Risk Management Framework Today…

and Tomorrow

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

Welcome, Step 0

*January, 2021 Volume 11, **Issue 1***

By Lon J. Berman, CISSP, RDRP

Q. The Risk Management Framework (RMF) life cycle is comprised of how many steps?

A. Oh, that's easy, it's six.

Well … not so fast.

As you probably know, the Risk Management Framework (RMF) has always been described as a six step process, to wit: 1-Categorize, 2-Select, 3-Implement, 4-Assess, 5-Authorize, 6-Monitor. The "traditional" pictorial view of the RMF life cycle (from NIST Special Publication 800-37 Rev 1) is shown in Figure 1 below.

This six step process was also adopted in DoD Instruction 8510.01, "Risk Management Framework for DoD IT".

In NIST Special Publication 800-37 Rev 2, a significant revision was made to the RMF life cycle. A new "Prepare" step has been added. The activities in the Prepare step provide information that feeds into the traditional six steps, as shown in Figure 2 on the next page.

NIST further divides the activities in the Prepare step into "Organization level activities" and "System level activities". Organization level tasks include assignment of RMF roles, initial risk assessment, common control identification, continuous monitoring strategy, and more. System level tasks include asset identification, system boundary determination, identification of information types, system registration, and more. RMF has thus morphed into a seven step process, but to preserve the numbering of the traditional six steps, the Prepare step is sometimes referred to as "Step 0".

DoD has yet to update DoDI 8510.01 to reflect the seven step RMF process.

See Step 0, Page 5 for more.

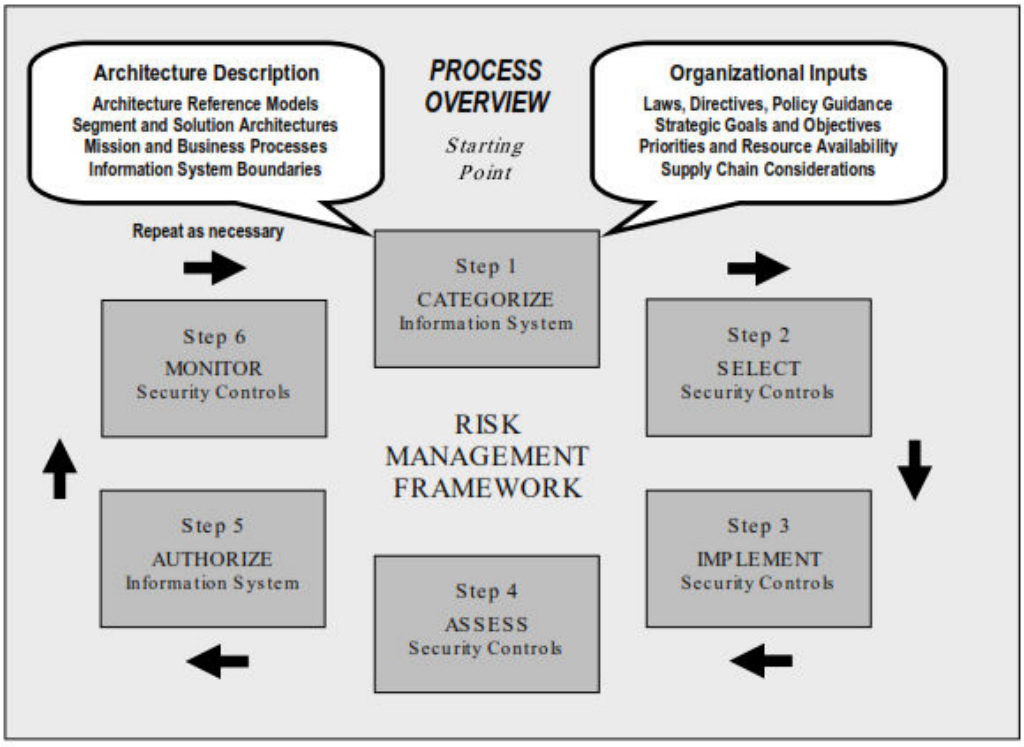

Figure 1: A traditional pictorial view of the RMF life cycle (from NIST Special Publication 800-37)

Risk Management Framework Today…

and Tomorrow

"If you are hesitant, it may not be as challenging as you might believe! The DoD needs good contractors, and want a successful outcome for everyone."

