Risk Management Framework Today…

and Tomorrow

October, 2021 Volume 12, **Issue 3**

AI Risk Management Framework (AI RMF): A Discussion of NIST's Recent RFI

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

I consistently experience two common scenarios at almost every DoD cybersecurity conference I attend. The first generally revolves around a high-ranking DoD official giving a presentation and RMF being referenced in a negative light with implications that RMF needs to be more efficient and effective or is possibly failing. This is followed by the folks around me having conversations about how RMF does not scale and is inefficient. The second scenario usually occurs in conversation with a vendor or a tradeshow attendee with themes of RMF automation.

Abridged RMF processes are familiar to the RMF community. Some prime examples of abridged RMF include the RMF Sentinel Project championed by Nancy Kreidler at CIO/G-6 as well as a similar program informally titled RMF Sprint which was implemented by the Air Force around 2017. I am confident other commands have also created their own abridged RMF programs like Sentinel and Sprint with varying levels of success. This article is not intended to provide a review of abridged RMF programs, but I think the mention of these programs are important to demonstrate that RMF inefficiency and automation topics have been an active conversation in the RMF community for many years.

NIST issued a Request for Information (RFI) titled Artificial Intelligence Risk Management Framework on July 29th 2021 which can be found at the following link: https://www.federalregister.gov/documents/2021/07/29/2021-16176/artificial-intelligence-risk-management-framework

According to the RFI the AI Framework should "provide a prioritized, flexible, risk-based, outcome-focused, and cost-effective approach that is useful to the community of AI designers, developers, users, evaluators, and other decision makers and is likely to be widely adopted." Additionally, RFI lists the following eight summarized RMF development attributes:

1. "Be consensus-driven and developed and regularly updated through an open, transparent process"
2. "Provide common definitions" for terms like "trust" and "trustworthiness"
3. "Use plain language that is understandable by" and useful to "a broad audience"
4. "Be adaptable to many different organizations, AI technologies, lifecycle phases, sectors, and uses"
5. "Be risk-based, outcome-focused, voluntary, and non-prescriptive"
6. "Be readily usable as part of any enterprise's broader risk management strategy and processes"
7. "Be consistent, to the extent possible, with other approaches to managing AI risk"; and
8. "Be a living document."

Goals of the RFI are then outlined which essentially involve the collection of experiences and ideas based on practitioners and researcher's implementation of AI. This is then followed by a more granular 12-topic focus.

See AI RMF, Page 4 for more.

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

Risk Management Framework Today…

and Tomorrow

"[Until] all STIGs are accounted for, you cannot state with confidence that your security control baseline is complete."

Find us on LinkedIn

BAI Information Security Consulting & Training

STIGs and the Security Control Baseline

By Lon J. Berman, CISSP, RDRP

So, you've got your System Categorization completed and you've included any applicable overlays. You've reviewed all the resulting security controls to see if any of them should be marked Not Applicable, and, for those, you've written a justification. You've even gone through the security controls "catalog" in NIST SP 800-53 to see if there are any security controls that should be added to your baseline!

Good job! Your security control baseline is complete and ready for approval by your Authorizing Official.

Uh … not so fast! If you haven't accounted for all the applicable Security Technical Implementation Guides (STIGs), your security control baseline may not be as complete as you thought.

As you probably know, there are STIGs that apply to numerous software components and processes within your system boundary, such as your operating systems (Windows, UNIX, etc.), database management systems (Oracle, SQL Server, etc.), web servers (Apache, Microsoft IIS, etc.), web browsers (Edge, Chrome, etc.)), commercial off-the-shelf software (COTS) products (Microsoft Office, Java, Microsoft .NET framework), network devices (firewalls, switches, etc.) and even software design/development (Application Security and Development, etc.).

Each STIG contains numerous (frequently *hundreds*) of individual items that may entail specific system settings or file permissions, system management processes, etc. Among the numerous pieces of information included with each STIG item is a "mapping" to a particular CCI (i.e., a sub-part of a security control). *If that particular control is not currently part of your system's security control baseline, it needs to be added!*

So, until all STIGs are accounted for, you cannot state with confidence that your security control baseline is complete. Depending on your system categorization level and the number of applicable STIGs, you may find a substantial number of new controls will be added.

