RISK MANAGEMENT FRAMEWORK (RMF) – FREQUENTLY ASKED QUESTIONS (FAQ)

1. **When should Industry submit for reauthorizations?** Industry reauthorization submissions should be submitted 90 days before the current Authorization to Operate (ATO) expires.
   DSS personnel must: 1) Review the System Security Plan (SSP); 2) Conduct an assessment; 3) Allow for interaction with Industry for potential corrections/updates to submitted SSPs.
   Note: The DSS goal is to make authorization decisions within 30 days.
2. **Can Industry continue to operate systems after an ATO expires?** No. Once an ATO expires, Industry must cease processing on that system.
   If Industry submitted a complete reauthorization package 90 days prior to ATO expiration and DSS was unable to process the package due to workload, then DSS will determine if a short term (Limited) ATO may be issued. Communication between the Information System Security Manager (ISSM) and the local DSS Information Systems Security Professional (ISSP) is the key to successfully achieving an ATO reauthorization. Waiting until the day before an ATO expires to engage will ensure the process fails.
   A short term ATO is not automatic and will involve input from the local Regional Authorizing Official (AO) representatives. It is incumbent on Industry to submit a timely and complete reauthorization package.
3. **Is the ODAA Process Manual still effective?** No. As of January 1, 2018, the *Defense Security Service Assessment and Authorization Process Manual (DAAPM) Version 1.2* will be used for all classified systems seeking authorization and/or re-authorization.
4. **Are Data Transfer Agents (DTA) considered privileged users?** Yes. Privileged users include anyone who conducts data transfers, including low to high.
5. **Is Industry required to review classification guidance when completing Risk Assessment Reports (RAR) and Plan of Action and Milestones (POA&M)?** Yes. Vulnerabilities identified in the Risk Assessment Report and/or the POA&M are subject to the Security Classification Guide (SCG) for that program. SCGs are required for every program per NISPOM 4-103 and 7-102.
6. **Will DSS publish a new list of Security Relevant Objects (SROs)?** No. DSS will no longer publish a list of Security Relevant Objects (SROs) to be audited.
   The ISSM must work with the Information Owner (IO)/Information System Owner (ISO) to determine what files are most appropriate to audit in order to mitigate the specific threats and vulnerabilities unique to the system.
7. **Can audit correlation controls be manual?** Yes. Audit correlation controls can be manual; they are meant to be a discussion between different security entities to determine if there is a pattern of security violations and insider threat concerns. Examples: 1) A pattern of similar software failures can point to a need to roll back a security patch; 2) Security violations from one individual in different areas might be correlated with Human Resource (HR) records.
8. **In order to meet one of the security controls, the facility will follow an internal policy. Does the policy need to be uploaded in OBMS with the System Security Plan (SSP)?** Yes. The internal policy should be included with the SSP as an artifact with

specific page numbers and/or sections referenced. If your policy refers to an internal policy that is proprietary or is too large to include as an artifact, it must be available for review during an assessment visit.

