakers in Congress have been considering a version of the Strengthening American Cybersecurity Act. With Russia's decision to attack Ukraine in February 2022 however, the senate unanimously passed the legislation.

"Cyber warfare is truly one of the dark arts specialized by Putin and his authoritarian regime, and this bill will help protect us from Putin's attempted cyber-attacks against our country," Senate Majority Leader Chuck Schumer (D-N.Y.) said on the Senate floor.

The bill contains three separate pieces of legislation:

1. **Requirement for critical infrastructure to report cyber attacks to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours**

2. **Federal Information Security Modernization Act of 2022**

3. **Federal Secure Cloud Improvement and Jobs Act of 2022**

Once the legislation passes the house, where it has broad bipartisan support, it will go to the President's desk for signature.

The FISMA update is the most significant part of the legislation. FISMA has not been updated since 2014 which is an exceptionally long time in the tech world. First, FISMA 2022 would require agency progress reports on implementing zero trust security based on the multi-year zero trust strategy with goals and milestones released last year by the White House. Additionally, FISMA 2022 pushes agencies to increase the use of automation to improve federal cyber security and visibility, as well as the use of presumption of compromise and least privilege principles to improve resiliency and timely response actions to incidents on Federal Systems. This new addition plays nicely into the Continuous Authorization to Operate (cATO) Memo released by DoD last month. FISMA 2022 also reduces FISMA reporting requirements by moving to an every two years assessment cadence from the current annual assessment requirement. To understand the totality of risk within the environment, agencies would be required to inventory their internet-accessible information systems and assets and allow CISA to perform risk assessments of agencies on an ongoing and continuous basis. Lastly, FISMA 2022 requires OMB, CISA and the National Cyber Director to develop a "risk-based budget model" for cyber security by identifying and prioritizing cybersecurity risks and vulnerabilities, including impact on agency operations in the case of a cyber-attack.

The intent of this update is to determine our federal cybersecurity posture for years to come. Hopefully not too many years before the next update! 8 years was a long time in the ever-changing tech industry!

> ***"The solution to RMF efficiency is better RMF education and cybersecurity SME's working together for evidence-based solutions vs. attempts to water down and take shortcuts when implementing RMF by making controls inaccurately not applicable."***

*AFCEA Observations, from Page 2*

**Theme 3: RMF needs to be automated. Can we just pay attention to technical controls and ignore the others?**

**Response:** This comes back to Theme 1, but this question keeps coming up. I am 100% behind the automation of the appropriate controls in the RMF process. The controls that are most likely to be automated are technical in nature and many programs are currently being developed to do this. With that said, NO, we cannot only focus on the technical RMF controls. As previously stated, if you look at major cybersecurity breaches historically, most of the impacted systems utilized non-technical controls to compromise.

Overall, when talking to RMF subject matter experts and cybersecurity personnel, the common theme was that of jaws dropping when the question was proposed if we "really need all of these controls". I sincerely hope it does not take a major breach and loss of life for DoD and the cybersecurity community to realize that we do indeed need all applicable controls. The solution to RMF efficiency is better RMF education and cybersecurity SME's working together for evidence-based solutions vs. attempts to water down and take shortcuts when implementing RMF by making controls inaccurately not applicable.

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

## 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/.**

**"Thirsty for Knowledge" asks:**
About a year ago I completed the 4-day RMF for DoD IT training with BAI. It was time well spent and has helped me in numerous ways. Now I'm searching for additional training that can help me build on the knowledge I gained in that RMF class. Do you offer any kind of "Advanced RMF" curriculum?

**Dr. RMF Responds:**
Dr. RMF is glad you asked … and so glad you found the RMF for DoD IT training helpful to you! Actually we have several training offerings that can complement your RMF training. If your RMF responsibilities include securely configuring servers and software, you should definitely consider our STIG 101™ one-day class. If your responsibilities include implementation of security controls and preparation for assessment, you might want to consider our "Security Control Implementation and Assessment" 4-day training program. This class includes a "deep dive" into the nuances of security control implementation as well as guidance to help you prepare for your independent assessment. Also, we have several one-day supplemental classes that cover specific topic areas. Depending on your specific role in the RMF process, any or all of these may be directly […]

*See Dr. RMF, Page 5 for more.*

***"DoD tends to work on new and updated RMF publications "in private" so to speak, and then just "throws them over the wall" when they are done. Drafts are rarely made available for review."***

***Dr. RMF, from Page 4:***

[…] applicable to you. Our two most popular one-day classes are called eMASS eSSENTIALS and STIG 101. If you are responsible for using eMASS to manage your RMF effort, you definitely should consider taking the eMASS class. This class literally includes "hands on" exposure to eMASS using our exclusive eMASS eXPERIENCE™ simulator. And finally, if you plan on taking the Certified Authorization Professional (CAP) exam, you may want to consider our one-day CAP Exam Prep class that builds on your RMF training to provide specific exam guidance, practice questions, etc.

