Risk Management Framework Today

… and Tomorrow

October, 2017
Volume 7, Issue 4

In this issue:

Is Your System a National Security System (NSS)? and How Does That Affect RMF Efforts?

By Lon J. Berman, CISSP, RDRP

By federal law, an information system will be designated as a National Security System (NSS) in accordance with the following definition:

The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function or use of which:

- involves intelligence activities
  - or -
- involves cryptologic activities related to national security
  - or -
- involves command and control of military forces
  - or -
- involves equipment that is an integral part of a weapon or weapons system
  - or -
- is critical to the direct fulfillment of military or intelligence missions *(with the exception of routine administrative of business systems)*
  - or -
- stores, processes or communicates classified information

If a system meets one or more of the above criteria, it should be designated as NSS. Systems that meet none of the above criteria are considered non-NSS. Additional information about NSS is provided in NIST Special Publication (SP) 800-59. This publication also includes the above NSS designation criteria in the form of a checklist.

Each agency is responsible for identifying all NSS under its ownership or control. The agency head is responsible for designating an agency information security official to determine which, if any, agency systems are NSS.

For non-NSS, the Secretary of Commerce is responsible for prescribing security standards and guidelines, based on publications of the National Institute for Standards and Technology (NIST). For NSS, the Committee on National Security Systems (CNSS) is responsible for providing security standards and guidelines.
At this point you might be thinking,

"Whoa … wait a minute! With two different organizations responsible for providing security standards, what's to stop things from ending up with totally different security controls and life cycle processes for NSS and non-NSS?" The reason we need not be fearful of things going in that direction can be summed up in three letters: R-M-F. Departments and agencies across the government landscape … including DoD, federal "civil" agencies, and the intelligence community … have all made a commitment to use the Risk Management Framework (RMF) as the basis of their information system security authorization and life cycle management processes.

Both NSS and non-NSS draw their security control baselines from the same "catalog" (i.e., NIST SP 800-53). The only difference lies in the process used to *build* the baseline. For non-NSS, systems are categorized as High, Moderate or Low, in accordance with FIPS 199, and the appropriate security control baseline is then selected from NIST SP 800-53. For NSS, categorization is done in accordance with CNSSI 1253 (rather than FIPS 199). NSS are categorized separately for each of the three security objectives (Confidentiality, Integrity and Availability), resulting in a categorization such as "Low, Low, Low", "Moderate, Moderate, Low", "Moderate, Moderate, High", etc. CNSSI 1253 further provides the appropriate baseline of security controls for each of the 27 possible system categorizations. The controls themselves still come from NIST SP 800-53.

Once the security control baseline has been established, the remainder of the RMF life cycle (i.e., security control implementation, security control assessment, system authorization, and continuous monitoring) is identical for both NSS and non-NSS.

That's the end of the story for systems owned by (or operated on behalf of) departments or agencies outside of DoD. For systems owned by (or operated on

See *Is Your System NSS?*, Page 2

RMF: Is It Effective?

By Kathryn Daily, CISSP, RDRP

"… The leading threat source is reported as careless untrained insiders..."

In July 2017, SolarWinds conducted an online survey via Market Connections aimed at approximately 200 federal government IT decision makers and influencers in order to determine challenges faced by IT professionals to prevent security threats, quantify sources and types of IT threats, determine elements that aid successful management of risk, gauge sentiments regarding mandates and compliance and address the effect of network modernization on agency IT security challenges. 95% of respondents were federal, civilian or independent government agencies or DoD or Military Service with a wide range of involvement in decision making.

More than three fourths describe their agency's ability to provide managers and auditors with evidence of appropriate IT controls as either excellent or good (27% excellent, 52% good). Not surprisingly, budget constraints top the list of significant obstacles. While foreign governments top the national news headlines, they are noted as only the second highest source of security threats (48%). The leading threat source is reported as careless/untrained insiders (54%). Careless/untrained insiders increased from 48% in 2016 to 54% with foreign governments remaining static since last year.

A significantly greater proportion of respondents that rate their agency's ability to provide managers with evidence of IT controls as fair/poor tend to indicate they have seen an increase in SPAM, external hacking and denial of service. A significantly greater proportion of respondents that rate their agencies ability to provide evidence of IT controls as excellent indicate that they have seen a decrease in most cyber security threats. This is an indication of the effectiveness of the Risk Management Framework. Over half of respondents indicated that while RMF posed more of a challenge, it also contributed to success.

NIST Cybersecurity Framework appears to be successful in promoting a dialog about managing risk, but opinions are split as to whether federal IT professionals fully understand the framework.

Over half of respondents state that federal agencies are more proactive than they were five years ago and that compliance has helped their agency improve its cybersecurity capabilities.