Find us on LinkedIn

BAI Information Security Consulting & Training

DFARS Compliance with CMMC/NIST SP 800-171

By Marilyn Fritz, CISSP, CISA, ITIL, PMP

The new DFARS Interim Rule that went into effect November 30, 2020 is a game changer for any entities that have or are pursuing Defense Industrial Base (DIB) contracts or subcontracts. Prior to the new Interim Rule, contractors and sub-contractors could self-attest that they met DoD cybersecurity requirements specified in NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". A key component of the new regulation is that contractors must demonstrate that they understand the requirements, are working towards compliance, and can provide a timeline when compliance will be complete. For DIB contractors relatively new to these cybersecurity requirements, the most important set of actions would be to understand what this will take - and to make a plan to get there.

The need for this newest set of regulations has been underscored by relentless and ever-increasing numbers of cyber breaches. Intellectual property theft from DoD defense contractors alone has resulted in dollar losses valued in the billions. Just in December, news reports revealed hacks that reach deep into US nuclear laboratories, the Pentagon, Treasury, Commerce departments, and beyond. These news reports continue to bear witness that immediate, effective action is urgently required.

Clearly, the DoD must get even more serious about cybersecurity. But how does that translate into the new DFARS Interim Rule requirements, and what does that now means for your ability to maintain or gain a DoD contract?

If you are hesitant, it may not be as challenging as you might believe! The DoD needs good contractors, and want a successful outcome for everyone. The rollout has been designed therefore to improve the cybersecurity posture across the supply chain, while causing the least amount of disruption to those serving as contractors and subcontractors in the DIB. This article covers the essentials of the new DFARS Interim Rule as it affects your journey towards compliance.

First, determine whether DFARS applies to your organization. DFARS is a requirement for entities that process, transmit or store Controlled Unclassified Information (CUI.) The DoD has stated that the contract will state whether it falls under DFARS. CUI is a designation for information that is not publicly available and meets certain criteria. The DoD provides 19 categories of CUI such as nuclear, privacy, international agreements and critical infrastructure. Typical examples include intellectual property, design specifications, contracts, legal, and project related documents, such as timelines and time cards. Although there is the potential for varying sources of information to be aggregated to create CUI (which is the contractor's responsibility to identify), the DoD will be the primary source for determining whether CUI protection levels are needed.

Next, the new DFARS Interim Rule implements the "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology". Although the methodology is new for most contractors, it can be viewed as a helpful stepping-stone to learning the requirements for compliance. Part of the mandate is that contractors must self-assess against NIST SP 800-171 requirements and enter results in the Supplier Performance Risk System "SPRS"[1]. Most

See DFARS, Page 3 for more.

[1]Supplier Performance Risk System "SPRS" https://www.sprs.csd.disa.mil/

Risk Management Framework Today…

and Tomorrow

"True to our motto of "We ARE RMF!", the "DFARS Compliance with CMMC/NIST SP 800-171" curriculum has been designed by RMF practitioners who can offer you the industry standard for getting through the process of control implementation and assessment."

Find us on LinkedIn

BAI Information Security Consulting & Training

contractors will self-assess and enter results from this "Basic" assessment SPRS. The DoD will conduct a small percentage of annual contract awards depending on the level of confidence required by the DoD for the particular contract. In which case, the DoD will assign personnel to conduct Medium or High reviews and to enter the results in SPRS.

The DFARS Interim Rule requires that going forward, contracting officers must confirm that an entity has entered an active SPRS Assessment prior to awarding a new or renewed contract.

The good news for getting started is that the Methodology currently does not stipulate a "passing" score. That is, entering a score in SPRS is sufficient to get started. The process will require a submitted "Plans of Action" (POA) that identifies compliance gaps, and commits to timelines for when these will be addressed. The submission of the POA provides a strong incentive for contractors to implement security controls – rather than leave them undone indefinitely.

The Interim Rule also strengthens the rollout of the Cybersecurity Maturity Model Certification (CMMC) program. The CMMC is a DoD certification process that measures an entity's implementation of cybersecurity processes and practices. There are five protection levels in CMMC, and a separate assessment process managed by the CMMC Accreditation Body. These results are also entered in SPRS. For DFARS purposes, CMMC Level 3 is designed to protect CUI. CMMC Level 3 contains 130 practices ("controls"). Of these, 110 are from NIST SP 800-171. As such, any contractor that works towards NIST SP 800-171 compliance is well on their way towards CMMC Level 3.