If your organization uses the eMASS tool to manage your RMF package, you are fortunate in this respect. If you are properly importing your STIG checklists into eMASS, the required controls will be *automatically* added to your security control baseline. You will then need to go back into each of the added security controls and provide responses (and artifact references) for those parts (CCIs) of the new controls that were *not* automatically covered by the STIG item.

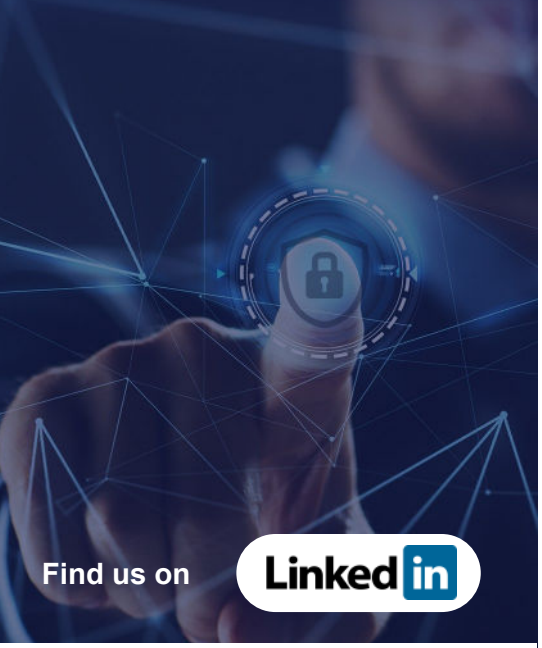
I know, you're probably thinking "Oh, just what I needed … *more* security controls to deal with!" Alas, I hate being the bearer of bad news.

But I do have some good news. I just saved 15% on my car insurance by switching to… :)

Risk Management Framework Today…

and Tomorrow

"Most ransomware attacks are made possible by users who engage in unsafe practices, administrators who implement insecure configurations, or developers who have insufficient security training. All users, regardless of function, should be informed, and trained, in security mechanisms within their role in the system."



Find us on LinkedIn

BAI Information Security Consulting & Training

NIST Creates CSF Ransomware Profile

By Kathryn Daily, CISSP, CAP, RDRP

Ransomware is one of the top buzzwords you here today in reference to cybersecurity with good reason. Ransomware attacks nearly doubled in the first half of 2021. Thanks to NIST, organizations now have a framework of security objectives that support preventing, responding to, and recovering from ransomware threats and to deal with the potential consequences of events.

"Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access."

As you know, the Cybersecurity Framework functional categories are as follows: Identify, Protect, Detect, Respond, and Recover. The Ransomware Profile applies security objectives to those categories to wit:

Identify: An inventory of physical devices should be undertaken, reviewed, and maintained to ensure there is no unprotected vector for a ransomware attack. A hardware inventory will also be necessary during the recovery phase, should a reinstallation of applications be necessary. Software inventories may track information such as software name, version, etc., devices where it's currently installed, last patch date, and current known vulnerabilities. This information supports the remediation of vulnerabilities that could be exploited in ransomware attacks. Organizational communications and data flows are mapped to enumerate what information or processes are at risk, should the attackers move laterally within the environment. External information systems must be catalogued so that organizations can communicate to partners and possible actions such as temporarily disconnection from external systems in response to ransomware events. Resources such as: hardware, devices, data, time, personnel, software, etc., should be prioritized based on their classification, criticality, and business value in order to understand the true scope and impact of ransomware events and is an important factor in contingency planning for future ransomware events, responses, and recovery actions.

Protect: Most ransomware attacks are conducted through network connections and ransomware attacks often start with credential compromise. Proper credential management is an essential mitigation. Additionally, most ransomware attacks are conducted remotely. Management of privileges associated with remove access can help to maintain the integrity of systems and data files to protect against insertion of malicious code and exfiltration of data. Using token-based multifactor-authentication will reduce the likelihood of account compromise. Network segmentation or segregation can limit the scope of ransomware events by preventing malware from proliferating among potential target systems. Most ransomware attacks are made possible by users who engage in unsafe practices, administrators who implement insecure configurations, or developers who have insufficient security training. All users, regardless of function, should be informed, and trained, in security mechanisms within their role in the system.

