Risk Management Framework Today…

and Tomorrow

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

*January, 2020 Volume 10, **Issue 1***

CMMC—What We Know and What We Don't

By Kathryn Daily, CISSP, CAP, RDRP

So by now, I'm sure you've seen a ton of articles on the Cybersecurity Maturity Model Certification (CMMC) initiative. A lot of information has been released but there are still a lot of unknowns.

What We Know

We know that it's mandatory for all contractors who wish to do business with the Department of Defense. We know that there are 5 levels of compliance ranging from level 1 (basic cyber hygiene) to level 5 (state of the art cyber program). We also know the full control set now with the release of CMMC Version 0.7 that came out last month.

What We Don't Know

We don't know who will make up the accreditation body and how assessors will be validated. It's great that we have the control set, so that we as contractors can begin working on our compliance, but until we know the entire process, it's hard to map out a project plan. Will there be a limited number of assessors that will cause a backlog of contractors waiting to get certified? Currently there are marketplaces popping up that purports to have a repository of auditors for the CMMC validation. One such marketplace has 120 (as of last week) auditors listed in their directory. At some point this makes no sense, we don't even have an accreditation process or body to oversee said process. At a minimum, it appears folks are seriously jumping the gun.

Which contracts will be coming out in the fall of this year with CMMC requirements? It's unfathomable that all contracts will include CMMC requirements out of the gate. Will it be specific DoD agencies that begin rolling out the CMMC requirements? Specific industries? Completely random? Who knows. We may not get an answer to this until fall.

Another unknown is which contracts will require which level of certification. Will a contract currently held by a small business eventually require a level 5 certification, thus requiring a state of the art cyber program that only a top defense contractor can comply with? DoD spokesperson Katie Arrington has stated several times that it won't be cost prohibitive for small business, and level 1 and 2 might be tolerable… and maybe level 3 but a small business with 5 employees will never have the resources to comply with a level 5 CMMC certification.

What will this all cost? Ms. Arrington has stated that CMMC compliance is an allowable cost. That means to me that subs will pass that cost onto primes and primes will pass it on to the government. This is going to result in contracts that are much more costly to the government. It will be interesting to see just how much overall this initiative ends up costing in the long run. Now I'm not saying security isn't worth an additional cost, because it is, but the end number should be interesting.

Conclusion

While we know enough to get us started, there are still a lot of unknowns that make planning for certification difficult. That being said, OUSD has stayed true to their word with respect to the schedule thus far, which is promising and helps us to prepare for milestones to come. Hopefully some of our unknowns will be answered with the release of V 1.0 that is scheduled to be published this month.

Risk Management Framework Today…

and Tomorrow

*"…*Project Sentinel is described as an adaption of the traditional RMF process with goals of streamlining RMF into a threat informed risk decision process. *…"*

Find us on LinkedIn

BAI Information Security Consulting & Training

U.S. Army Moves Towards Threat-Based RMF Approach (Project Sentinel)

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

What is Project Sentinel?

The United States Army recently announced that it is launching a new initiative called Project Sentinel. Project Sentinel is described as an adaption of the traditional RMF process with goals of streamlining RMF into a threat informed risk decision process. Due to criticisms of RMF as a check-the-box compliance process that is laborious and lacking agility, the Army feels a threat-informed risk management decision process would be effective.

Project Sentinel will utilize authoritative threat sources such as Critical Security Controls for the Effective Cyber Defense published by the Center of Internet Security (formerly SANs top 20) to establish a threat hierarchy containing the most common attacks and controls relating to them. Additionally, the project will review Army Cyber Command (ARCYBER) threat trends from the Intelligence Community and its partners. By focusing on these high priority threats, it will be possible to tailor the RMF control set to save time in navigating all the RMF controls vs. controls related to high priority threats. Additionally, the Army will create a risk threshold which will prioritize controls changing based on continuously monitored emerging threats.

Initial steps of Project Sentinel will be to review threat sources and map threats to RMF controls in Phase 1, and then after pilots in the next few months, the level of assurance in relation to control identification will be assessed. After the entire process is reviewed, a phase 1 capability statement will be available in the April-May 2020 timeframe.

My Thoughts

You may recall an article I published in October 2018 titled "RMF 30-Day Sprint". For those of you not religiously tracking BAI's RMF article publication cycle, I'd be happy to elaborate. During the summer of 2018, I attended the Air Force Information Technology & Cyberpower Conference (AFITC). During this conference, I caught wind of an Air Force initiative (a version now exists for Navy as well) called The RMF 30-Day Sprint. Goals of the sprint were quicker ATO's and maximized RMF efficiency.

Since the article's publication, the Air Force has moved away from the RMF 30-Day Sprint. These example elaborate that abridged controls sets with goals of maximizing RMF efficiency are not new to the services.

Overall, I recognize that RMF is often viewed as a burdensome overly robust process that does not have the agility required to keep up with the evolving threat landscape, but due to the holistic nature of RMF, I am not entirely convinced taking a subsection of RMF controls is the solution to these pain points. Although some RMF controls are more aligned with the evolving threat landscape than others, all RMF controls attached to a system are important due to their interconnectedness. Taking RMF's holistic nature into consideration, I worry that Project Sentinel will place focus on a specific section of controls and neglect others.

