RMF TODAY ...AND TOMORROW
APRIL 2023
VOLUME 15, ISSUE 2

NEWSLETTER

REFLECTIONS FROM ISSA COLORADO SPRINGS CYBER FOCUS WEEK

BY PHILIP D. SCHALL, PH.D., CISSP, RDRP

"SBOMs, Quantum Computing and Space: The Final Frontier "

Cont. on Page 2

NIST SP 800-53 REV 5 – COMING SOON TO AN RMF PACKAGE NEAR YOU

BY LON J. BERMAN, CISSP, RDRP

"It turns out it's not as simple as DoD saying "Well, there's an updated version of SP 800-53. Everyone start using it now."

Cont. on Page 3

THE CURRENT STATE OF SCAP BENCHMARKS

BY KATHRYN DAILY, CISSP, CGRC, RDRP

"As some may have heard, SCAP Compliance Checker (SCC) has lost funding from DISA as of the end of FY22. "

Cont. on Page 4

STIG 101 TRAINING UPDATED TO INCLUDE EVALUATE-STIG

BAI RMF Resource Center is pleased to announce that the STIG 101 curriculum has been updated to include Evaluate-STIG into both the lecture and the hands-on lab.

STIG 101 - Online, Instructor-Led

Friday, May 19, 2023
Friday, June 2, 2023
Tuesday, June 20, 2023

Register today at https://register.rmf.org

Risk Management Framework Today... *and Tomorrow*

In This Issue:

BAI Information Security RMF Resource Center

https://rmf.org

REFLECTIONS FROM ISSA COLORADO SPRINGS CYBER FOCUS WEEK

BY PHILIP D. SCHALL, PH.D., CISSP, RDRP

On March 30th, I had the opportunity to attend the primary conference day for Information Systems Security Association (ISSA) Colorado Springs Cyber Focus Week hosted at University of Colorado, Colorado Springs (UCCS). After traveling throughout much of the US, Colorado Springs is on the top of my list as favorite places to visit as well as always being on the shortlist of great locations to live and have a bustling DoD cyber career. The purpose of this article is to touch on the highlights and main topics of the conference.

Throughout the day, three major topics continued to reverberate, for the sake of clarity and brevity, I will list them in chronological order with a summary of each.

1. The importance of SBOM

Full disclosure here, when I first heard this term a few years ago, I initially thought it was referencing profane language, but I quickly realized no one “dropped an SBOM”. What is an SBOM you ask? Well, the acronym stands for software bill of materials (SBOM). The primary takeaway from a presentation on SBOM and some conversation with fellow RMF folks was that many think an SBOM should be a requirement from acquisitions in RMF contracts (this is unfortunately not a reality) and with so many supply chain threats every cybersecurity professional needs to be familiar with SBOM and the role it plays. For more information, I suggest visiting nist.gov and searching the term SBOM. The following link is a great start.

https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

2. Advances in Quantum Computing/Threats to Cryptography

I was anticipating more conversations on OpenAI than quantum cryptography, but quite frankly, I was relieved to be given a break from AI. Quantum cryptography came up multiple times with an excellent roundtable discussion amongst leaders in quantum during a morning session. The primary takeaways from this session were that NIST is actively pursuing post-quantum cryptographic algorithms to replace our aging cryptographic standards which are not quantum resistant. The second big moment for me in this session was that breaking RSA and predicting keys is a big concern for the future, but we do not have to panic quite yet as quantum computing still has some progress to make before becoming a significant threat. For more information, I suggest checking out the links below on NIST’s Post-Quantum Cryptography Project as well as a highly recommended book called Quantum in Pictures.

https://csrc.nist.gov/projects/post-quantum-cryptography

https://www.quantinuum.com/news/quantum-in-pictures

3. Space: The Final Frontier

Primary topics here were the infancy of cybersecurity in space and the evolving threats to the cybersecurity space landscape. I was very interested to hear that cybersecurity policy for space and satellites are currently very limited. I imagine this will be an area we will look back on in 10-20 years like I currently look at the early NIST documents during the infancy of cybersecurity. Standby for BAI’s next course offering titled RMF in Space. Following is a NIST article that has some good information.

STORY CONTINUES ON PAGE 4

ASK DR. RMF!

A reader who calls herself "Cleanup Mode" writes:

Dear Dr. RMF,

I have recently taken over responsibility for a couple of systems and the RMF packages are a mess! I'm trying to make some sense out of how they handled the STIGs and it just makes no sense to me. When I go through the STIG Viewer, I find numerous STIG items marked as Compliant, but the comments indicate they are actually not compliant and there is still work left to do. Dr. RMF, do you have any idea what might be going on? How do I address it?