The 20 controls CMMC Level 3 adds to NIST SP 800-171 are primarily process based. For example, CMMC measures the extent to which policies are communicated, understood, and followed within the organization. The CMMC also provides a maturity model which defines common sense indicators for the level to which cybersecurity practices are conducted, and to which these are embedded within the culture of an organization. This is a commendable goal, as embedding cybersecurity within an organization has proven to be one of the most reliable ways to develop a strong defense against attacks.

Finally, you should know that NIST SP 800-171 controls are excerpted from the NIST SP 800-53 control catalog – the gold standard for DoD and Federal internal systems protection. BAI's training has long been recognized as the standard bearer for the Risk Management Framework, which implements these NIST SP 800-53 controls. Given the reliance on the same controls, and with BAI's established leadership as the "go to" training and consulting experts on the NIST SP 800-53 control set (and assessment!), you can be confident that BAI's training will provide you with the knowledge and skills you need to set you on the path towards DFARS compliance.

True to our motto of "We ARE RMF!", the "DFARS Compliance with CMMC/NIST SP 800-171" curriculum has been designed by RMF practitioners who can offer you the industry standard for getting through the process of control implementation and assessment. BAI is uniquely positioned to help DoD contractors and subcontractors navigate the complexities of DFARS, whether with CMMC or NIST 800-171, so that you can be confident of success on your journey towards compliance.

[2]Cybersecurity Maturity Model Certificate (CMMC) Framework https://www.acq.osd.mil/cmmc/draft.html

NIST Rev. 5 Supplemental Materials

By Kathryn Daily, CISSP, CAP, RDRP

Back in September of last year (2020), NIST finally published the final version of Special Publication 800-53 Revision 5. Most notably, this revision incorporated privacy considerations in the security controls themselves rather than having separate control families for the privacy controls (e.g., AR, AP, IP, etc.). This is a considerable change from Rev. 4 that completely reorganizes the control catalog. To help with the transition, NIST has provided some supplemental materials to make the transition easier to manage.

"[Revision 5] incorporated privacy considerations in the security controls themselves rather than having separate control families for the privacy controls..."

The first supplemental item is the analysis of updates between the 800-53 Rev. 5 and Rev. 4. This Excel spreadsheet describes the changes to each control and control enhancement, provides a brief summary of the changes, and includes an assessment of the significant changes. The change notations are as follows:

- New base control indicates that the control did not exist in Rev. 4.
- New control enhancement indicates that it is a new enhancement either of a Rev. 4 base control or a new base control.
- Withdrawn indicates that the Rev. 4 control or control enhancement is no longer present in Rev. 5.
- Changes title indicates that a control title has been changed.
- Adds control text indicates that additional text has been added to the definition of the control, whether base control or enhancement.
- Adds parameter indicates that a new parameter has been added. Typically, the new parameter is quoted or characterized in the detail column.
- Changes control text refers to the definition of the control whether base control or enhancement.
- Change Parameter demonstrates that the text of an existing parameter has been modified.
- Removes parameter indicates a parameter that no loner exists in Rev. 5. Typically, the removed parameter is given in the detail column.
- Add discussion adds discussion text that previously did not exist in Rev. 4. This might be the benefit or advantage provided by the control, further definition, etc.
- Changes discussion indicates that the discussion text has been modified from what existed in Rev. 4. (e.g., "adds privacy references," provides examples or advantages)
- Adds to Privacy Control Baseline (SP 800-53B) indicates that the control or control enhancement has been added to the NIST SP 800-53B Privacy Control Baseline

As you can see from these change notations, Rev. 5 is a complete overhaul from the previous Rev. 4.

See NIST Rev. 5 Supplemental Materials, Page 5 for more.

Risk Management Framework Today…

and Tomorrow

"... Rev. 5 is a complete overhaul from the previous Rev. 4. Analyzing these changes sooner, rather than later, will position you to quick(ish)ly transition from Rev. 4 to Rev. 5."

Find us on LinkedIn

BAI Information Security Consulting & Training

Step 0, Page 1

That said, however, you should note the References section of DoDI 8510.01 cites the NIST publication as follows: "NIST Special Publication 800-37 … *as amended*". It is therefore safe to assume DoD has fully embraced the revised RMF life cycle, and we can expect this to be reflected in the next publication of DoDI 8510.01.

