Risk Management Framework Today

... and Tomorrow

April, 2018
Volume 8, Issue 2

Find us on LinkedIn

In this issue:

RMF and the Defense Security Service (DSS)

By Lon J. Berman CISSP, RDRP

The Defense Security Service (DSS) serves as an interface between the government and cleared industry. DSS administers and implements the National Industrial Security Program (NISP) by providing oversight and assistance to cleared contractor facilities to ensure protection of classified information. In short, if your company maintains cleared personnel and/or processes classified information at your premises on behalf of a government customer, DSS will be part of your life.

Classified Information Systems (IS) at cleared contractor facilities are subject to Assessment and Authorization (A&A) in accordance with RMF. DSS has developed its own "flavor" of RMF that is tailored to best meet the needs of the cleared contractor community. The DSS Assessment and Authorization Program Manual (DAAPM) is the governing publication.

For the most part, DAAPM delineates the customary RMF roles and responsibilities – Authorizing Official (AO), Security Control Assessor (SCA), Information System Owner (ISO), Information System Security Manager/Officer (ISSM/ISSO), etc. Some of the role assignments are unique to DSS. For example, DSS Information System Security Professionals (ISSPs) are assigned the SCA role. DAAPM defines the role of Data Transfer Agent (DTA) with responsibility for secure transfer of information to and from the system. Additionally, there are specific training requirements for ISSMs, selected from the DSS Center for Development of Security Excellence (CDSE) catalog.

DAAPM specifies the customary six-step RMF process – Categorize, Select, Implement, Assess, Authorize, Monitor – and, again, there is some DSS-specific tailoring. For example, the system categorization for Confidentiality is limited to Moderate or High, due to the presence of classified information (Integrity and Availability categorization can still be Low, Moderate or High). To serve the needs of most customers, DSS publishes a security control baseline spreadsheet for a Moderate-Low-Low categorization, including the Classified overlay.

DAAPM also includes DSS-specific overlays that deal with three types of systems: Single User Standalone (SUSA), Multi User Standalone (MUSA) and Isolated LAN. Because of their limited connectivity, many controls have been removed from the system baselines by these overlays.

In the area of documentation, DAAPM provides a template for the System Security Plan (SSP) and the required appendices. The eMASS tool is not used, however DSS does provide the Office of the Designated Approving Authority Business Management System (OBMS) to facilitate submittal of completed RMF packages for DSS approval.

Overall, the DSS RMF process is largely similar to the standard RMF for DoD IT process, so "standard" RMF training is a good starting point. You can also visit www.dss.mil/rmf for additional information from DSS.

U.S. Department of Defense
DEFENSE SECURITY SERVICE

BAI Introduces: STIG 101 Training

By Kathryn Daily, CISSP, RDRP

NIST 800-53, and specifically Security Control CM-6, requires an organization to

a. Establish and document configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Note that DoD has mandated the use of "DoD security configuration or implementation guidance, e.g., Security Technical Implementation Guides (STIGs)" as the "organization-defined security configuration checklists" cited in paragraph a, above. STIGs are published by the Defense Information Systems Agency (DISA) and cover a wide variety of information technology products and processes. Unfortunately, simply having the STIGs does not ensure compliance. There are numerous challenges, such as:

- Limited Resources to assess compliance with numerous requirements
- Understanding what documents apply (STIGs, Checklists, Bench marks, etc.)
- Identifying a process by which to implement STIG guidance

STIG 101 meets the challenges above and more in a one-day STIG Overview course. Topics such as STIG Content, STIG Development, STIG Tools, and Best Practices are discussed. Demonstrations of STIG Viewer, SCAP Compliance Checker (SCC), and STIG implementation will be conducted to provide the students with a real world understanding of the STIG process. The development process will also be covered to give students an idea of where STIGs come from, who creates them, and how they get published.

This one-day course is suitable for anyone wishing to gain insight into STIG content and process. It is ideally suited to those with limited exposure to STIGs ... or even none at all!"

The course will be taught via Online Personal Classroom™. This is a fully interactive, instructor-led experience. There will be an initial informational section that introduces the concepts and best practices then we will move to the screensharing capability to demo the various tools that are available. We'll demo SCC, STIG viewer, and other tools while giving an overall approach to best practices. Specific pain points for students will be addressed, provided that it's feasible and within the scope of the course.

The biggest benefit from the class will be getting a process down to manage the often-cumbersome task of 'STIGing' your machines from the initial configuration through the quarterly STIG update process.

Questions regarding the upcoming STIG 101 course can be directed to kathryn@rmf.org; Registration can be done via the web at http://rmf.org/register or by contacting Alice at 800-763-1903 x106.

