Risk
Management
Framework
Today…

and Tomorrow

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

July, 2021 Volume 11, **Issue 3**

RMF Sentinel:

Army streamlines RMF… or weakens it?

By Lon J. Berman, CISSP, RDRP

Anyone who has endured the “adventure” of going through the full RMF life cycle can attest to the daunting amount of work and attention to detail required to be successful. Some even question whether or not all this effort is really making our IT systems more secure. It is therefore natural for departments and agencies to pursue some sort of “streamlining” of the process. The Army’s answer lies in something they are calling Project Sentinel (or sometimes “RMF 2.0”).

Project Sentinel aims to streamline the RMF process by identifying a subset of the baseline controls that are deemed “critical” and focusing on those rather than on compliance with the full set. Their choice of critical controls is intended to be “threat-focused” and “dynamic”, meaning that it can evolve over time in response to the changing threat landscape.

The Army’s Network Enterprise Technology Command (NETCOM) is managing the Sentinel program, and they are using the eMASS tool to implement it. Sentinel is set up as a Common Control Provider (CCP), from which systems can receive security control inheritance. System owners place a request for inheritance from Sentinel, just as they would for a hosting data center or cloud service provider. NETCOM then reviews the requesting system’s eMASS record to ensure the hardware/software inventory is complete and all applicable Security Technical Implementation Guides (STIGs) have been identified. They will then approve the inheritance request and the system owner will see literally *hundreds* of inheritable controls available to them.

The only caveat is that system owners are advised not to accept inheritance for any controls that are directly mapped to STIG items. All other inherited Sentinel controls will show up as *Not Applicable* (NA) in the receiving system’s eMASS record, which of course means they are not required to implement the control nor are they required to provide supporting documentation. Along with each such NA control comes a “justification” provided by NETCOM that states the control is subject to review and the inheritance may be withdrawn in response to a changing threat environment. Should that occur, the receiving system would immediately become responsible for implementing and documenting the control.

The net effect of receiving inheritance from Sentinel is that the receiving system will be responsible for implementing and documenting a considerably smaller number of controls. The independent assessment teams (*required* for all Army RMF efforts) will therefore have a smaller number of controls and documentation artifacts to review. It can be said that Sentinel inheritance de-emphasizes management and operational controls in favor of technical controls, thus making STIG compliance the focus of RMF.

See RMF Sentinel, Page 4 for more.

Risk Management Framework Today...

and Tomorrow

Cybersecurity Programs Need Teeth (Beyond RMF)!

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

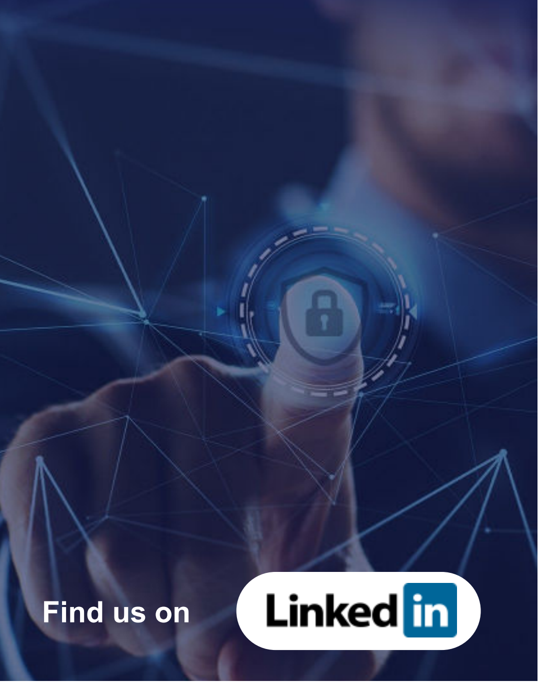
After the recent Colonial Pipeline and JBS Meat Processing ransomware attacks, I was approached multiple times by concerned friends asking if BAI could start offering cybersecurity training targeted towards private industry. My quick reply to these folks was that we have tried offering Cybersecurity Framework (CSF) training previously, and we received limited interest. CSF is essentially a cybersecurity framework that was created with a focus on critical infrastructure and then evolved to being applicable to all companies (private or public). CSF has a neat feature of providing its users the option to choose the control set they wish to use. The control reference options include COBIT 5, ISO/IEC 27001:2013, ISA 62443-2.1:2009, CIS CSC, and our favorite NIST 800 -53.