When it comes to compliance and risk management, 70% agree that being compliant does not necessarily mean being secure, 58% agree that risk management is too often treated as a compliance issue

See *RMF: Is It Effective?*, Page 3

***Is Your System NSS?*, from Page 1**

behalf of) DoD, things are a bit different – but simpler!

In its adoption of RMF, DoD has mandated that system categorization and security control selection be performed in accordance with CNSSI 1253 for all systems, regardless of whether they are NSS or non-NSS. Another way to put this is that DoD has mandated that, for RMF purposes, all information systems be treated as if they were NSS. DoD system owners using eMASS will be asked to indicate whether their system is NSS or non-NSS, but the answer provided will have no material effect on the RMF process itself.

It's important to understand that DoD has not declared all of its information systems to be NSS. Neither DoD, nor any other federal department or agency, has the statutory authority to do such a thing, and the criteria for designating a system as NSS are clearly stated in FISMA.

Cybersecurity Can't Be Bolt-On

By P. Devon Schall, CISSP, RDRP

As I work with clients on assessing their posture with the RMF control families, I am consistently amazed at how many businesses see cybersecurity as an afterthought. More and more often I conclude that many small to medium sized DoD contractors would not implement cybersecurity controls unless required to. The conversation of cybersecurity comes up when these companies discover their contractual RMF obligations. Unfortunately, upon the "do RMF" discovery, they realize they are not prepared for the financial and workload magnitude of the requirement. Some common statements are, "we have so many other more important things than RMF to do" and "RMF is not increasing our bottom line." With or without expansive budgets, companies must come to the table with cost effective cybersecurity defensive strategies. The three suggestions below provide solutions to strengthen cybersecurity posturing with ever tightening budgets while satisfying some of those pesky RMF security controls.

1. Introduce "Lunch and Learn" events that reinforce cybersecurity awareness training for your staff. After all, people are the biggest risk in cybersecurity. Implementing a few trainings sessions yearly is far less costly than having a cybersecurity incident. These cybersecurity trainings will also satisfy Awareness and Training (AT) RMF controls. We often take non-technical staff members for granted and assume they think about cybersecurity as much as we do. In reality, they may forget about their annual cybersecurity awareness training as quickly as they registered for it.

2. Consider choosing a member of your IT staff and authorizing them to obtain a credential such as CompTIA's Security+ or the gold standard, Certified Information System Security Professional (CISSP) offered by (ISC)2. By getting a member of your IT staff certified, you're creating expertise and showing your staff that you believe in investing in them. Contrary to popular belief, these exams can be "cleared" with minimal financial investment, and if CISSP is too intensive, take a look at Security+ which is much more approachable and a good jumping off point.

3. Consider engaging a Virtual Information Systems Security Officer (vISSO) or a Virtual Chief Information Security Officer (vCISO). Every large company, at the very least should have a dedicated CISO on staff, but for a smaller business full-time CISOs may be out of reach. Virtual ISSOs or CISOs can be put on retainer, hired by project, or provide a block of monthly support hours. Having these kinds of experts provide expertise that may be out of scope for a local hire.

RMF: Is It Effective?, From Page 2

and security regulations and mandates lead to complacency since tasks are performed to 'check a box'.

When compared to the commercial sector, nearly half feel their agency's security practices are on par with commercial companies and slightly over half indicate that their ability to provide managers with evidence of IT controls is more robust than those in the commercial sector.

I believe that the key takeaway from this data is that while most agree that compliance has helped their agency improve its cybersecurity capabilities, 70% believe that being compliant does not mean being secure, and over half believe that regulations and mandates can lead to complacency as tasks are performed to check a box.

See the entire survey here: https://www.slideshare.net/SolarWinds/solarwinds-federal-cybersecurity-survey-2017-government-regulations-it-modernization-and-careless-insiders-undermine-federal-agencies-security-posture/1

Top Ten—Differences Between RMF and CSF

By P. Devon Schall, CISSP, RDRP

I was reading an article recently about Cybersecurity Framework (CSF) and the continued confusion with Risk Management Framework (RMF). In the research, the consensus was the majority of government IT professionals don't fully understand CSF or RMF and find it easy to confuse the two. As a follow up to my previous CSF article, I hope the top 10 list below can continue to clear up the differences in the frameworks.

10. **RMF automated tools do not support CSF.** Numerous tools have been developed (such as DoD eMASS) to streamline RMF process workflow. There are no known plans for any of these tools to provide CSF support.

9. **RMF is much more prescriptive than CSF.** RMF's audience is the entire federal government and CSF was initially developed for critical infrastructure. CSF has also been recommended for use in organizations regardless of size, degree of cybersecurity risk, or cybersecurity sophistication including industry. Bottom line: RMF has a very prescriptive process including formal Authorization to Operate (ATO) whereas CSF is still in initial stages of implementation with recommended voluntary usage.

"...CSF does not have Authorizing Officials (AO's)..."