**"Just want to be informed" writes:**
As a consultant, I try very hard to keep up with all the RMF publications so I can best serve my clients. On the NIST website I found a mailing list you can subscribe to. I signed up and now I receive regular e-mails from NIST when any of their publications are updated. They also send me notifications when draft publications are available for review, and I even get the opportunity to send in comments. I've been looking for a similar service from DoD but I've had no luck finding anything. So, Dr. RMF, do you know of any way I can receive notification of new or updated DoD publications?

**Dr. RMF Responds:**
I agree the NIST mailing list is wonderful, but, to the best of my knowledge, there is nothing like that available from DoD. DoD tends to work on new and updated RMF publications "in private" so to speak, and then just "throws them over the wall" when they are done. Drafts are rarely made available for review.

That said, there are some things you can do to stay informed. Dr. RMF recommends you monitor the Recent Publications page on the DoD Issuances website (https://esd.whs.mil/Directives/Recent-Publications). Also, make sure you visit the RMF Knowledge Service (https://rmfks.osd.mil) regularly.

By the way, one notable exception within DoD is DISA, where you can subscribe to a mailing list for notifications regarding their Security Technical Implementation Guides (STIGs).

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

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

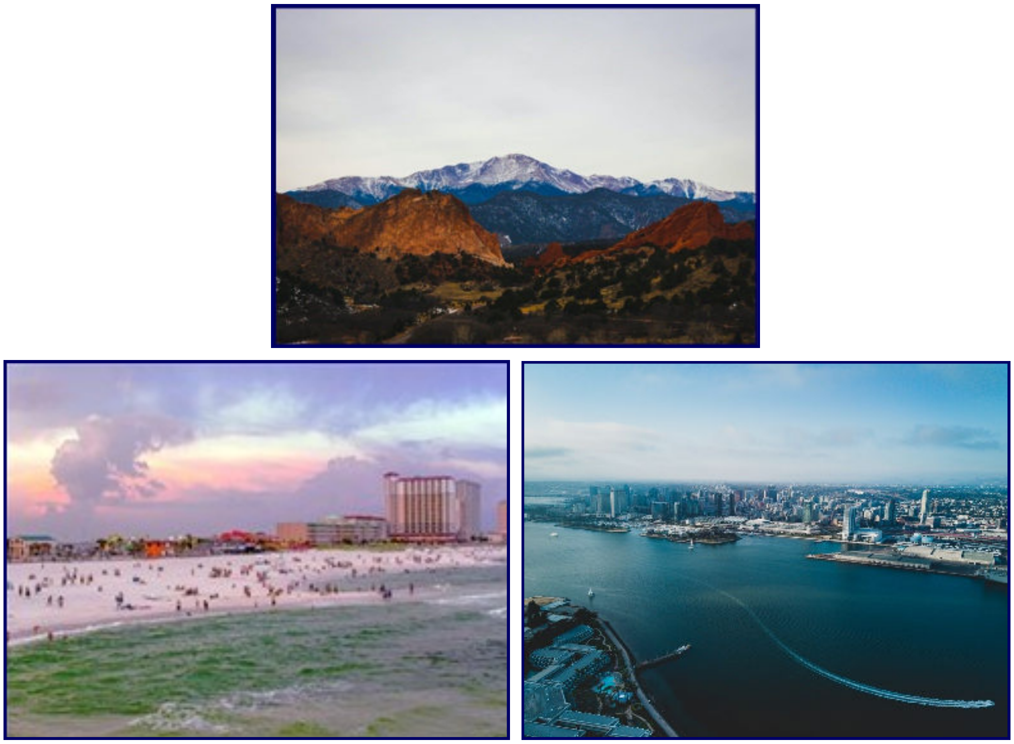
BAI RMF Resource Center is pleased to announce the return of RMF, eMASS, Security Controls, and STIG training classrooms with the addition of our new locations in Colorado Springs, Pensacola, San Diego, and San Antonio!