Dear "Cleanup",

Dr. RMF has acquired lots of experience over the decades, but mind reading is still not part of my skill set, so I can't tell you for sure what sort of thought process led to them filling out the STIG Viewer like that. It's possible they were wanting to be sure none of their non-compliant STIG items translated into non-compliant controls when the STIG Viewer file was imported into eMASS. Dr. RMF is more than a bit surprised that sort of deception actually got past the assessor and the AO, but, as they say, stranger things have happened!

To make it right, you'll need to go back to the STIG Viewer and correct the compliance status of those STIG items, then re-import the STIG Viewer file into eMASS. You'll end up with a bunch of non-compliant controls and corresponding POA&M items you'll need to complete. Better yet, start from scratch and go through the STIGs yourself and fill out fresh STIG Viewer files and import those into eMASS. That way, you can be sure any additional "cover-ups" have been removed.

NIST SP 800-53 REV 5 – COMING SOON TO AN RMF PACKAGE NEAR YOU

BY LON J. BERMAN, CISSP, RDRP

Those of us who have worked with government information systems for a number of years have come to realize the wheels of change turn very slowly – but they do turn! Case in point – DoD adoption of NIST Special Publication (SP) 800-53 Rev 5.

As you probably know, SP 800-53 is the source of the security controls upon which the RMF process is based. NIST released Revision 5 of this publication way back in 2020, yet DoD is still relying on Revision 4 as the official source of RMF security controls. Why the long delay?

It turns out it's not as simple as DoD saying "Well, there's an updated version of SP 800-53. Everyone start using it now." There are several key dependencies, to wit:

- An updated version of NIST SP 800-53A to provide assessment procedures to match the controls in the updated SP 800-53.
- An updated version of CNSSI 1253 with security controls matching the updated SP 800-53.
- A policy specifying when existing RMF packages need to transition from SP 800-53 Rev 4 to Rev 5.
- An updated version of eMASS with security controls matching the updated SP 800-53 along with a process for transitioning an RMF package from Rev 4 to Rev 5.

Slowly but surely, NIST and DoD have been working to address these dependencies.

- NIST SP 800-53A (Assessment Procedures) has been published.
- CNSSI 1253 has been updated accordingly.
- DoD will soon release a transition policy and an updated version of eMASS supporting the SP 800-53 Rev 5 controls, as well as transition of existing RMF packages from Rev 4 to Rev 5. DoD expects formal adoption of SP 800-53 Rev 5 as soon as April, 2023 (i.e. NOW).

DoD realizes they cannot "magically" throw a switch and have tens of thousands of RMF packages updated to SP 800-53 Rev 5. Instead, they plan on adopting a more realistic phased approach to this transition. Here are some of the highlights:

- New systems or those without existing authorization will transition to the new SP 800-53 and CNSSI 1253 within six months of DoD adoption.
- Systems in the midst of RMF activities will continue using the existing versions of SP 800-53 and CNSSI 1253, but will also develop a plan for transition to the new versions, and have said plan approved by their Authorizing Official (AO).
- Systems with a current Authorization to Operate (ATO) will develop a transition plan and have said plan approved by the AO.
- In all cases, transition to the new SP 800-53 and CNSSI 1253 must take place before the next system re-accreditation date.

So that's it, right? Wellllll … not quite. Once DoD has everything in place, it will be up to each DoD component (Air Force, Army, Marine Corps, Navy, etc.) to adopt these changes as part of their information security policies and procedures. For some DoD components, adoption will come very quickly, but for others, it might take weeks … or even months! At this point we can safely say it will be happening "soon", but just how soon is still a matter of speculation. Those of us who were around for the DIACAP to RMF transition (Several years ago) will readily affirm the possibility of further delays at the component level.

STORY CONTINUES ON PAGE 4

ASK DR. RMF!

A reader who calls himself "Between a Rock and a Hard Place" writes:

Dear Dr. RMF,

My unit is in the early stages of our RMF efforts for a new information system and we are having a little bit of a "debate" about which "version" of the RMF controls we should be following. I know DoD is in the process of moving from the NIST 800-53 Rev 4 controls to the Rev 5 controls. Some folks here are saying we should stick with Rev 4 since that is the current DoD policy, while others are advising me to "lean forward" and go with the Rev 5 controls since the change is sure to happen "soon". In either case, I know it's a major effort to go through all those controls and I want to do it right. What do you recommend, Dr. RMF?