I applaud the Army for taking the perceived RMF crisis seriously and looking for solutions to increase efficiency, but if Project Sentinel moves forward, it must be stressed that the controls at the bottom of the "risk threshold" are given appropriate attention and not just pushed to the side in efforts to implement high priority controls and achieve quick conditional ATO's. After all, if higher priority controls become the primary focus of RMF the lack of attention to other controls perceived as lower priority will create new risk conditions. Additionally, a focus on continuous monitoring and DoD publishing clear continuous monitoring guidance would potentially strengthen DoD's risk posture more than an abridged RMF control set project, but that is a topic for another article. I truly hope Project Sentinel is success in strengthening Army cyber defenses and reducing risk and it helps mitigate the perceived "RMF crisis".

Risk Management Framework Today…

and Tomorrow

"...It is not considered acceptable by most independent validators for the system owner to tailor out the "NSS-only" controls. Sorry for the bad news!..."

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 is a Ph.D. researcher with a primary research focus of RMF.

Dr. RMF submissions can be made at https://rmf.org/dr-rmf/.

Dear Dr. RMF,

We are having a dispute in our office about how to handle security control selection for a "non-National Security System" (non-NSS). We know DoD has mandated that System Categorization and Security Control Selection shall be done "in accordance with CNSSI 1253". However, the CNSSI 1253 security control baselines include numerous controls that are intended for use in NSS only; these are the ones marked with a plus sign ("+") in CNSSI 1253 Appendix D.

The two schools of thought are:

- Since the controls marked with a plus sign are intended for use in NSS only, we are justified in tailoring them out of the baseline (or making them NA) for a non-NSS
- The DoD mandate to use CNSSI 1253 for security control selection implies that all controls in the baseline (including those marked with a plus sign) are in scope.

It's quite a few additional controls, so we want to be sure we're going about this correctly. Please Dr. RMF, can you point us in the right direction here?

Non-plussed

Dear Non-plussed,

It does seem logical that controls marked as being applicable to NSS only should not be included in the baseline for non-NSS. However, this question has been hotly debated within DoD and it has been determined that the DoD mandate to "use CNSSI 1253" requires that *all* controls should be included in the baseline, even those marked with the plus sign. If you're using eMASS to manage your RMF package, you'll see that all controls are included in the baseline by default. It is not considered acceptable by most independent validators for the system owner to tailor out the "NSS-only" controls. Sorry for the bad news!

Risk Management Framework Today…

and Tomorrow

"...Cleared contractors who operate classified information systems on their own premises are subject to Assessment and Authorization and therefore must comply with RMF requirements..."

Find us on LinkedIn

BAI Information Security Consulting & Training

RMF and eMASS in the National Industrial Security Program (NISP)

By Lon J. Berman CISSP, RDRP

Organizations performing classified work for DoD (aka. Cleared Contractor Facilities) are governed by the National Industrial Security Program (NISP). NISP is administered by the Defense Counterintelligence and Security Agency (DCSA), formerly known as the Defense Security Service (DSS). In general, companies covered by NISP engage in one or more of the following activities:

- Maintaining cleared personnel
- "Safeguarding" printed classified material on their premises
- Operating classified information systems on their premises

All classified contractors maintain personnel clearances, and for many companies, that is as far as it goes – all cleared personnel are working "on site" at DoD or prime contractor facilities and no classified information is present at the company's own location(s). The subset of classified contractors who actually operate classified information systems *on their own premises* are subject to Assessment and Authorization (A&A) and therefore must comply with RMF requirements.

The DCSA Assessment and Authorization Program Manual (DAAPM) is the governing document for RMF that applies to the classified contractor community. While closely resembling the "generic" RMF process as described in DoD and NIST publications (e.g., DoDI 8510.01, NIST SP 800-37), DCSA has "tailored" the process to best fit the needs of the community. Here are some examples:

- The Security Control Assessor (SCA) role is assigned to DCSA Information System Security Professionals (ISSPs).
- The role of Data Transfer Agent (DTA) has been added.
- Information System Security Managers (ISSMs) are subject to specific training requirements selected from the DCSA Center for the Development of Security Excellence (CDSE).
- System categorization levels for Confidentiality are limited to High and Moderate categorization of Low is not permitted due to the presence of classified material. Categorization levels for Integrity and Availability can still be High, Moderate or Low.
- DCSA has developed Overlays to address three types of systems in common use at cleared contractor facilities: Single User Standalone (SUSA), Multi User Standalone (MUSA) and Isolated LAN. Because of their limited connectivity many controls have been removed from the customary RMF baselines with these overlays.