9. **Can a facility create one policy that incorporates all the -1 controls?** Yes. Every security control family has a -1 control that requires a policy. It may be appropriate to roll all or some of the policies into a site IS Policy.
10. **What is the time period for audit retention?** Audit retention is for one year or one assessment cycle, whichever is longer.
    The SCG and other program requirements should be reviewed to determine how long audit information is required to be retained. Example: Audit logs for a system processing Top Secret data which supports a weapon system might require a 5 year retention period.
11. **Does a PL2 System exist within RMF?** No. Under RMF, ISs are now categorized based on the impact due to a loss of confidentiality (moderate/high), integrity (low/moderate/high), and availability (low/moderate/high) of the system according to information provided by the IO.
    DSS and the National Industrial Security Program Policy Advisory Committee (NISPPAC) has identified a categorization of M-L-L as the baseline absent information which would move it higher. With the transition to RMF, the facility is responsible for categorizing the system and selecting the controls that will address the requirements for Need To Know (NTK). ISSMs will then define the strategy for the affected controls within the individual control implementation justification, subject to ISSP and AO review.
12. **All Information Systems (IS) requiring authorization or reauthorization must use the DAAPM version 1.2 and the RMF process. However, the DAAPM does not have overlays for WAN systems. If Industry must use the RMF process for "all" ISs, what control guidance is required on non-isolated systems?** RMF requires the facility to categorize the system and select the applicable controls. A DSS Overlay will not be created for Wide Area Networks (WAN).
    An overlay was only created for Standalone Systems and Isolated LANs/Peer-to-Peer. Selecting security controls for WANs will start with the initial baseline (DAAPM Appendix A). The security controls listed in the initial baseline are not a minimum, but rather a proposed starting point from which controls may be removed or added based on tailoring. However, all controls must be addressed. Tailoring guidance is provided in DAAPM page 21 and NIST SP 800-53.
13. **Can Industry assume tailored-in controls that the DSS SCAs will require for DIBNet-S or SECRET IP Data Network nodes will be the same for all contractors who submit assessment packages to DSS for these 'WAN' systems?** No. All security controls must be addressed. RMF is not a one size fits all approach.
    Every facility has different operational security requirements based on the level of safeguarding required for the data processed. Since WANs do not have an overlay, you are not tailoring in additional controls. These controls are part of the baseline. As with all SSP packages, you will need to first conduct a risk assessment. Once you have conducted a thorough risk assessment and reviewed all contractual requirements, you will need to select the appropriate controls for the system. If controls from the baseline are

not selected, you will need to tailor out these controls and provide proper written justification.

14. **To fully comply with the spirit and intent of control CP-9 'Information System Backup', does the contractor have to perform a full backup of all software and data on the MUSA system weekly and record evidence they performed a weekly Continuous Monitoring (ConMon) audit to enable DSS to confirm this action has been executed weekly by the user, system administrator or ISSM of Record?** CP-9 requires the organization to conduct the following: (1) Backups of user-level information contained in the information system weekly; (2) Backups of system-level information contained in the information system weekly; (3) Backups of information system documentation including security-related documentation as required by system baseline configuration changes in accordance with the contingency plan (4) Protect the confidentiality, integrity, and availability of backup information at storage locations. System-level information includes system-state information, operating system and application software, and licenses.
    Backup plans should be developed for all systems and be included in your contingency planning policy. The backup plan should consider data loss risks. The areas of risk that should be identified and planned for include, but are not limited to: loss of power, loss of network connectivity, loss or corruption of data, and facility disruptions, such as loss of air conditioning, fire, flooding, etc.
15. **Does guidance and supporting policies exist for the classification of a system as a PIT (Platform Information Technology) versus an IS and a modified authorization process?** As detailed in the DAAPM Version 1.2 (Sections 6.1 and 6.2), the ISSM is required to define the system in the System Description section of the SSP. The ISSM will document the controls as appropriate for any system type. Controls that require tailoring out due to a lack of system capabilities will need to have documented justification(s) and/or mitigations within the SSP.
16. **Does DSS NAO believe Change Request (CRs) must be populated and pre-approved in writing by the ISSM for 1) all uploaded vendor 'patch' updates to operating system or business/security relevant software noted in the AO approved 'Software Listing' and 2) all anti-virus 'signature file' updates uploaded periodically to the Information System (IS)?** Facilities must operate in accordance with their Configuration Management Plan. The plan will detail the roles, responsibilities, policies, and procedures that are applicable when managing the configuration of products and systems. The ISSM is responsible for ensuring the policies and procedures are followed and that all additions, changes or modifications to hardware, software, or firmware are documented and that security relevant changes are appropriately coordinated. If the Configuration Management Plan requires a CR for vendor OS patches; then a CR is required. If the plan addresses vendor patches as a "weekly system maintenance activity," then a CR may not be required if this activity is captured in a Maintenance log or other similar tracking document.
17. **Since the implementation of a Diskless Computer is consistent regardless of make/model of system (i.e. any computer that does not have the ability to store/retain information), will DSS make this a third option to the SSP template (i.e. in addition to SUSA/MUSA and Isolated LAN/P2P) and tailor out the appropriate controls?** At this time, DSS will not create an overlay for Diskless Workstations. As

with all systems authorized under RMF, the correct balance of security commensurate with risk is found by using the tailoring process.