"... The biggest benefit from the class will be getting a process down to manage the often-cumbersome task of 'STIGing' your machines..."

Reflections from AFCEA Industry Days

By P. Devon Schall, M.S., MA.Ed. CISSP, RDRP

"... DoD executive level decision makers are very frustrated with RMF..."

On April 3rd and April 4th, I attended the Armed Forces Communications and Electronic Association (AFCEA) annual industry event titled AFCEA Belvoir Industry Days hosted at The Gaylord National Harbor in Maryland. The Belvoir chapter supports the Fort Belvoir community by connecting the government with IT industry professionals.

Fort Belvoir is home to over 90 diverse tenant and satellite organizations from the Department of Defense, including PEO EIS, INSCOM, Defense Logistics Agency (DLA), Army Cyber Command, Defense Threat Reduction Agency (DTRA), National Geospatial-Intelligence Agency (NGA), DTIC, PEO Soldier, and many others.

I was slightly hesitant to attend this event, as my previous experience with trade shows have not been very positive as they are often plagued with "swag collectors" and minimal decision makers. I am happy to report, AFCEA Belvoir Industry Days did not fall into this category, and I had the opportunity to network and meet many DoD and private industry leaders. RMF was a very hot topic at the event. My three biggest takeaways are listed below.

1. DoD executive level decision makers are very frustrated with RMF

RMF was created as a holistic cybersecurity framework to replace DIACAP and improve DoD cybersecurity, but it is turning into cybersecurity via compliance checklist. Lieutenant General Bruce T. Crawford, the Army Chief Information Officer/G-6 echoed this sentiment in his keynote speech saying that RMF needed to be turned on its side as it is not working the way it was intended to. Lieutenant General Crawford's statements were supported by Mr. David Kim the Chief Technology Officer & Director of The Technical Warfare Center as he presented a host of RMF questions and concerns.

2. DoD/private industry are experiencing a shortage of qualified RMF practitioners

I was continually asked if I had access to any "boots on the ground" RMF personnel. As a provider of training services, we do not currently place RMF contractors, but I was asked if I had access to qualified RMF workers a multitude of times. To help our students secure positions as RMF practitioners, BAI is responding to this shortage by developing an RMF job board which will be available to our students who are part of the Registered DoD RMF Practitioner Program (RDRP). If you would like to join the Registered DoD RMF Practitioner Program (RDRP) please go to https://rmf.org/rdrp/.

3. A need for **quality** RMF training exists

After reading the two statements above, it has been expressed that an immense amount of confusion exists regarding RMF and there is a shortage of RMF workers.

The solution to these two issues are quality RMF training solutions. Many organizations and training companies think they have a good understanding of RMF, but they may not be implementing RMF in the most effective capacity.

Our niche is RMF, and we have great pride in being "laser focused" on RMF. We often joke in our meetings that we should be using the tag line "RMF – It's Who We Are", but that catchphrase rings exceedingly true and is a great benefit in the current RMF landscape.

AFCEA

RMF Applied to Modern Vehicles

By P. Devon Schall, CISSP, RDRP

"...the most overwhelming issue I often see with RMF is that it has a lack of scalability…"

During a recent RMF literature search, I came across an interesting article titled "RMF Applied to Modern Vehicles". The article was published by Charlie McCarthy and Kevin Harnett in 2014 and sponsored by the National Highway Traffic Safety Administration (NHTSA). The overall goal of the research was to collect knowledge of how RMF applies to the automotive sector. Although the article provides a bulk of general RMF information, some interesting more granular observations were made and sharing these as well as discussing the scalability of RMF will be the focus of this article.

Modern automobiles have gone through dramatic technological advances in the last decade. Gone are the days of buying a Haynes or Chilton repair manual and performing maintenance in your driveway on a sunny spring afternoon. Modern vehicles have incredibly complex information systems and have an average of 80+ embedded control units (ECUs) as well as wired and wireless communications. The lines of code on these vehicles are also developing exponentially, with increasing likelihood of vulnerabilities being introduced in the System Development Life Cycle (SDLC).

The main conclusions of the study indicated that two primary considerations must be made in evaluating RMF implementation in automobiles.

1. System categorization would be difficult as a vehicle is not an information system, but more of a collection of complex interactions with various degrees of criticality. A modern vehicle cannot be used as a single purpose information system and the complexity of a modern vehicle would present numerous issues.

