**RMF – Frequently Asked Questions (FAQ)**

1. **Do all facilities have to implement RMF?** Yes. Beginning 1 January 2018 all submissions will be required to be under the NIST RMF process in accordance with the DAAPM.
2. **How long would it take for Industry to prepare and complete the RMF package?** As with any new process, the first SSP submission will be the most challenging. RMF is a new process for both ISSPs and ISSMs. Success can only be achieved by becoming familiar with the DAAPM and utilizing all available resources. After the first SSP submission is completed, the process will become more routine.
3. **How long will accreditation of systems take under the new process? Is the expectation that the ISSP will just review within 30 days or will there be constant contact from the ISSP once the package is submitted?** Upon receipt of a complete and accurate System Security Plan (SSP) with all required supporting artifacts, DSS’s goal is to complete authorization actions within 30 days. However, sending a submission back for clarification stops the clock. The status of all submissions can be tracked via the ODAA Business Management System (OBMS).
4. **How many controls are there for a MUSA?** The number of controls is decided in Step 2 of the RMF Process. The initial set of baseline security controls for the IS are based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions. The ISSM or designee will utilize the DSS Overlays to assist with tailoring control selection.
5. **For proposal systems that are already built and hardened but have no information on them, does that help expedite the RMF process?** Yes. By taking proactive measures and utilizing the DSS Overlays and DISA Scanning Tools to prepare the SSP and configure the IS, the ISSM assists in expediting the authorization process while allowing NAO to maintain appropriate oversight. The AO has the authority to issue an authorization with an option to waive the on-site. The AO has the final decision to determine if the on-site will be waived. It is imperative that ISSMs identify the IS Profile name as "Proposal System" within OBMS, provide a proper system description, and contact their assigned ISSP.
6. **Is the Mobility System Plan attached to the RMF SSP or is it a separate document?** For IS submissions including a Mobility System Plan, include the required supporting artifact. A Mobility System Plan template is located in the SSP Appendices (http://www.dss.mil/documents/rmf/SSP\_APPENDICES\_8\_23\_16.docx).
7. **Who is responsible for the categorization/definition of systems?** The categorization/definition of systems is responsibility of the ISSM, who proposes the initial impact levels based upon contractual requirements and the Risk Assessment. DSS has identified a categorization of M-L-L as the baseline absent information which would move it higher.
8. **How do you determine the risk assessment baseline?** A Risk Assessment Report (RAR) template is located within the SSP Template Appendices on the DSS RMF website (http://www.dss.mil/rmf/). The ISSM can use NIST-800-30 for further guidance about how to perform a risk assessment. Each contractor has specific concerns for their facility/program which should be taken into consideration when performing the assessment. The ISSM will categorize the system based on the impact due a loss of confidentiality, integrity, and availability of the information according to data provided by the Information Owner (IO) or DSS (CI-Threat reports). It is highly recommended to leverage the Insider Threat Program implemented at the facility.
9. **Are the overlays located on the DSS website?** The overlays are located in the DSS Assessment and Authorization Manual Process Manual (DAAPM). The DAAPM is located on the RMF website (http://www.dss.mil/rmf/).
10. **What is the timeline for requiring the other system types (LANs/WANs/Test Stands) to be submitted under RMF?** See question number 1 for the timeline. Facilities also have the option of submitting all plans under RMF at any time.
11. **In RMF, how will networks with different Need To Know (NTK) and Formal Access Approvals be handled?** With the transition to NIST RMF, the controls will address the requirements. The facility will then be able to address NTK and Formal Access Approval.
12. **For those in Industry with DoD-Approved External PKI certificates (not CAC cards), what is the process for obtaining DoD employee sponsorship to gain access to the** [**DoD RMF Knowledge Service**](https://rmfks.osd.mil/login.htm)**?** Currently, industry does not need access to the DoD RMF Knowledge Service.
13. **Will Industry be assessed against PKI-protected DISA STIGs? If so, could this content be added to OBMS?** In order to streamline the onsite validation of a system, DSS will utilize the DISA STIG, associated benchmark and STIG Viewer to assess the controls documented within the System Security Plan (SSP). Industry is not required to STIG their systems. However, they must identify their baseline standards within their SSP (e.g. NIST, NSA, STIG). DSS as the Security Control Assessor (SCA) and NISP authorization authority will leverage the DISA STIGs for assessment of the implementation of RMF technical security controls. In coordination with DISA and SPAWAR, DSS received approval to host PKI-protected Security Content Automation Protocol (SCAP) Compliance Checker (SCC). PKI protected SCC files are now available for download through the OBMS Headquarters Bulletin Board.