Detect: Multiple sources and sensors along with a security information and event management (SEIM) solution would improve early detection of ransomware. Determining the impact of

See Ransomware, Page 4 for more.

Risk Management Framework Today…

and Tomorrow

"Although it is far too early to tell what will come out of this initiative, it is important that NIST is looking at the future of AI to create more efficiency in RMF and address perceived weakness."

Find us on LinkedIn

BAI Information Security Consulting & Training

AI RMF, from Page 1

This RFI sets the stage for a collaborative process between NIST and the industry in the formal exploration of AI and RMF. In the immediate future, NIST is hosting a public workshop on 19-21 October.

It is also of note that NIST has provided in the link below initial comments on the AI RMF process: https://www.nist.gov/itl/ai-risk-management-framework/comments-received-rfi-artificial-intelligence-risk-management

Overall, I commend NIST for formally starting a conversation on AI and RMF. I think this reflects new leadership at NIST with Victoria Pillitteri assuming the role of Acting Manager for the Security Engineering and Risk Management Group. Although it is far too early to tell what will come out of this initiative, it is important that NIST is looking at the future of AI to create more efficiency in RMF and address perceived weakness. With that being said, the nature of RMF involves subjective risk-based decisions that in my opinion should not be fully automated. Research has shown that automated tools can lead to users being less engaged and focused due to the assumption of the automated process completing the intended goal on their behalf. I believe that RMF can be made more efficient with AI, but it is critical that major RMF elements that rely on human interaction are not automated such as informal risk assessments and authorization decisions. Although AI RMF is in its infancy, I intend on tracking this very closely and will be writing additional articles on the topics after attending the October workshop.

Ransomware, from Page 3

events can inform response and recovery priorities. This information should be in the contingency planning documentation. Network monitoring might detect intrusions before malicious code can be inserted or large volumes of information are encrypted or exfiltrated. Monitoring personnel activity might detect insider threats or insecure staff practices or compromised credentials and thwart potential ransomware events. Vulnerabilities can be exploited during a ransomware attack. Regular vulnerability scans can allow an organization to detect and mitigate most vulnerabilities before they are used to execute ransomware.

Respond: Response to ransomware events include both technical and business responses. An efficient response requires all parties to understand their roles and responsibilities. Coordination priorities include stemming the spread of misinformation as well as preemptive messaging. Information sharing may also yield forensic benefits and reduce the impact and profitability of ransomware attacks. Forensics help identify the root cause to contain and eradicate the attack, including things like resetting passwords of credentials stolen by the attacker, deleting malware used by the attacker, and removing persistence mechanisms used by the attacker.

Recover: Immediate initiation of the recovery plan after the root cause has been identified can cut loses. Recovery plans must incorporate lessons learned to minimize the probability of future successful ransomware attacks.

Risk Management Framework Today…

and Tomorrow

"...most DoD systems are not NSS. NIST Special Publication 800-59 provides the criteria for determining whether or not a system is NSS. All classified systems are NSS, but unclassified systems are only NSS if they meet one or more of seven specific criteria…"

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/.

Meredith writes:
Hi Dr. RMF! We are working on the RMF package in eMASS for a new system and there is a check box labeled "National Security System". We're not sure whether to check this box or not. One of my colleagues thinks we should check the box because "all DoD systems are considered National Security Systems". That sounds plausible, but still I'm not sure. I'm afraid if we check that box it will have undesirable effects, like adding more security controls to our baseline. Please, Dr. RMF, can you give us some assistance on this?

Dr. RMF responds:
It does seem plausible to think all DoD systems are National Security Systems (NSS). After all, aren't we supposed to use CNSSI 1253 to guide us through system categorization and security control selection … and CNSS stands for the Committee on *National Security Systems*? Alas, it is not true. In fact, most DoD systems are not NSS. NIST Special Publication 800-59 provides the criteria for determining whether or not a system is NSS. All *classified* systems are NSS, but unclassified systems are only NSS if they meet one or more of seven specific criteria, such as intelligence activities or command and control of military forces.

That being said, why does DoD require the use of CNSSI 1253 on all systems, regardless of whether they are NSS or not? The answer is that DoD wanted to leverage the system categorization methodology as defined in CNSSI 1253, i.e., to have separate categorization for Confidentiality, Integrity, and Availability. Outside of DoD, CNSSI 1253 is only used for NSS. Non-NSS are categorized using FIPS 199, which results in just a single categorization level of High, Moderate or Low.