I am not a CSF expert, but after talking to BAI's CSF SME, Marilyn Fritz, I discovered that CSF is a very flexible and well created cybersecurity program that can be used by all lines of business, and it is very approachable. I have since reviewed the most recent version of CSF and found it to be very easy to understand with documentation that is not as robust RMF. CSF is by no means RMF light, but unlike RMF which people often complain is very heavy reading with hundreds of pages of guidance, the primary CSF document is only 55 pages. The bottom line is that NIST has created a cybersecurity framework that is very easy to use and implement into every business.

If NIST has created CSF and many other free compliance programs are available why are companies continually getting hacked every minute at an alarming rate? I recognize scenarios such as these have a variety of elements at play, but I continue to be a firm believer that executives who are focused on shareholder returns still do not see cybersecurity training and the implementation of cybersecurity compliance programs as a top priority, and since they do not "have teeth" such as legal requirements these programs are not implemented as thoroughly as they should be.

For the past few years, a trend has existed where companies have purchased cybersecurity insurance with the thought that they are mitigating risk. With the uptick in attacks, recent data is indicating that the major cyber insurance companies are no longer paying out on cyber insurance if sufficient controls are not in place. I hope this is the beginning of the required compliance we need to encourage private industry to take cybersecurity seriously, but I am still concerned that too many companies will wait until it is too late to implement a program such as CSF in their organization. This brings me back to the initial topic of this article. BAI would love to offer CSF training regularly, but history shows that organizations will not pay for cybersecurity compliance and training unless it is a mandated requirement such as RMF. Beyond the business case of being Director of Training for BAI, I hope that C suite executives start making cybersecurity program implementation a priority instead of waiting to clean up messes that end up having long lasting financial and reputational impacts.

> ***"CSF is by no means RMF light, but unlike RMF which people often complain is very heavy reading with hundreds of pages of guidance, the primary CSF document is only 55 pages. The bottom line is that NIST has created a cybersecurity framework that is very easy to use and implement into every business."***



Risk Management Framework Today...

and Tomorrow

Zero Trust Architecture in the DoD and Federal Civil Agencies

By Kathryn Daily, CISSP, CAP, RDRP

If you follow any cybersecurity news, I am sure you have heard about zero trust architecture (ZTA). Historically, the authorization process has existed primarily at the perimeter of the network. In zero trust architectures, authorization happens across the surface of the network. Essentially, zero trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

"...zero trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters..."

In February of 2021, DISA and NSA put out the Department of Defense (DoD) Zero Trust Reference Architecture. It was publicly released in May of 2020. Within this document, DISA/NSA identify 5 high-level goals for the ZTA implementation, to wit:

1. **Modernize Information Enterprise to Address Gaps and Seams.** It's no secret that DoD IT has been underfunded and over time has become completely decentralized as each service/agency fits their networks and IT assets to meet their specific mission needs and budgetary constraints. The ZT RA aims to resolve these gaps in command configuration and processes by establishing an inclusive, responsive, and near-real time common operating picture.
2. **Simplify Security Architecture.** Rather than trying to secure circuits with crypto devices, enclaves with firewalls, data centers with DMZ security stacks, and operating systems with HBSS, ZTA instead focuses on the interaction between the user (the point of entry/exit of most data) and the application software (the source/destination of most data).
3. **Produce Consistent Policy.** Historically DoD networks have been configured and managed inconsistently through waivers and exceptions that have left the security of DoD systems porous and ineffective. By pushing to the Zero Trust Reference Architecture DoD-wide, security should be improved through consistently applied polices across environments to maximize effectiveness.
4. **Optimize Data Management Operations.** Mission success and advanced analytics rely on consistently structured and tagged data. While standards and policies have always existed, they have been inconsistently implemented. By standardizing data management operations, organizations can better leverage the benefits of cloud computing, data analytics, machine learning and artificial intelligence. It will also enhance interoperability between applications, organizations and with external partners.
5. **Provide Dynamic Credentialing and Authorization.** DoD ICAM (Identity, Credential, and Access Management) Reference Design aims to rectify outdated authentication and authorization processes by focusing authorizing access to resources at the point in time the entity requests access to the resource based on the digital policy rule for the resource and authorization and environment attribute values.

