NCMS - The Society of Industrial Security Professionals
2017 Questions and Answers

1. You mentioned the Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM) update version 2 is scheduled to be released in September; will I fail the onsite or plan review if I draft the System Security Plan (SSP) to meet the DAAPM version 1.1 prior to the release of version 2.0?

Answer: If the SSP is submitted prior to the release of DAAPM version 2.0, the Information Systems Security Manager (ISSM) will not fail the plan review or on-site for preparing the SSP in accordance with DAAPM version 1.1. Regardless of status, you should immediately begin planning to transition to RMF. As always, work with your assigned Information Systems Security Professional (ISSP).

2. Do we have to update the SSP to meet DAAPM version 2.0 requirements when the SSP (submitted under DAAPM ver. 1.1) is kicked back for revision after DAAPM version 2.0 is released?

Answer: No. If the SSP is submitted prior to the release of DAAPM version 2.0, the ISSM will only be required to correct the deficiencies identified by the ISSP. As always, work with your assigned ISSP.

3. Do you have anything in place to get plans approved quicker so that we can respond to Request For Proposals (RFPs)?

Answer: The ISSM can assist in expediting the authorization process by taking proactive measures and utilizing the DSS Overlays and Defense Information Systems Agency (DISA) Scanning Tools to prepare the SSP and configure the Information System (IS) thereby enabling National Industrial Security Program (NISP) Authorization Office (NAO) to maintain appropriate oversight. The Authorizing Official (AO) has the authority to issue an authorization with an option to waive the on-site. It is imperative that ISSMs identify the IS Profile name as "Proposal System" within the Office of the Designated Approving Authority (ODAA) Business Management System (OBMS), provide a proper system description, and contact their assigned ISSP.

4. What kind of artifacts are required for a proposal system?

Answer: Artifacts that are required for *all systems* include the following:

- System Security Plan (SSP)
- Certification Statement
- Risk Assessment Report (RAR)
- Plan of Action and Milestones (POA&M) - if applicable
- Supporting Contractual Requirements (i.e. RFP)
- Artifacts that support SSP implementation strategy (i.e. Standard Operating Procedures (SOPs), Facility Policies, Risk Acknowledgement Letters (RALs), etc.)

5. Can we get more than one system approved on the Department of Defense Form 254 Contract Security Classification Specification (DD-254)?

Answer: No.

6. What is the total number of days to get a system approved?

Answer: Upon receipt of a complete and accurate SSP with all required supporting artifacts, DSS's goal is to complete authorization actions within 30 days. The status of all submissions can be tracked via the OBMS.

7. Please explain Type Authorization. Is it the same as self-certification? ISSM can add a workstation to the Local Area Network (LAN) but can they standup a new Multi-User Standalone (MUSA) system?

Answer: Type authorization is an official authorization decision to employ identical copies of an information system or subsystem (including hardware, software, firmware, and/or applications) in specified environments of operation (i.e., same classification, contract, and physical environment). This form of authorization allows a single authorization package (i.e., system security plan, security assessment report, and plan of action and milestones) to be developed for an archetype (common) version of an information system that is deployed within the specified Commercial and Government Entity (CAGE) code resulting in a single Authorization to Operate (ATO).

Type authorization is NOT the same as self-certification. With Type Authorization, facilities cannot use a combination of conditions from multiple authorized Master System Security Plans (MSSPs). The system must be an exact carbon copy.

Under an ATO granting Type Authorization, facilities can add identical workstations to the authorized LAN. At this time, facilities cannot standup a new MUSA utilizing Type Authorization.

8. Can we have Type Authorization for systems under different DD-254s?

Answer: As stated above, Type Authorization is an official authorization decision to employ identical copies of an information system or subsystem (including hardware, software, firmware, and/or applications) in specified environments of operation (i.e., same classification, contract, and physical environment). Thus, systems under different DD-254s would need to meet all the conditions of Type Authorization listed above.

9. Is DSS managing Type Authorization by operating system or hardware (example: do I need to have the same laptop model number?)

Answer: The hardware does not need to be the same make and model/SKU (e.g. Dell XPS 13 laptop) to be Type Authorized. However, the hardware must be the same type (laptop vs. workstation, etc.) and operate under the same conditions and controls as the authorization (i.e. same operating system, applications, connectivity, classification, contract, and physical environment).

10. Do contractor ISSMs/Information Systems Security Officers (ISSOs) need to meet the Department of Defense (DoD) 8570.01-M training requirement?

Answer: No. However, DoD 8570 certification is a best practice and sponsors may sometimes require it as a condition of the contract. Review the associated contract, associated attachments and appendix to determine the DoD 8570.01-M training requirement from the government contracting authority.

11. Why have the Excel spreadsheet SSP templates when my ISSP refuses to accept it?

Answer: A facility may submit the SSP in either the Word or Excel template. The deciding factor in acceptance of the SSP will be the submission of a complete and accurate SSP.

12. What are the requirements for getting open source software approved for use on a classified system? Some software does not have source code for review. Also, do I need to review the source code for open source operating systems (such as Ubuntu)?