As is the case for most DoD organizations, cleared contractors are now using the Enterprise Mission Assurance Security Service (eMASS) tool to build their RMF documentation package. A specific "version" of eMASS called "NISP eMASS" has been developed for classified contractors and is accessible at https://nisp.emass.apps.mil. NISP eMASS is configured with the roles, categorization limitation and overlays as described above. Other "unique features" of NISP eMASS include:

- NISP eMASS is *Unclassified*. eMASS Asset Manager module is not used in NISP eMASS, since scans, checklists and other technical artifacts will contain classified information. Additionally, users are cautioned not to upload any other system artifacts that are Classified.
- The Approval Chains have been customized to reflect the DCSA roles and responsibilities. For example, step 2 in the Control Approval Chain is assigned to the DCSA ISSP.
- NISP eMASS is accessible with an External Certificate Authority (ECA) certificate – other eMASS versions require a DoD Common Access Card (CAC).

Risk Management Framework Today…

and Tomorrow

"...BAI RMF Resource Center is proud to announce that we are continuing to broaden our RMF training footprint to provide the most robust RMF educational offerings in the United States by adding Charleston, South Carolina, Seattle, Washington, and Honolulu, Hawaii in 2020..."

Find us on LinkedIn

BAI Information Security Consulting & Training

New Locations for 2020!

Location! Location! Location!

(Charleston, Seattle and Honolulu)

BAI RMF Resource Center is proud to announce that we are continuing to broaden our RMF training footprint to provide the most robust RMF educational offerings in the United States by adding Charleston, South Carolina, Seattle, Washington, and Honolulu, Hawaii in 2020. Seattle and Charleston will be offered in the 2nd quarter of 2020 to start with Honolulu rolling out in the 3rdquarter.

At BAI, we recognize the need for comprehensive and practical U.S. government cybersecurity training, and we feel by broadening our physical location offering, we enable our customers to maximize their access in attaining the training they need.

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.
- **CMMC Readiness Workshop**—prepares DoD contractors for the impending mandatory Cybersecurity Maturity Model Certification.
- **eMASS eSSENTIALS** – provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is utilized.
- **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 Assessment (SCA) Workshop** – provides a current approach to evaluation and testing of security controls to prove they are functioning correctly in today's IT systems.
- **Continuous Monitoring Overview** – 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.
- **Certified Authorization Professional (CAP) Preparation** – this course provides preparation for the Certified Authorization Professional (CAP) certification administered through (ISC)2.

Our training delivery methods:

- **Traditional classroom**
- **Online Personal Classroom™ (live instructor-led)**
- **Private group classes for your organization (on-site or online instructor-led)**

Regularly-scheduled classes through June, 2020:

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

- **Dayton ▪ 27-30 APR**
- **Herndon, VA (Washington DC area) ▪ 27 JAN -30 JAN ▪ 6 –9 APR**
- **Huntsville ▪ 30 MAR – 2 APR**
- **Pensacola ▪ 24-27 FEB ▪ 4-7 MAY**
- **Colorado Springs ▪ 16-19 MAR ▪ 22-25 JUN**
- **San Diego ▪ 3-6 FEB ▪ 13-17 APR**
- **San Antonio ▪ 2-5 MAR ▪ 18-21 MAY**
- **Virginia Beach ▪ 23-26 MAR ▪ 29 JUN-2 JUL**
- **Charleston ▪ 8-11 JUN**
- **Seattle ▪ 15-18 JUN**
- **Online Personal Classroom™ ▪ 13-16 JAN▪ 10-13 FEB ▪ 9-12 MAR ▪ 13-16 APR ▪ 11-14 APR ▪ 15-18 JUN**

CMMC Readiness Workshop—2 day program

- **Online Personal Classroom™ ▪ 22-23 JAN ▪ 24-25 MAR ▪ 5-6 MAY ▪ 23-25 JUN**

eMASS eSSENTIALS—1 day program

- **Dayton ▪ 1 MAY**
- **Herndon, VA (Washington DC area) ▪ 31 JAN ▪ 10 APR**
- **Huntsville ▪ 13 DEC ▪ 3 APR**
- **Pensacola ▪ 28 FEB ▪ 8 MAY**
- **Colorado Springs ▪ 20 MAR ▪ 26 JUN**
- **San Diego ▪ 7 FEB ▪ 1 MAY**
- **San Antonio ▪ 6 MAR ▪ 22 MAY ▪ 26 MAY ▪ 4 JUN**
- **Virginia Beach ▪ 27 MAR ▪ 3 JUL**
- **Charleston ▪ 23 JUN**
- **Seattle ▪ 19 JUN**
- **Online Personal Classroom™ ▪ 23 JAN ▪ 20 FEB ▪ 22 APR**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 17 JAN ▪ 14 FEB ▪ 19 FEB ▪ 13 MAR ▪ 17 APR ▪ 21 APR ▪ 15 MAY ▪ 27 MAY ▪ 2 JUN ▪ 19 JUN**

Continuous Monitoring Overview—1 day program

- **Online Personal Classroom™ ▪ 18 FEB ▪ 3 JUN**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 22 JAN ▪ 1 JUN**

CAP Prep—1 day program

- **Online Personal Classroom™ ▪ 21 FEB**

SCA Workshop—2 day program

- **Online Personal Classroom™ ▪ 26-27 FEB ▪ 26-27 MAY**