# NCMS the Society of Industrial Security Professionals

## 2018 Frequently Asked Questions (FAQs)

1. **I am a Facility Security Officer (FSO), will I have a role in the Defense Information Systems Agency (DISA) Enterprise Mission Assurance Support Service (eMASS) tool?**

   **Answer:** Roles within the eMASS tool are determined by the company/organization. However, the FSO is responsible for supporting the ISSM in their efforts to implement the systems security program and policies for their assigned area of responsibility. See DAAPM V1.3, Section 3.8 for more information on FSO roles and responsibilities.

2. **If I have reached out to my ISSP several times and have not heard anything back, how long should I wait before escalating to the ISSP's Team Lead or Regional Authorizing Official?**

   **Answer:** There is no definitive length of time that an ISSM should wait before escalating an issue. If the ISSM has been unsuccessful in attempting to communicate with their assigned ISSP (phone call, voicemail and email) for an issue that may cause a major disruption to the overall mission; reach out to the ISSP's team lead or AO.

3. **In the past, we have been told "verbally" by our ISSP that as long as we have submitted our RMF package prior to the expiration date, we should be able to continue to operate while the package is being reviewed. Is a verbal Authority to Operate (ATO) sufficient if we have done our due diligence to submit our package ahead of time?**

   **Answer:** No. A verbal ATO does not exist. Processing classified information must stop immediately. It is recommended that packages are submitted 90 days prior expiration to allow time to actively engage with you ISSP and escalate is necessary prior to expiration.

4. **On the RMF site, one of the questions listed on the 2017 NCMS FAQs state that Risk Acknowledgement Letters (RAL) are no longer required. However, my current ATOs with Conditions are still requiring RALs.**

   **Answer:** A Risk Acknowledgement Letter (RAL) is no longer a requirement for RMF packages. If a security control(s) within the DSS baseline is tailored out, modified or listed as not applicable, the AO must be provided with the complete rationale. The justification should be described as to why the control does not apply or how it is satisfied by other mitigating factors. (e.g., contractual requirements listed in DD254, defense in depth etc.)

5. **Will eMASS notify the ISSPs when a package has been submitted? Currently OBMS does not.**

   **Answer:** Yes. Email notifications for workload tasks are generated when a specific event occurs that requires an action to be performed by the authorized user. Workload tasks are reported to all users given a specific role in a system when an event has taken place related to that role.

   Examples of Workload notifications include: Packages pending review and approval, security controls approaching revalidation, systems approaching the Authorization Termination Date etc.

6. **What information should be listed on the POAM? All items or IT security related items?**

   **Answer:** Some items that should be listed in the Plan of Actions and Milestones (POA&M) include:

   - Remediation or mitigation tasks for non-compliant security controls
   - Required resources
   - Milestones and completion dates
   - Inherited vulnerabilities

7. **Should we be tailoring out security controls? The guidance that I received was not to tailor out any controls from the DSS baseline.**

   **Answer:** Yes. Security controls may be tailored in, tailored out or modified as needed. If a security control identified in the DSS baseline is tailored out, an explanation must be provided in the SSP, describing the rationale as to why the control does not apply or how it is satisfied by other mitigating factors. See DAAPM v1.3, section 6.2 for more information on the selection and tailoring of security controls.

**8. Do ISSPs have the ability to sponsor ISSMs for the RMF Knowledge Service?**

**Answer:** Yes. Your assigned ISSP has the ability to sponsor ISSMs on the RMF Knowledge Center website. A Job Aid is available with details on obtaining sponsorship at the RMF Information and Resources Page: (http://www.dss.mil/rmf/) Please contact your local ISSP for more information.

**9. With the release of DAAPM V1.3, should we expect an update to the templates, appendices, and job aids?**

**Answer:** No. The release of DAAPM v1.3 does not require an update to any existing templates, appendices or job aids.

**10. What does type authorization look like under RMF? Is it still authorized?**

**Answer:** Per the DAAPM v1.3, Type Authorization will only be granted if the AO/ISSP has determined that the ISSM has the requisite knowledge and skills. Type Authorization is used in conjunction with the authorization of site-specific controls (e.g., physical and environmental protection controls, personnel security controls) inherited by the system. The exception to Type Authorization includes all Interconnected Government-to-Contractor connections (Examples: SIPRNet, MDACNet, SDREN, etc.).