14. **What are high-level plans for flaw remediation under the NIST RMF for operating systems, firmware and applications? Will Industry be expected to follow the DIACAP IAVA / IAVM processes?** The ISSM will define an appropriate flaw remediation plan within the associated System Security Plan (SSP). The defined time periods for updating security-relevant software and firmware may vary due to a variety of factors including security category and criticality of the update (e.g. severity of the vulnerability related to the discovered flaw). Industry will not be expected to follow the DIACAP IAVA / IAVM processes.
15. **Will there be an equivalent to RALs under the NIST RMF, or, should current RALs go into the POA&M?** For controls tailored out based on program or system requirements, justification must be provided via a SOW, contract, or artifact from the Information Owner (IO).
16. **Are there plans to use the DISA Secure Host Baseline on ISs under NIST RMF?** No. The ISSM will document their operating system configuration tool within their SSP. If the contractor is required to utilize the DISA SHB through a contractual agreement or interconnection service agreement (ISA/MOU), then the contractor will coordinate with the sponsor to obtain appropriate licenses for the software.
17. **Will DSS stay with the current OBMS tool using MS Office document templates or transition to an IA Management Tool like Xacta or eMass? If transitioning to another IA Management tool, what the timing might be?**OBMS is the system of record for all DSS Assessment and Authorization actions.
18. **The Clearing and Sanitization Matrix is no longer referenced or is included in the DAAPM. Should we be following the NIST SP 800-88 Rev. 1?** The Clearing and Sanitization Matrix is included in DAAPM v1.1, released 31 March 2017. It is located within Appendix L.
19. **OBMS does not support all file types – we just submitted 2 RMF laptop packages, but had to email the SSP.xls files.** The Instructions Tab of the Excel RMF SSP provides instructions on converting the .xls files to .pdf and uploading to OBMS.
20. **In order to address RMF -1 controls, can a facility utilize corporate policy documents rather than creating individual policy documents?** If the corporate policy document clearly addresses all policies and procedures applicable to the control, this would be acceptable.
21. **Previous DSS Guidance on Legacy Operating Systems identified that “Standard test equipment and/or peripherals with unsupported operating systems do not require a RAL or POA&M (note: this is true test equipment…examples include but are not limited to logic/spectrum analyzers, oscilloscopes, signal tracers/generators, frequency synthesizers, meters, etc.).” Will this remain the case under RMF?** Within RMF the ISSM will document the controls as appropriate for any system type (e.g. Test Equipment). Controls that require tailoring out due to a lack of system capabilities will provide appropriate justification or mitigations within the SSP.
22. **Is Industry currently required to submit a POA&M regarding the plans to upgrade to RMF after receipt of an ATO? Upon release of the DAAPM, verbiage to this effect had originally been included in ATOs and is still referenced on the DSS website.** The requirement for a POA&M has been removed from DAAPM v1.1 and from the DSS web site.
23. **Under RMF, will there be a need to separately identify operating system Security Relevant Objects (SROs) (such as %SystemRoot%\system32\kerberos.dll) to lock down and audit since they are not addressed in the STIGs? If so, will DSS be providing a list of these SROs on new operating systems?** No, DSS will not publish a separate SRO listing as in previous DSS Baseline Technical Security Guides. Please refer to the applicable operating system STIG for specific audit requirements. In the case of operating systems that do not have STIG baselines available, ISSMs will define the strategy for affected controls within the individual control implementation justification, subject to SCA and AO review.
24. **Is the POA&M, SSP, Scan Results, and Supporting Artifacts considered classified?** DSS is not a classification authority for the POA&M, SSP, Scan Results, and Supporting Artifacts. Therefore, ISSMs are required to review Security Classification Guidance (SCG) and/or seek guidance from the appropriate Information Owner (IO) or Program personnel before submitting or storing information on an unclassified medium. Only unclassified documents can be uploaded and submitted via OBMS. If artifacts are deemed classified, contact assigned ISSP for guidance.