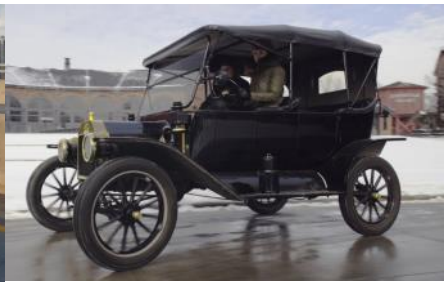
2. Vehicle sectors need to consider developing their own security control catalog that relates to this specific sector. The current security control catalog would not allow the level of granularity necessary in modern automated vehicles.

The findings above may appear to be common sense, but the most overwhelming issue I often see with RMF is that it has a lack of scalability. This lack of scalability becomes an issue when basic systems are subject to the equivalent amount of security controls as others which are more complicated and vice versa. RMF is not agile, and this lack of agility presents major problems regarding RMF scope and the pace at which RMF can be implemented.

BAI does not have a solution to the scalability issue discussed above, but we welcome comments and suggested RMF improvements. After visiting National Institute of Standards (NIST) and communicating with the team that creates these policies, it is critical that feedback is communicated to them. NIST also recognizes this and often provides a public comment timeframe before their publications are finalized. It is easy to 'rest on our laurels' regarding RMF, but it is far more effective to communicate with the team at NIST to work towards improving RMF and the state of our nations cyber defense.

References

McCarthy, C., & Harnett,(2014,October). National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles. (Report No. DOT HS 812 073). Washington, DC: National Highway Traffic Safety Administration



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, security controls, and transition from DIACAP to RMF.
- **RMF for Federal Agencies** - recommended for Federal "civil" agency (non-DoD) employees and contractors that require detailed RMF knowledge and skill training; covers the RMF life cycle, documentation, security controls, and transition from DIACAP to RMF.
- **eMASS eSSENTIALS** – designed as an add-on to RMF for DoD IT. This training program provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is utilized.
- **Continuous Monitoring Overview** – designed as an add-on to RMF for DoD IT. This is a one day "fundamentals" program.
- **RMF in the Cloud** – designed as an add-on to RMF for DoD IT. This one-day training program will provide students the knowledge needed to begin shifting their RMF efforts to a cloud environment.
- **Certified Authorization Professional (CAP) Preparation** – designed as a one-day add-on to RMF for DoD IT. CAP Prep provides preparation for the Certified Authorization Professional (CAP) certification administered through $(ISC)^2$.
- **STIG 101** – is designed to answer core questions and provide guidance on the implementation of DISA Security Technical Implementation Guides (STIGGs).

Our training delivery methods:

- **Traditional classroom** – regularly-scheduled training programs are offered at various locations nationwide, including Colorado Springs, Huntsville, National Capital Region (Pentagon/Crystal City area), Dallas, and San Diego.
- **Online Personal Classroom™** – regularly-scheduled training programs are also offered in an online, instructor-led format that enables you to actively participate from the comfort of your home or office
- **On-site training** – our instructors are available to deliver any of our training programs to a group of students from *your* organization at *your* site; please contact BAI at 1-800-RMF-1903 to discuss your requirements

Regularly-scheduled classes through September, 2018:

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

- **National Capital Region ▪ 9-12 JUL**
- **Huntsville ▪ 24 - 27 SEP**
- **Pensacola ▪ 7-10 MAY ▪ 13-16 AUG**
- **Colorado Springs ▪ 11-14 JUN ▪ 27-30 AUG**
- **San Diego ▪ 4-7 JUN ▪ 17-20 SEP**
- **Dallas ▪ 30 JULY - 2 AUG**
- **Online Personal Classroom™ ▪ 14-17 MAY ▪ 18-21 JUN ▪ 16-19 JUL ▪ 20 - 23 AUG ▪ 24 - 27 SEP**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 4 MAY ▪ 5 JUN ▪ 24 JUL ▪ 6 SEP**
- **National Capital Region ▪ 13 JUL**
- **Huntsville ▪ 28 SEP**
- **Pensacola ▪ 17 AUG**
- **Colorado Springs ▪ 31 AUG**
- **San Diego ▪ 21 SEP**
- **Dallas ▪ 3 AUG**

Continuous Monitoring Overview —1 day program

- **Online Personal Classroom™ ▪ 2 MAY ▪ 7 JUN ▪ 25 JUL**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 3 MAY ▪ 8 JUN ▪ 8 AUG**

CAP Prep—1 day program

- **Online Personal Classroom™ ▪ 1 MAY ▪ 6 JUN ▪ 5 SEP**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 30 APR ▪ 4 JUN ▪ 20 JUL ▪ 24 AUG ▪ 28 SEP**

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.

BAI