The NISP SIPRNet Circuit Approval Process (NSCAP), in conjunction with the DISA DISN Connection Process Guide (CPG), must be followed for design, implementation, operation, and decommissioning (disposal) of SIPRNet systems. The facility is not authorized to utilize a combination of conditions from multiple authorized MSSPs. The system must be an identical copy.

For example, a Type Authorized system must be:

1. Operating under the same security categorization (low, moderate, or high).
2. Possessing the same technical configuration.
3. Possessing operating characteristics and security needs that are essentially the same (e.g., configuration, operating system (OS), hardware, risk profile, network policy, security suite, physical controls, etc.).
4. Residing in the same general operating environments.

Please see DAAPM v1.3, section 9.2 for more information and guidance on Type Authorization.

**11. How long is the turnaround for proposal systems?**

**Answer:** No definitive turnaround time is established for proposal systems. The ISSM can expedite the authorization process by taking proactive measures. These actions include utilizing the DSS Overlays and Defense Information Systems Agency (DISA) Scanning Tools to prepare the SSP and properly configure the system. The Authorizing Official (AO) has the authority to issue an authorization with an option to waive the on-site. The ISSM must identify the System Profile name as "Proposal System" within the Office of the Designated Approving Authority (ODAA) Business Management System (OBMS) or NISP-eMASS as applicable. A proper system description is also required. The last step is to contact the assigned ISSP.

**12. I have a plan that has been in the cue for 81 days, now that DAAPM 1.3 has been released, should I recall my plan or continue to proceed with the steps.**

**Answer:** Contact your assigned ISSP or Team Lead for guidance or questions regarding your current RMF package.

**13. I am in step 2 (SELECT) phase of the RMF process, I have a TS system, and does my CIA classification remain Moderate-Low-Low?**

**Answer:** According to the NISPOM Change 2, Section 8-301, the contractor will categorize the potential impact level for confidentiality based on the classification level of the system (CONFIDENTIAL = Low; SECRET = Moderate; TOP SECRET = High). When the loss of availability and integrity is not required by contract, the security control baseline will be Low, Low. See NISPOM Change 2, section 8-301 and DAAPM v1.3, section 6.1 for more information on system categorization.

**14. I am currently working under C&A accreditation. I am utilizing windows 7 operating system but want to add Windows 10 computers, will I need to wait for my C&A package to expire then add the WIN 10 under the new RMF process or can I add it to my current C&A ATO?**

**Answer:** Contact your assigned ISSP or Team Lead for guidance or questions regarding your current RMF package.

15. **I am an FSO/ISSM, I have unable to get in contact with my ISSP for a couple months and I have packages sitting in the cue and continuing to expire. What should I do?**

**Answer:** If you are unable to contact your assigned ISSP for an extended amount of time, please reach out to the assigned Team Lead or AO.

16. **Is there regional organizational chart available to Industry to provide the chain of command structure for each region? Specifically, the contact information for ISSPs, team leads, AO's and Regional Directors (RD)?**

**Answer**: Contact your assigned field office for more information on the RD/AO/ISSP Team Lead/ISSP organizational structure. Visit the "DSS Field Office Locations" site (http://www.dss.mil/isp/dss_oper_loc.html) to obtain the email mailbox and phone numbers for your assigned region.

17. **Will the DSS instance of eMASS sit on the SIPRNET?**

**Answer:** No. The NISP instance of eMASS will be hosted on the unclassified network. Similar to the RMF implementation, the transition to eMASS will be a phased approach. Please visit the RMF Resource Center (http://www.dss.mil/rmf/) for the latest news on the eMASS transition timeline.

18. **How do I obtain access to eMASS?**

**Answer:** The NISP Authorization Office (NAO) has created a job aid for cleared industry to obtain access and sponsorship to the NISP eMASS. These instructions will allow NISP partners to access and complete the required DISA computer-based training beginning on July 2, 2018. Please visit the RMF Resource Center located at (http://www.dss.mil/rmf/) under the "Resources" header.

19. **Will training be available in preparation for the eMASS transition?**

**Answer:** Yes. Visit the RMF Resource Center (http://www.dss.mil/rmf/) for information on upcoming training, webinars, and job aids regarding eMASS.

**20. I have a security control that requires me to have a 14 character password but my customer requirements call for the system to have a 10 character password. Detailing this information in the POAM now serves as a vulnerability. What should I do?**

**Answer:** If the Information Owner (IO) has specific requirements that do not comply with to the NIST security control set, proper justification and supporting artifacts should be included in your SSP. A POA&M should include items that have a plan in place to mitigate. If there is no plan to mitigate due to IO requirements, the control should not be listed on the POAM.