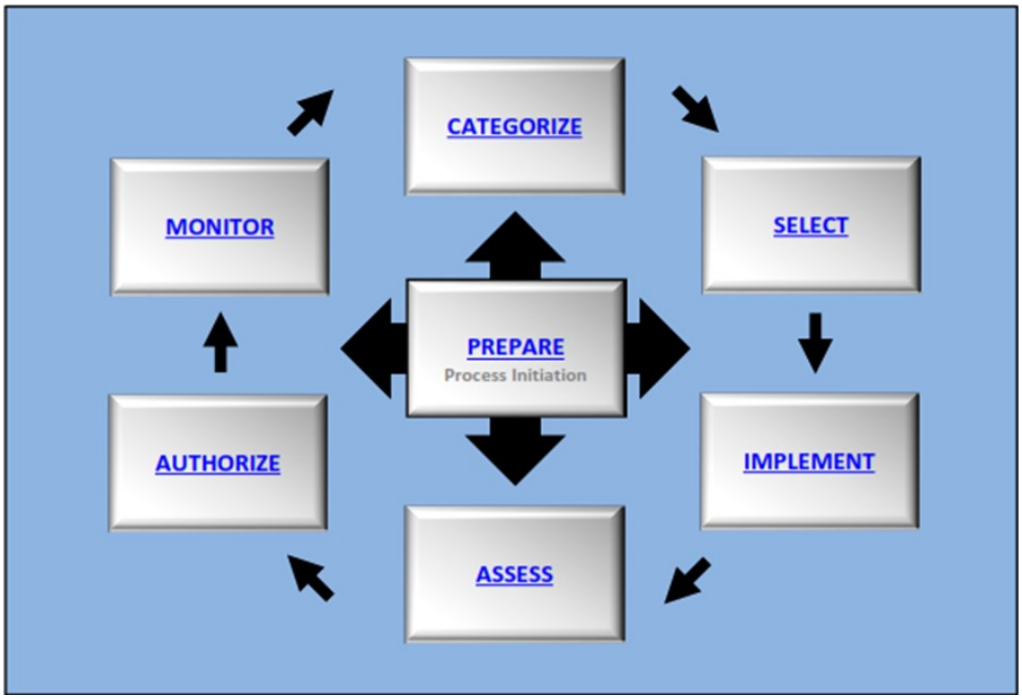

Figure 2: A pictorial view of the RMF life cycle with the "Prepare" step included.

NIST Rev. 5 Supplemental Materials, Page 4

Analyzing these changes sooner, rather than later, will position you to quick(ish)ly transition from Rev. 4 to Rev. 5

In addition to the analysis of updates, NIST has provided a mapping of Appendix J Privacy controls. As noted earlier, the privacy controls are no longer separate families but are organized into an integrated control catalog for a more holistic approach from a privacy and security standpoint. The mapping provides a listing of all privacy controls in Rev. 4 alongside their new Rev. 5 control. For example, AP-1: Authority to collect has been moved into the new PT family (Personally Identifiable Information Processing and Transparency) as PT-2 (Authority to Process Personally Identifiable Information). Some privacy controls have been cut up and placed into several new and existing controls. For example, AR-5 (Privacy Awareness and Training) has been incorporated into existing controls AT-1, AT-2, AT-3 and PL-4.

It is imperative that we get out in front of this major change and these supplemental materials will make that transition much easier. DoD likely will not adopt this new revision absent the implementation guidance (and your guess is as good as mine as to when that will come out) but the transition is coming. The old boy scout motto of "be prepared" is good advice here. Get prepared. It's coming.

Risk Management Framework Today…

and Tomorrow

"It is important to realize that not all online classes are built the same, and research has shown the most effective online instruction is delivered through interactive, live, instructor-led training."

Find us on LinkedIn

BAI Information Security Consulting & Training

Ready for In-Person Classroom RMF Training?

By P. Devon Schall, Ph.D., CISSP

Tired of Microsoft Teams and Zoom meetings yet? As a trained instructional designer, online college professor, residential (in-person) college professor, and Director of Training at BAI RMF Resource Center, I am opinionated and passionate about pedagogy and training delivery methods. 2020 has been full of unexpected challenges in all aspects of life, including education. We have seen DoD and most of industry embrace remote working and training organizations, including BAI, have been forced to pivot to primarily offering online training. We provide this in a live, instructor-led setting via our Online Personal Classroom. With all of this said, the title of this article says it all.