Find us on LinkedIn

BAI Information Security Consulting & Training

See Zero Trust, Page 4 for more.

Risk Management Framework Today…

and Tomorrow

> ***"Recent highly-publicized security incidents such as ransomware attacks can best be prevented or managed through operational controls (e.g., end user training, incident response planning) rather than technical system configuration."***

Find us on Linked in

BAI Information Security Consulting & Training

RMF Sentinel, from Page 1

Critics see all of this as a weakening of RMF by the Army, and, more broadly, a weakening of the "Holistic Security" philosophy that has traditionally been the centerpiece of enterprise security management frameworks across government and industry. They fear this over-emphasis on technical compliance will result in system owners becoming less vigilant about things like policies, operational procedures (such as Incident Response and Disaster Recovery plans) and even training. Failures in these areas can have consequences that are just as devastating as those that come from technical vulnerabilities. Recent highly-publicized security incidents such as ransomware attacks can best be prevented or managed through operational controls (e.g., end user training, incident response planning) rather than technical system configuration. Some dyed-in-the-wool cynics even go so far as to suggest that the whole threat-focused "thing" is just a smokescreen and the reality is that Army has caved to the "this is too hard" whiners.

The bigger "RMF 2.0" picture in Army also includes plans to enhance continuous monitoring (of technical controls) and to move towards a "continuous authorization" model (vice periodic re-authorizations). Again, opinions vary on whether these are good things or just more cutting of corners.

Will Sentinel and "RMF 2.0" make Army systems more secure … or less secure? Will similar programs take hold in other DoD components? Time will tell. Stay tuned!

Zero Trust, from Page 3

Likewise, for Federal Civil Agencies, President Joe Biden issued an Executive Order that mandated civil agencies to create plans for the adoption of zero-trust architectures within 60 days of the issuance of the EO in an effort to push the modernization of federal cybersecurity following major software exploits, most notably by SolarWinds. Unlike the DoD, the federal Executive Order does not provide a consistent framework to implement ZTA within the Federal Civil Agencies. Many agencies are leveraging the NIS SP 800-207, while others are basing their approach on the Forrester Zero Trust Model, Garner's Continuous Adaptive Risk and Trust Assessment, Garter's Secure Access Service Edge, or have completely created their own implementation.

It is my hope that the Federal Civil Agencies will either create a standardized approach to the adoption of Zero Trust Architecture or at least adopt the DoD ZTA RA in order to ensure that policies are applied consistently throughout the fed.

To view the DoD Zero Trust Reference Architecture, visit the Library page at https://dodcio.defense.gov/.

Risk Management Framework Today…

and Tomorrow

"In this day and age, most systems are hosted by data centers or cloud service providers, thus all access is "network access" – that in itself is the "compelling operational need" for network access to privileged commands."

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/.

JZ writes:
I have a question regarding Control Enhancement AC-6(3). The control states that the organization authorizes network access to organization-defined privileged commands only for organization-defined compelling operational needs and documents the rationale for such access in the security plan for the information system. Does this mean that every privilege level command has to be listed? Can a general one liner be used that states that privileged functions are limited to those needed for their admin role or something like that? For example Exchange servers Admin are limited to exchange privilege level command? What is the best way to state the authorized privilege level commands in the SSP?

Dr. RMF responds:
JZ, You are correct in saying it would be utterly infeasible to list individual "privileged commands" in the security plan so a general statement will have to do. In this day and age, most systems are hosted by data centers or cloud service providers, thus all access is "network access" – that in itself is the "compelling operational need" for network access to privileged commands. Dr. RMF notes that Control Enhancement AC-6(3) applies only to systems categorized as High for Confidentiality or Integrity, so this situation will occur only in a small minority of information systems.

"Assessed" writes:
Please help me better understand RMF Assess Only. Some of my colleagues are saying we should consider pursuing an Assess Only ATO because it's so much easier than going through the full ATO process. Is that even for real?