8. **RMF is much more extensively documented than CSF.** The document outlining CSF titled "The Framework for Improving Critical Infrastructure" is 41 pages. "The Guide for Applying the Risk Management Framework to Federal Information Systems" is 102 pages and is supported by numerous NIST Special Publications (SPs). It is very easy to start reading RMF documentation and get "stuck in the weeds". One of my favorite aspects of CSF is approachable documentation.

7. **CSF is aimed at private industry.** The National Institute of Standards and Technology (NIST) encourages CSF use in private industry, particularly those supporting "critical infrastructure" (e.g., transportation, public utilities). A great example can be seen in the Intel Corp. case study "An Intel Use case for the Cybersecurity Framework in Action". RMF is aimed primarily at government and is only rarely used in the private sector.

6. **The steps in the RMF and CSF process are different.** The RMF process has six steps. These steps are: Categorize, Select, Implement, Assess, Authorize, and Monitor. The CSF process has seven-steps. CSF steps are: Prioritize and Scope, Orient, Create a Current Profile, Conduct a Risk Assessment, Create a Target Profile, Determine, Analyze, and Prioritize Gaps, and Implement Action Plan.

5. **RMF controls can be used with CSF, but CSF does not have its own set of security controls.** CSF maps to a variety of functions titled: Identify, Protect, Detect, Respond, and Recovery. Each of these functions ties to categories that can be satisfied via a variety of controls families such as COBIT 5, NIST SP 800-53, and ISO/IEC 27001.

4. **CSF does not have Authorizing Officials (AOs) or an Authority to Operate (ATO).** RMF involves ATOs with determined authorization periods requiring approval by an Authorizing Official (AO). In contrast, CSF is a voluntary framework intended to strengthen cybersecurity posturing. CSF does not have an AO function or finite ATO's.

3. **RMF generally requires the participation of a variety of government entities.** For example, Joe Contractor cannot go through the complete RMF process alone. The involvement of government officials is required in achieving an ATO. CSF can be implemented without government assistance.

2. **NIST has recommended that CSF be used to strengthen RMF.** Elements of CSF can be used to make RMF more robust. Personally, I don't know who has the time to make RMF more complicated than it is, but with unlimited time to implement cybersecurity frameworks anything is possible.

1. **CSF is not intended to replace RMF.** CSF is NOT a "rip and replace" of RMF. The sweat and tears we have gone through in learning RMF are not in vain. NIST has suggested we may see some CSF language in new releases of NIST SPs, but overall the goals of the two frameworks are very different.

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. The program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **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. The program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **eMASS eSSENTIALS** – designed as an add-on to RMF for DoD IT. Recommended for government employees and contractors working (or planning to work) in the DoD environment, this one-day training program provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is used to reinforce the practical skills needed to use eMASS.
- **Information Security Continuous Monitoring (ISCM)** – open to all, however prior knowledge of RMF is recommended. This is a three day "in depth" program.
- **Information Security Continuous Monitoring (ISCM) Fundamentals** – 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. Recommended for government employees and contractors working (or planning to work) in the cloud environment, 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 an add-on to RMF for DoD IT. Recommended for government employees and contractors interested in preparation for the Certified Authorization Professional (CAP) certification administered through (ISC)2.
- **Certified Information Systems Security Professional (CISSP) Preparation** – recommended for anyone interested in preparation for the "gold standard" Certified Information Systems Security Professional (CISSP) certification administered through (ISC)2.

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, Oakland 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 April, 2018:

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

- **National Capital Region ▪ 29 JAN-1 FEB**
- **Huntsville ▪ 4-7 DEC ▪ 26 FEB-1 MAR**
- **Colorado Springs ▪ 4-7 DEC ▪ 26-29 MAR**
- **Pensacola ▪ 6-9 NOV**
- **San Diego ▪ 11-14 DEC ▪ 12-15 MAR**
- **Dallas ▪ 12-15 FEB**
- **Online Personal Classroom™ ▪ 13-16 NOV ▪ 11-14 DEC ▪ 22-25 JAN ▪ 12-15 FEB ▪ 19-22 MAR**

CISSP Preparation—5 day program

- **Oakland ▪ 26 FEB - 2 MAR**
- **Dallas ▪ 19-23 MAR**
- **National Capitol Region ▪ 9-13 APR**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 25 OCT ▪ 15 NOV ▪ 13 DEC ▪ 15 JAN ▪ 6 FEB ▪ 7 MAR ▪ 5 APR**

ISCM Fundamentals —1 day program

- **Online Personal Classroom™ ▪ 8 FEB ▪ 9 MAR ▪ 3 APR**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 9 FEB ▪ 6 MAR ▪ 4 APR**

CAP Prep—1 day program

- **Online Personal Classroom™ ▪ 7 FEB ▪ 8 MAR ▪ 6 APR**

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.