Having experienced both in-person and live instructor-led training from a student and instructional perspective, I have an appreciation for both delivery methods, and I think both can be done well. As an instructor, I personally enjoy the connection I make with students when I teach in-person classes. This may be selfish of me, but I feel like I can build a stronger rapport with my students when I meet with them face to face. Regarding quality of training, in my experience live instructor-led training is equally as effective as in-person training, as long as the student is comfortable with training in a remote virtual environment and the training provider understands the nuances of remote training.

It is important to realize that not all online classes are built the same, and research has shown the most effective online instruction is delivered through interactive, live, instructor-led training. I cannot fully stress the importance of interactive participation when students are trying to absorb a complicated cybersecurity process such as RMF.

As we begin to resume in-person classroom training, I suggest you ask yourself the questions below when making the decision between live instructor-led training in the Online Personal Classroom and In-Person Classroom training.

1. Am I prepared to fully participate in a live instructor-led online class (this includes group work and turning your microphone on to participate in discussions)?
2. Can I be free from distraction during the class if I choose to take it in The Online Personal Classroom™?
3. Am I confident that I can access a laptop that can connect to the class free from firewall or other technology issues?

If any of the three questions above present challenges to you, I suggest you keep an eye on our training calendar for upcoming in-person RMF classes as we plan to resume in-person RMF instruction with the goals of continuing to provide you with the highest quality RMF and RMF Ancillary training available! Additionally, BAI can arrange a "private in-person class" for your organization. You will have a dedicated instructor who will travel to your location and meet your RMF training needs.

Risk Management Framework Today…

and Tomorrow

"When we introduced our first DIACAP class, we wanted to do something a little different."

Find us on LinkedIn

BAI Information Security Consulting & Training

The RMF Hot Sauce Story

By Lon J. Berman, CISSP, RDRP

If you have attended a BAI training class you should have received a "special gift" from BAI – a bottle of "RMF Hot Sauce". Naturally we hope you and your family or friends enjoyed our little spicy treat. Over the years, lots of people have asked about it. Perhaps you were wondering "Do they always do that?" or even "Why hot sauce?" We thought this would be a good time to finally tell the BAI "hot sauce story". And, in the spirit of so many technology products, we thought it appropriate to tell the story in a Frequently Asked Questions (FAQ) format. So, here goes…

RMF Hot Sauce FAQ

How long have you been giving hot sauce to your students?

The BAI Hot Sauce tradition began in 2006. It was DIACAP Hot Sauce back then and now it's RMF Hot Sauce. So this year (2021) will be the 15th anniversary of BAI Hot Sauce!

Why hot sauce?

Training providers have routinely given out pads and pens, coffee mugs or T-shirts to students. When we introduced our first DIACAP class, we wanted to do something a little different. BAI founder Lon Berman is an aficionado of all things hot and spicy, so hot sauce was a natural, and it turned out to be a big hit with our students.

What if I attend one of your online classes? Is downloadable hot sauce even a "thing"?

Unfortunately, we haven't figured out how to download hot sauce, or even how to send it by FAX! But don't worry. If you attend one of our online, instructor-led classes, you will be sent a bottle of RMF Hot Sauce by mail. In order for this to work, please make sure we have a good shipping address for you (home or office, whichever works best).

Do you actually make the hot sauce? Is there a BAI Hot Sauce Factory somewhere?

Well, maybe someday, but no, we do not actually manufacture the hot sauce. We've used a couple of different manufacturers over the years. Currently, BAI Hot Sauce is made by a company called J's Small Batch Hot Sauce (jshotsauce.com). They produce and bottle the sauce and then apply our custom labels with the BAI logo and RMF life cycle steps. That said, we did conduct a "taste test" before selecting the particular sauce we provide. We hope it passes your personal "taste test" as well!

Why such a small bottle?

Our original DIACAP Hot Sauce came in "standard" size hot sauce bottles, which are 5 oz. We quickly heard from some students who were upset that their hot sauce had been confiscated from their carry-on bag by TSA at the airport. Alas, "3 oz. or less" was … and still is … the rule for liquids in carry-on baggage! We switched to a smaller bottle, which, over the years has been either 2 oz. (the size of a Tabasco sauce bottle) or 3 oz., which we use now.