Anyway, in your case Dr. RMF recommends you consult your system owner to help in making this determination. And, by the way, you can rest easy about that check box – near as we can tell, it is informational only and does not have any undesirable side-effects.

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 Alexandria South and San Antonio!

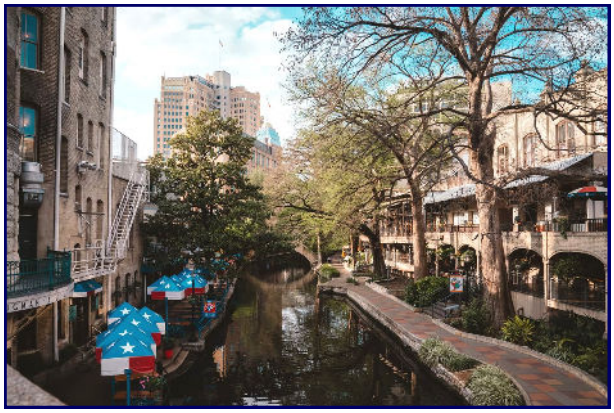
RMF for DoD IT and Federal Agencies & eMASS eSSENTIALS ™

Alexandria, VA (Fort Belvoir area) — January 24th – 28th
Colorado Springs, CO — February 28th – March 4th
Huntsville, AL — November 1st – 5th
San Diego, CA — October 18th – 22nd and March 28th – April 1st

Enjoy the scenery after class in Alexandria (Fort Belvoir Area, top left), Colorado Springs (top right), Huntsville (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 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 March, 2022:

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

- **Online Personal Classroom™ ▪ 18 - 21 OCT ▪ 25 - 28 OCT ▪ 1 - 4 NOV ▪ 15 - 18 NOV ▪ 13 - 16 DEC ▪ 10 - 13 JAN ▪ 24 - 27 JAN ▪ 14 - 17 FEB ▪ 28 FEB - 3 MAR ▪ 14 - 17 MAR ▪ 28 - 31 MAR**
- **Colorado Springs, CO ▪ 28 FEB - 3 MAR**
- **Huntsville, AL ▪ 1 - 4 NOV**
- **San Diego, CA ▪ 18 - 21 OCT ▪ 28 - 31 MAR**
- **Alexandria, VA (Fort Belvoir area) ▪ 24 - 27 JAN**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 22 OCT ▪ 29 OCT ▪ 5 NOV ▪ 19 NOV ▪ 17 DEC ▪ 14 JAN ▪ 28 JAN ▪ 18 FEB ▪ 4 MAR ▪ 18 MAR ▪ 1 APR**
- **Colorado Springs, CO ▪ 4 MAR**
- **Huntsville, AL ▪ 5 NOV**
- **San Diego, CA ▪ 22 OCT ▪ 1 APR**
- **Alexandria, VA (Fort Belvoir area) ▪ 28 JAN**

Security Controls Implementation & Assessment Workshop—4 day program

- **Online Personal Classroom™ ▪ 1 - 4 NOV ▪ 29 NOV - 2 DEC ▪ 13 - 16 DEC ▪ 17 - 20 JAN ▪ 7 - 10 FEB ▪ 7 - 10 MAR**
- **San Antonio, TX ▪ 21 - 24 MAR**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 29 OCT ▪ 3 DEC ▪ 9 DEC ▪ 17 DEC ▪ 21 JAN ▪ 11 FEB ▪ 11 MAR**
- **San Antonio, TX ▪ 25 MAR**

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

- **Online Personal Classroom™ ▪ 6 - 8 DEC ▪ 22 - 24 FEB**

RMF Supplement for DCSA Cleared Contractors—1 day program

- **Online Personal Classroom™ ▪ 10 NOV**

Information Security Continuous Monitoring—1 day program

- **Online Personal Classroom™ ▪ 7 OCT ▪ 9 NOV ▪ 10 DEC ▪ 19 JAN ▪ 9 FEB ▪ 9 MAR**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 8 OCT ▪ 12 NOV ▪ 8 DEC ▪ 20 JAN ▪ 10 FEB ▪ 10 MAR**