Janel L. Akande, MA

Brandywine, MD, 20613 holmesjl3@alumni.vcu.edu 804.334.0060

Application owners should consider the timeline, resources, and milestones required to categorize the various information types, register the system and enter data into eMASS, and assess the system for an ATO. Upon execution of a successful RMF and Cybersecurity Plan, the application owner will have obtained the appropriate accreditation under the RMF in the target environment.

Data and applications migrating to new hosting environments must be accredited under the RMF. Data and applications that are not currently accredited under the RMF (i.e., DIACAP accreditation or Tenant System Security Plan) must complete this as part of the migration effort. For capabilities that are accredited under RMF, capability owners must ensure that associated documentation is updated for acceptance in the target hosting environment including all cybersecurity controls and control enhancements updated for compliance status as provided by, and in the new hosting environment. These changes may require reassessment of the system and AO approval. The following are some considerations:

- Whether a capability is deemed a system or application, it will likely be considered a system once migrated from its origin environment to its target environment, requiring its own RMF ATO
- The AO may need to change if the current host AO is no longer applicable in the target environment
- The authorization package will need to be updated with the target environment's common/hybrid controls as well as system specific control status in the new hosting environment, and AO notification will need to occur regarding the significance of change to the system to determine what authorization is required
- Consider the timeline, resources, and milestones required to categorize the various information types, register the system and enter data into the eMASS, and assess the system for an ATO

The actions and considerations that should be included in the RMF are listed in the Execution section below. These actions are necessary to identify, document, and implement the respective security controls in the eMASS tool in accordance with the RMF as specified in the following documents:

Additional resources for capability owners developing a RMF and Cybersecurity Plan include:

- NETCOM eMASS Training
- NETCOM RMF Home: https://army.deps.mil/NETCOM/sites/RMF/SitePages/Home.aspx
- DoD RMF Knowledge Service: https://rmfks.osd.mil/rmf/Pages/default.aspx
- The capability AO and Information Assurance Manager (IAM) or Information System Security Manager (ISSM) should be a major resource/point of contact (POC) for developing the RMF and Cybersecurity Plan
- If the current authorization is for a system, the authorization boundary is unlikely to change and the capability owner's responsibilities will be generally the same in the target environment
- If the current authorization is for an application (e.g., a CoN/Assess Only), the authorization boundary will likely expand to that of a system and the capability owner's responsibilities will increase in the target environment

- NETCOM; Risk Management Framework: Assess or Assess and Authorize; Operational Tactics, Techniques, and Procedures (TTP); June 2016 https://army.deps.mil/NETCOM/sites/RMF/SitePages/TTPs.aspx