Can I buy BAI Hot Sauce?

No, sorry. BAI Hot Sauce is normally available only to students who attend our training classes. However, from time to time, BAI attends various trade shows such as AFCEA West in San Diego, CA, AFITC in Montgomery, AL, or AFCEA Belvoir in Washington, DC. If you stop by our BAI booth at one of those events, you will most likely see a basket of hot sauce. Feel free to help yourself to a bottle.

I have a bottle of RMF Hot Sauce from the class I took a few months ago, but I'm a little bit afraid to try it. Just how hot is this stuff?

I'm not going to lie, it does have a good bit of heat to it. But it's nowhere near the heat level of those "physical challenge" type hot sauces you've probably seen. And besides, it's got lots of flavor. Go ahead, give it a try! *Accept the risk!*

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 (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 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.
- **Continuous Monitoring Fundamentals** – 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 June, 2021:

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

- Online Personal Classroom™ ▪ 11 - 14 JAN ▪ 25 - 28 JAN ▪ 1 - 4 FEB ▪ 8 - 11 FEB ▪ 22 - 25 FEB ▪ 1 - 4 MAR ▪ 15 - 18 MAR ▪ 29 MAR - 1 APR ▪ 5 - 8 APR ▪ 12 - 15 APR ▪ 26 - 29 APR ▪ 3 - 6 MAY ▪ 10 - 13 MAY ▪ 17 - 20 MAY ▪ 24 - 27 MAY ▪ 7 - 10 JUN ▪ 14 - 17 JUN ▪ 28 - 31 JUN
- San Diego ▪ 22 - 25 FEB ▪ 28 - 31 JUN
- Pensacola ▪ 8 - 11 MAR ▪ 26 - 29 APR
- Colorado Springs ▪ 15 - 18 MAR ▪ 14 - 17 JUN
- Virginia Beach ▪ 29 MAR - 1 APR ▪ 17 - 20 MAY

RMF Supplement for DCSA Cleared Contractors—1 day program

- Online Personal Classroom™ ▪ 19 JAN ▪ 24 MAR ▪ 19 APR ▪ 4 JUN ▪ 24 JUN

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

- Online Personal Classroom™ ▪ 19 - 21 JAN ▪ 16 - 18 FEB ▪ 22 - 24 MAR ▪ 19 - 21 APR ▪ 1 - 3 JUN ▪ 21 - 23 JUN

eMASS eSSENTIALS—1 day program

- Online Personal Classroom™ ▪ 15 JAN ▪ 29 JAN ▪ 5 FEB ▪ 12 FEB ▪ 26 FEB ▪ 5 MAR ▪ 12 MAR ▪ 19 MAR ▪ 2 APR ▪ 9 APR ▪ 30 APR ▪ 7 MAY ▪ 21 MAY ▪ 28 MAY ▪ 11 JUN ▪ 18 JUN
- San Diego ▪ 26 FEB ▪ 1 JUL
- Pensacola ▪ 12 MAR ▪ 30 APR
- Colorado Springs ▪ 19 MAR ▪ 18 JUN
- Virginia Beach ▪ 2 APR ▪ 21 MAY

STIG 101—1 day program

- Online Personal Classroom™ ▪ 21 JAN ▪ 16 FEB ▪ 19 MAR ▪ 16 APR ▪ 14 MAY ▪ 21 JUN ▪ 1 JUL

Continuous Monitoring Fundamentals—1 day program

- Online Personal Classroom™ ▪ 18 FEB ▪ 23 APR ▪ 3 JUN

RMF in the Cloud—1 day program

- Online Personal Classroom™ ▪ 22 JAN ▪ 26 MAR ▪ 23 APR ▪ 1 JUN ▪ 23 JUN

Security Controls Implementation & Assessment Workshop—4 day program

- Online Personal Classroom™ ▪ 25 - 28 JAN ▪ 22 - 25 MAR ▪ 19 - 22 APR ▪ 1 - 4 JUN ▪ 21 - 24 JUN

CAP Exam Preparation—1 day program

- Online Personal Classroom™ ▪ 26 MAR

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

- Online Personal Classroom™ ▪ 22 - 25 MAR