Dr. RMF responds:
RMF Assess Only is absolutely a real process. The RMF Assess Only process is appropriate for a component or subsystem that is intended for use within multiple existing systems. The idea is to assess the new component or subsystem once, and then make that assessment available to the owners of receiving systems in order to expedite addition of the new component or system into their existing system boundary. In other words, RMF Assess Only expedites incorporation of a new component or subsystem into an existing system that already has an ATO. And by the way, there is no such thing as an Assess Only ATO. If you think about it, the term Assess Only ATO is self-contradictory. After all, if you're only doing the "assess" part of RMF, then there is no "authorize" and therefore no ATO.

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

Risk Management Framework Today...

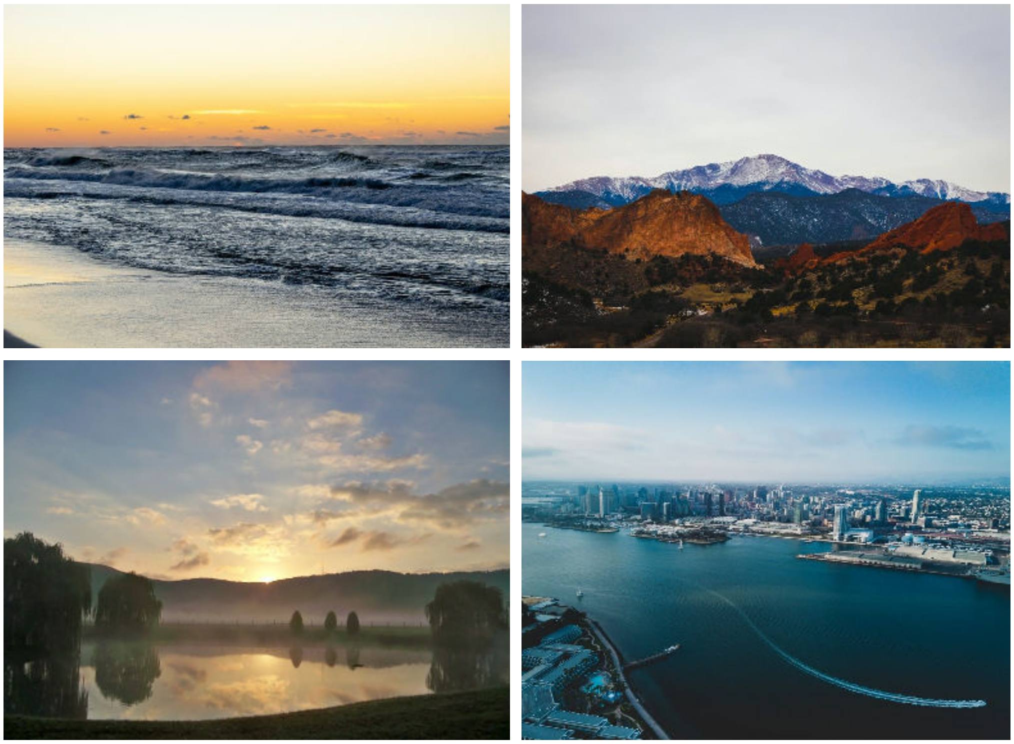
and Tomorrow

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 a new location in Alexandria South adjacent to Fort Belvoir!

RMF for DoD IT and Federal Agencies & eMASS eSSENTIALS ™

Pensacola — August 2nd – 6th & November 1st – 5th
Colorado Springs — September 13th – 17th
Huntsville — September 20th – 24th
San Diego — October 18th – 22nd



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

Security Controls Implementation and Assessment Workshop & STIG 101™

Alexandria (Fort Belvoir) — September 27th – October 1st

Alexandria boasts historic views and plenty of attractions for our students to enjoy outside of class hours.