Dear Between,

All other things being equal, Dr. RMF would put himself firmly in the "lean forward" camp (i.e., go with the Rev 5 controls). That said, Dr. RMF recommends you first seek guidance from your Authorizing Official (AO). I'm hoping he or she will advise you to start with the Rev 5 control set, but you never know. Oh, and there's one more thing to keep in mind. If your organization requires you to use eMASS, you may find it will not support the Rev 5 controls until a software upgrade, not yet scheduled, occurs. You may be forced to start with the Rev 4 controls and then "convert" your RMF package after the eMASS update takes place.

THE CURRENT STATE OF SCAP BENCHMARKS & POSSIBLY THE FUTURE

BY KATHRYN DAILY, CISSP, CGRC (FORMERLY CAP), RDRP

As some may have heard, SCAP Compliance Checker (SCC) has lost funding from DISA as of the end of FY22. Their development team has been reduced to only 6 GS-13 developers. During FY23 they were able to obtain short term funding from a few government agencies and are now being funded by two anonymous donors. The have no prospects for funding for FY24. The plan as it has been communicated from the SCC dev team is that SCC will switch to a pay as you go model where government agencies (not commercial companies) will pay for the use of SCC. There is no requirement to pay, but they do provide suggested amounts with the minimum being $1500 per year. As of the newly released version (5.7.1), there is now a dialog box on every third application launch if you have not paid for it.

To their credit, since DISA dropped funding, they have been pushing out updates like I've never seen before. They have created, "enhanced" benchmarks (available on NIWC's Enhanced SCAP Content Repository (link below), and not on the DISA Cyber Exchange where the standard SCAP benchmarks are located. With this enhanced content, they have added the capability to answer manual questions through the SCC app, they also have added functionality to create the .ckl files directly in SCC. They are trying to stay relevant.
Enhanced SCAP Content Repository:
https://www.niwcatlantic.navy.mil/scap/scap-content-repository/

Note: the version numbers do differ between standard and enhanced benchmarks to allow both to be imported into SCC. The format is DISA Version + NIWC Version. For brevity, NIWC drops the leading zeros on the DISA version number, and adds their version number to the right. If DISA updates their version and NIWC does not, the first two digits will change to reflect the new DISA version while the last digit will remain the same.

Example:
Microsoft IIS 10.0 Server STIG vs Enhanced Benchmark:

- STIG Manual Version: 2.8
- Enhanced Benchmark: 2.8.2

So, what other SCAP tools exist from the DoD? I'm glad you asked! NSWC Crane has developed a tool called Evaluate-STIG that is picking up steam in the DoD. It has official approvals in DADMS for Navy, Army has it listed in eMASS with an Assess Only ATO (eMASS ID 4546), NAVAIR, and NMCI (CCSW eMASS ID 13969 and UCSW eMASS ID 14441.

While SCC provides both a command line and a graphical user interface, Evaluate-STIG is simply a PowerShell script that automatically scans and documents STIG compliance.Evaluate-STIG also has significantly more functionality. It can scan your local or remote machine(s) to identify all applicable STIGs (who hasn't forgotten a STIG or two?) and then scans the target machines for compliance with those applicable STIGs. Evaluate-STIG also automates significantly more STIGs than SCC. As of 3/16/2023, Evaluate STIG supports 81 STIGs while SCC supports only 26. Lastly, Evaluate-STIG provides the capability to create an answer key for known opens and findings that cannot be evaluated through technical means (i.e., policy checks).

While SCC has been publicly available since version 5.4, Evaluate-STIG does require a CAC to obtain.The following links will provide access to the download.

- NIPR – Unclass: https://spork.navsea.navy.mil/nswc-crane-division/evaluate-stig/-/releases
- SIPR – Unclass and CUI: https://intelshare.intelink.sgov.gov/sites/NAVSEA-RMF
- Commercial Internet w/ CAC: https://intelshare.intelink.gov/sites/NAVSEA-RMF

BAI's STIG 101 class is in the process of being updated to include Evaluate-STIG in the hands-on lab and should be complete for the April class. It is currently incorporated into the lecture.

Reflections Continued from page 2
https://www.nist.gov/speech-testimony/exploring-cyber-space-cybersecurity-issues-civil-and-commercial-space-systems

If you are looking for an ISSA Chapter to join, visit, or involve your business with, I cannot say enough positive things about the Colorado Springs chapter. They also have a symposium coming up in September called the Peak Cyber Symposium with Ron Ross as keynote which is linked below. I hope to see you there!
https://www.peakcyberco.com/

800-53 Rev. 5 Continued from page 3
Regardless of the specific timing within your DoD component, there are some things you can do now to prepare yourself. The most important of these is to familiarize yourself with NIST SP 800-53 Rev 5. Also, take a look at NIST SP 800-53A Rev 5, the new 800-53B, and the recent update of CNSSI 1253. That ought to keep you busy until the other shoe drops.