18. **What are the "security markings" required by DAAPM and control MP-3?** The contractor is required to follow both the NISPOM and DAAPM. The DAAPM is the manual that provides the "additional security controls."
    NISPOM 8-101 states: The contractor will maintain an ISs security program that incorporates a risk-based set of management, operational, and technical controls, consistent with guidelines established by the CSA.
    NISPOM 8-300 states: Additional security controls may be provided by the CSA to establish the baseline security control set required for each IS processing classified information.
    NISPOM 4-200 states: Physically marking classified information with appropriate classification markings serves to warn and inform holders of the information of the degree of protection required. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all classified information and material be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, the identity (by name and position or personal identifier) of the classifier, the source(s) for derivative classification, and any other notations required for protection of the information.
    NISPOM 8-302g.(1) states: Mark, label, and protect ISs media to the level of authorization until an appropriate classification review is conducted and resultant classification determination is made.
    The DAAPM (Appendix A) MP-3 Supplemental Guidance states that security markings refer "to the application/use of human readable security attributes."
19. **Does DAAPM MP-3 require volatile hardware component security markings to include CLASSIFIED BY, DERIVED FROM, and DECLASSIFY ON?** MP-3 marking requirements include "distribution limitations, handling caveats, and applicable security markings (if any) of the information." In addition, the NISPOM must be referenced for additional media marking information. It is important to note that the intent of the markings is to ensure that the classification of the item is clear to the holder (NISPOM 4-200) so that proper protection can be provided.
    DSS recognizes forms of media as special types of material generally containing multiple files and coming in all shapes and sizes, which makes marking and labeling more difficult than for individual documents. Such media often contain both unclassified and classified documents and may include multiple categories of information and/or handling caveats. Therefore, the highest classification of any classified item contained within the media (overall marking) along with any and all associated categories/caveats (e.g., CNWDI, NATO) will be conspicuously marked (stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device) on the exterior of such material (or, if such marking is not possible, on documentation that accompanies the media) so it is clear to the holder (NISPOM 4-203).
    If each document on a removable device contains all of the required information for that document, only the overall classification and associated caveats markings must be marked on the exterior of the device. Other notations such as names, addresses, subjects/titles, source of classification and declassification instructions are not necessary

on the exterior of removable media. Additionally, unclassified media and systems located in areas approved by the CSA for classified processing must also be marked and labeled so that the overall classification and associated caveats are apparent to the user.

20. **Is encryption of data at rest always required regardless of the type of system? Some ISSPs are stating that it is a requirement while others are not.** No. The ISSP should be looking at the threats and overall security posture of the facility. This requirement may be met using alternate controls or methods. Each situation and system must be evaluated separately. For example, if it is a laptop that does not travel or create media and is stored in a container when not in use, this control could be mitigated and acceptable by using the container as a means of controlling access to data.
21. **Are all POA&M items required to be closed out/completed prior to the system being granted an Authorization to Operate (ATO)?** No. POA&Ms are required when a control is not met. The ISSM must identify and mitigate any control that is not met or claimed as not being required. Open items do not prevent a system from being authorized. Some items may never be closed out, while others may be implemented at a later time. An example would be if the contractor system replicates or is supporting a fielded system that cannot be upgraded at the moment. Documentation should be provided detailing when the fielded item will be updated and that date reflected. The POA&M is reviewed under the continuous monitoring program.
22. **Is Industry required to shut down C&A accredited systems in order to transition to RMF?** No. C&A accredited systems may continue to operate during the transition process. If the ISSM has failed to submit a complete RMF SSP prior to the ATO expiration, the AO/ISSP will work with the facility and determine whether or not an extension to the current authorization may be issued to complete the RMF process.
23. **When can we expect to see the next update of the DAAPM?**
    NAO is in the process of releasing DAAPM 1.3 which will become effective on June 4, 2018. The DAAPM will be accessible from the http://www.dss.mil/rmf/ RMF Resource Center.