Answer: Facilities should work with their DSS ISSPs to determine the feasibility of implementing open source software solutions on classified information systems, and the review requirements to do so in accordance with applicable policy on a case-by-case basis.

13. My information system's ATO expires in September 2017, do I submit under Risk Management Framework (RMF) or Certification and Accreditation (C&A) process? I'm getting conflicting answers from ISSPs.

Answer: Regardless of status, you should immediately begin planning to transition to RMF. Technically, you can submit under the C&A process depending on the system type. However, the Regional AO may only grant an ATO for a short period of time and you will have to do the RMF submission in the very near future.

14. What are the common mistakes ISSMs make when they submit an RMF package? Can we get a list of Top Mistakes?

Answer: The most common mistakes DSS ISSPs encounter when reviewing RMF packages are:

- Missing or inadequate control implementation language in the SSP
- Tailored out controls without justification
- Missing or incomplete supporting artifacts
- Improper system categorization and improper use of overlays
- Incomplete or inaccurate system configuration diagrams
- Submission of SSP in C&A format instead of RMF format
- Misjudging how much time is necessary to prepare the SSP and Body of Evidence (BOE) necessary for authorization
- Inadequate training and knowledge of RMF to build confidence in the process
- Not engaging early with the assigned ISSP
- Lack of familiarization with the DAAPM
- Inadequate system description

15. Do I have to add a registry entry for the network Security Technical Implementation Guide (STIG) check in order to pass the Security Content Automation Protocol (SCAP) scan even though this is a MUSA with no network connection?

Answer: If a vulnerability is deemed a false positive, it is not required to be resolved.
All vulnerabilities identified by the DSS ISSP during the technical assessment of a system will be reconciled with regards to applicability to the system type and contract requirements.

16. I have a plan submitted several months ago but have not received any status update from my ISSP. How do I escalate the issue appropriately?

Answer: The chain of command for ISSPs is Team Lead, Regional AO, and Regional Director. Please work through the chain of command to escalate issues.

17. What should our company do to speed up the RMF process in the case of a short turn-around proposal where we have to respond to the customer with a tight deadline?

Answer: In the "System Description" form field within OBMS, identify the system as a "Proposal System" to alert the ISSP. In the case of a proposal system, a limited ATO (e.g. 30-60 days) may be granted by the AO without the requirement for on-site validation.

18. During the transition from C&A to RMF, can I continue to process on my system?

Answer: Only if the system in question has a valid, unexpired ATO. Systems accredited under the C&A process are authorized to continue processing until the expiration of the currently issued ATO, unless a security-relevant change that would have necessitated re-accreditation occurs prior to ATO expiration.

19. What is the difference between the Assessment & Authorization (A&A) performed by the Industrial Security Representatives (ISR) and the A&A performed by the ISSP?

Answer: There are two definitions for the acronym "A&A" and they are not interchangeable. Both ISRs and ISSPs conduct a wide range of activities to oversee the protection of classified information and technologies in the hands of cleared industry. These activities include interactions with industry such as Advice and Assistance (A&A) actions, Security Vulnerability Assessments (SVAs), discoveries and inquiries on security violations, and oversight of industry's actions to mitigate vulnerabilities. ISSPs are primarily (and solely) responsible for the Assessment and Authorization (A&A) process which under Risk RMF replaces the term C&A. ISSP A&A actions are part of RMF Step 4, "Assess" and necessary to facilitate a recommendation for an authorization decision.

20. Have you seen a situation where the customer approved a RAR and the ISSP has problems with it?

Answer: The assigned ISSP will work with the customer and the DSS Regional AO to determine whether the RAR is sufficient.

21. How many customers need to approve the RAR? Is there reciprocity for RARs? Can a customer reject a RAR?

Answer: A requirement does not exist for customers to approve the RAR. The RAR is provided to the DSS AO. However, DSS will communicate with customers as appropriate to confirm their concurrence with the RAR as needed. The RAR is an integral part of the RMF A&A process. DSS adopted the National Institute of Standards and Technology (NIST) RMF as a common set of guidelines in order to streamline and build reciprocity into the DSS processes.

22. You said the ISSP should process the SSP within 30 days. But if the plan is sent back to the ISSM in OBMS does the clock reset?

Answer: Yes. The "clock" for DSS starts when the final, satisfactory SSP and supporting artifacts is submitted to DSS for authorization.

23. How are Memorandums of Understanding (MOUs) handled by DSS NAO? What is the proper way to submit an MOU for signature?

Answer: The NAO has provided a template for MOUs to facilitate connections between government and contractor systems. This template has the appropriate signature block and references, and will be the most up-to-date approved version. The template can be found in the ODAA Bulletin Board within OBMS, under "Headquarters Bulletin Board". Industry is not required to use the DSS template; however doing so may expedite the coordination and approval process. MOU's should be submitted for signature by the facility within OBMS, and forwarded within the OBMS application to their assigned ISSP for review.