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

Find us on LinkedIn

BAI Information Security Consulting & Training

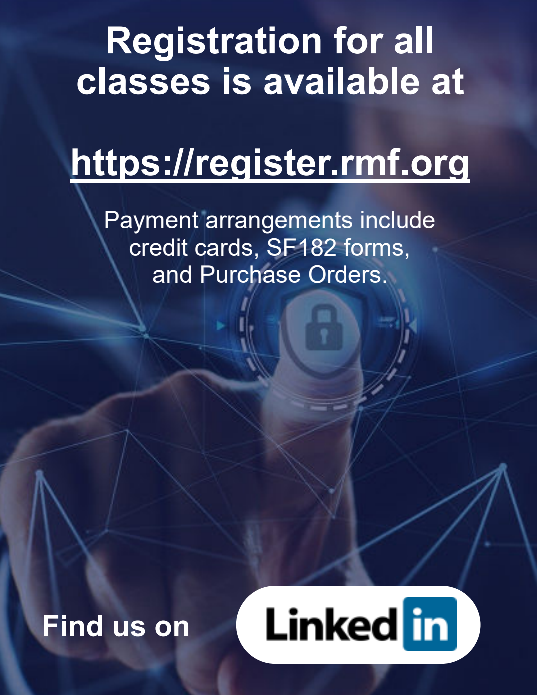
Risk Management Framework Today…

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 September, 2021:

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

- ♦ Online Personal Classroom™ ▪ 12 - 15 JUL ▪ 19 - 22 JUL ▪ 26 - 29 JUL ▪ 9 - 12 AUG ▪ 16 - 19 AUG ▪ 30 AUG - 2 SEP ▪ 13 - 16 SEP ▪ 27 - 30 SEP ▪ 18 - 21 OCT ▪ 25 - 28 OCT ▪ 1 - 4 NOV ▪ 15 - 18 NOV ▪ 13 - 16 DEC
- ♦ Pensacola ▪ 2 - 5 AUG ▪ 1 - 4 NOV
- ♦ Colorado Springs ▪ 20 - 23 SEP
- ♦ Huntsville ▪ 20 - 23 SEP
- ♦ San Diego ▪ 18 - 21 OCT

RMF Supplement for DCSA Cleared Contractors—1 day program

- ♦ Online Personal Classroom™ ▪ 8 JUL ▪ 5 AUG ▪ 9 SEP ▪ 10 NOV

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

- ♦ Online Personal Classroom™ ▪ 6 - 8 JUL ▪ 7 - 9 SEP ▪ 4 - 6 OCT ▪ 8 - 10 NOV ▪ 6 - 8 DEC

eMASS eSSENTIALS—1 day program

- ♦ Online Personal Classroom™ ▪ 16 JUL ▪ 23 JUL ▪ 30 JUL ▪ 6 AUG ▪ 13 AUG ▪ 20 AUG ▪ 3 SEP ▪ 17 SEP ▪ 1 OCT ▪ 6 OCT ▪ 22 OCT ▪ 29 OCT ▪ 19 NOV ▪ 17 DEC
- ♦ Pensacola ▪ 6 AUG ▪ 5 NOV
- ♦ Colorado Springs ▪ 24 SEP
- ♦ Huntsville ▪ 24 SEP
- ♦ San Diego ▪ 22 OCT

STIG 101—1 day program

- ♦ Online Personal Classroom™ ▪ 30 JUL ▪ 27 AUG ▪ 24 SEP ▪ 29 OCT ▪ 3 DEC ▪ 9 DEC ▪ 17 DEC
- ♦ Fort Belvoir ▪ 1 OCT

Information Security Continuous Monitoring—1 day program

- ♦ Online Personal Classroom™ ▪ 9 JUL ▪ 30 JUL ▪ 10 SEP ▪ 7 OCT ▪ 9 NOV ▪ 10 DEC

RMF in the Cloud—1 day program

- ♦ Online Personal Classroom™ ▪ 8 JUL ▪ 4 AUG ▪ 8 SEP ▪ 8 OCT ▪ 12 NOV ▪ 8 DEC

Security Controls Implementation & Assessment Workshop—4 day program

- ♦ Online Personal Classroom™ ▪ 26 - 29 JUL ▪ 23 - 26 AUG ▪ 20 - 23 SEP ▪ 25 - 28 OCT ▪ 29 NOV - 2 DEC ▪ 13 - 16 DEC
- ♦ Fort Belvoir ▪ 27 SEP - 30 SEP

CAP Exam Preparation—1 day program

- ♦ Online Personal Classroom™ ▪ 23 JUL ▪ 5 NOV