## RMF for DoD IT and Federal Agencies & eMASS eSSENTIALS ™

Pensacola, FL — April 25th – 29th and July 11th – 14th

Colorado Springs, CO — May 23rd – 27th and September 19th – 23rd

San Diego, CA — June 27th – July 1st and August 8th – 11th



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

**New Course Announcement: RMF for DoD IT & Federal Agencies**
*****CAP Bootcamp*****

Due to demand, BAI is now offering a CAP bootcamp taught by our in-house certification expert William Alan Matthey II, FITSP-M, CISSP/CAP/CCSP, CISM, MCSE/MCT, RDRP! This course will be focused on delivering BAI's practitioner based RMF training and prepare students to sit for the CAP exam! Seats currently available for 18-22 July and 8-12 August, sign up now!

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

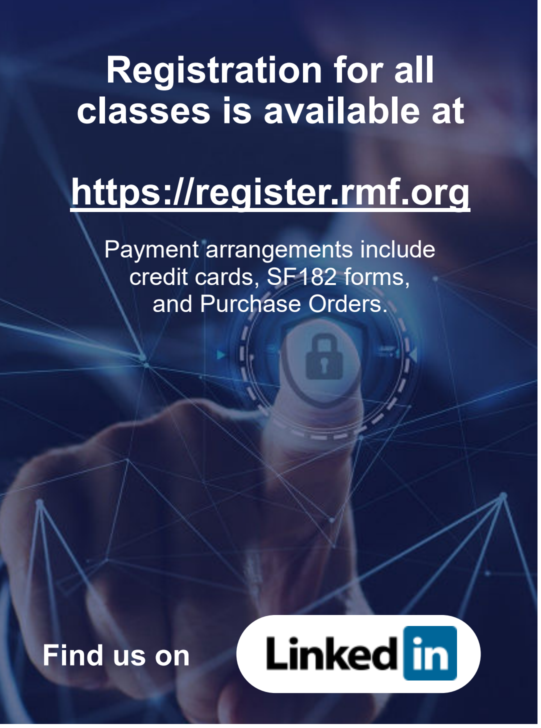
# Risk Management Framework Today…

*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).
- **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$^{TM}$ (interactive, live, instructor-led)**
- **Private group classes for your organization (on-site or online instructor-led)**

## Regularly-scheduled classes through September, 2022:

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

- **Online Personal Classroom™ ▪ 25 - 28 APR ▪ 9 - 12 MAY ▪ 23 - 26 MAY ▪ 6 - 9 JUN ▪ 27 - 30 JUN ▪ 18 - 21 JUL ▪ 25 - 28 JUL ▪ 8 - 11 AUG ▪ 29 AUG - 1 SEP ▪ 19 - 22 SEP ▪ 26 - 29 SEP**
- **Colorado Springs, CO ▪ 23 - 26 MAY ▪ 19 - 22 SEP**
- **Pensacola, FL ▪ 25 - 28 APR ▪ 11 - 14 JUL**
- **San Diego, CA ▪ 27 - 30 JUN ▪ 8 - 11 AUG**

### RMF for DoD IT and Federal Agencies + CAP Bootcamp—5 day program

- **Online Personal Classroom™ ▪ 18 - 22 JUL ▪ 8 - 12 AUG**

### eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 29 APR ▪ 13 MAY ▪ 27 MAY ▪ 10 JUN ▪ 1 JUL ▪ 29 JUL ▪ 15 AUG ▪ 2 SEP ▪ 23 SEP ▪ 30 SEP**
- **Colorado Springs, CO ▪ 27 MAY ▪ 23 SEP**
- **Pensacola, FL ▪ 29 APR ▪ 15 JUL**
- **San Diego, CA ▪ 1 JUL ▪ 12 AUG**

### Security Controls Implementation & Assessment Workshop—4 day program

- **Online Personal Classroom™ ▪ 18 - 21 APR ▪ 2 - 5 MAY ▪ 31 MAY - 3 JUN ▪ 13 - 16 JUN ▪ 18 - 21 JUL ▪ 1 - 4 AUG ▪ 22 - 25 AUG ▪ 12 - 15 SEP**

### STIG 101—1 day program

- **Online Personal Classroom™ ▪ 22 APR ▪ 6 MAY ▪ 17 JUN ▪ 6 JUL ▪ 22 JUL ▪ 5 AUG ▪ 26 AUG ▪ 6 SEP ▪ 16 SEP**

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

- **Online Personal Classroom™ ▪ 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™ ▪ 12 APR ▪ 16 MAY ▪ 7 JUL ▪ 18 AUG ▪ 9 SEP**

### RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 17 MAY ▪ 23 JUN ▪ 8 JUL ▪ 16 AUG ▪ 7 SEP**

### Certified Authorization Professional (CAP) Supplement—1 day program

- **Online Personal Classroom™ ▪ 18 MAY ▪ 22 JUL ▪ 12 AUG ▪ 8 SEP**