WHAT IS REGISTERED DOD RMF PRACITIONER?

The Registered DoD RMF Practitioner (RDRP) program was created in response to BAI RMF Resource Center recognizing the need for a credential which shows competency and proficiency in the understanding and application of RMF for DoD. RDRP is comprised of a network of information security professionals specializing in supporting Risk Management Framework (RMF) in the Department of Defense (DoD) programs. The requirements to join RDRP are very straightforward:

Step 1: Attend 4 days or more of RMF for DoD IT training.
Step 2: Remit the initial credentialing fee.
Step 3: Complete the 50 questions "RMF for DoD IT Competency Test" with a passing score of 70%.

Being part of the RDRP registry not only adds credentialing value, but it also shows employers and government officials that registrants have a comprehensive understanding of RMF as it is implemented within DoD. Registrants are also joining a community that fosters RMF inquiry as well as networking opportunities amongst colleagues.

The only cost associated with becoming an RDRP is a one-time $100 administration fee that covers program administration. Once an RDRP candidate passes the RDRP exam and remits their $100 registration fee, they will become a lifetime RDRP member.

BAI's students who have completed 4-days or more of RMF DoD IT training may go to rmf.org/rdrp to begin the registration process.

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

What are People are Saying About Us?

Looking Forward to the Next One
"Excellent course! Great content for even those of us with limited experience in the DOD/Compliance space. Looking forward to the next one."
- Sanford
Epirus

Phenomenal
"The instructor for this course was phenomenal. Her knowledge of RMF was very helpful in answering some scenarios that I was confused on."

- Darrell
DoD Army Futures Command

Fantastic Real-World Experience
"The class was great. The instructor had fantastic real-world experience to share that helped to solidify the concepts."

- Matthew
National Guard

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).
- **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.
- **RMF Project Management Advantage –** provides "how to" guidance for the most commonly-used RMF strategies in project management.
- **RMF and Supply Chain Security -** equips personnel to develop a tailored C-SCRM program that is cost effective and addresses the necessary supply chain requirements.

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 SEPTEMBER, 2023:

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

- Online Personal Classroom™ ▪ 8-11 MAY ▪ 12-15 JUN ▪ 26-29 JUN ▪ 17-20 JUL ▪ 31 JUL-3 AUG ▪ 7-10 AUG ▪ 28-31 AUG ▪ 11-14 SEP ▪ 25-28 SEP
- Colorado Springs, CO ▪ 22-25 MAY ▪ 14-17 AUG
- San Diego, CA ▪ 26-29 JUN ▪ 25-28 SEP
- Pensacola, FL ▪ 17-20 APR ▪ 10-13 JUL

eMASS eSSENTIALS—1 day program

- Online Personal Classroom™ ▪ 12 MAY ▪ 16 JUN ▪ 30 JUN ▪ 21 JUL ▪ 4 AUG ▪ 11 AUG ▪ 1 SEP ▪ 6 SEP ▪ 15 SEP ▪ 29 SEP
- Colorado Springs, CO ▪ 26 MAY ▪ 18 AUG ▪
- San Diego, CA ▪ 30 JUN ▪ 29 SEP
- Pensacola, FL ▪ 21 APR ▪ 14 JUL ▪

Security Controls Implementation & Assessment Workshop—4 day program

- Online Personal Classroom™ ▪ 24 - 27 APR ▪ 15 - 18 MAY ▪ 5 - 8 JUN ▪ 24-27 JUL ▪ 21-24 AUG ▪ 18-21 SEP

STIG 101—1 day program

- Online Personal Classroom™ ▪ 19 MAY ▪ 2 JUN ▪ 20 JUN ▪ 6 JUL ▪ 4 SEP

Information Security Continuous Monitoring—1 day program

- Online Personal Classroom™ ▪ 30 MAY ▪ 21 JUN ▪ 28 JUL ▪ 25 AUG

RMF in the Cloud—1 day program

- Online Personal Classroom™ ▪ 1 JUN ▪ 22 JUN ▪ 5 JUL ▪ 7 SEP

RMF Project Management Advantage (PMA)—1 day program

- Online Personal Classroom™ ▪ 9 JUN ▪ 22 SEP

RMF and Supply Chain Security—1 day program

- Online Personal Classroom™ ▪ 23 June ▪ 7 JUL ▪ 8 SEP