NISP ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (eMASS) – FREQUENTLY ASKED QUESTIONS (FAQ)

1. **I am trying to complete the eMASS Training on the RMF Knowledge Service portal. However, I am unsure of who my sponsor should be?** Users with an External Certificate Authority (ECA) must request sponsorship from the designated Information Systems Security Professional (ISSP) in order to access the DISA eMASS Computer Based Training (CBT) via the RMF Knowledge Service (KS). Refer to the NISP eMASS Training Access and Procedures Guide for Cleared Industry located on the NISP eMASS Information and Resource Center: https://www.dss.mil/ma/ctp/io/nao/rmf/ under the Training Tab.
2. **I submitted the required forms to the Defense Counterintelligence and Security Agency (DCSA) eMASS mailbox months ago, but my account has not been created. Can you provide a status?** The required forms are prerequisites for establishing your account. In order to complete the account request process and activate your account, you must access the eMASS instance and register your user profile. The registration instructions are posted on the eMASS Information and Resource Center: https://www.dss.mil/ma/ctp/io/nao/rmf/ under the Account Management Tab.
3. **I have an active eMASS account and recently received a new PKI/ECA certificate. How do I update my ECA credentials?** In the DISA eMASS User Guide (RMF User Guide) - Located on the eMASS Site (Click "Help"), it details the process for adding new credentials (Section 5.2 - ADD NEW CREDENTIALS TO AN EXISTING USER ACCOUNT). If you are still experiencing issues, reach out to the DCSA eMASS Mailbox: dss.quantico.dss.mbx.emass@mail.mil.
4. **I am trying to access the Risk Management Knowledge Service portal to take the eMASS Training, but I am receiving an access error.** DCSA does not own/manage the RMF Knowledge Service. If you are having application issues, you must contact the RMF Technical Inquiries Team at:
   osd.pentagon.dod-cio.mbx.support-rmfknowledgeservice@mail.mil
   The following information must be included with each help desk ticket submission:
   - Contact information
   - Domain: NIPR
   - Errors: What type of error? What does the error say? When do you receive the error? If possible, provide screenshots.
5. **My eMASS prerequisite forms were rejected because my SAAR form was incomplete/incorrect. How do I correct this issue?** Users must use the DCSA eMASS pre-populated DD2875 System Authorization Access Request (SAAR) form. For specific instructions on how to complete the SAAR form, use the Industry SAAR instructions guide located on the NISP eMASS Information and Resource Center: https://www.dss.mil/ma/ctp/io/nao/rmf/ under the Account Management Tab.
6. **I received notification from DCSA NAO that my forms were received. I have also registered my user profile in eMASS. How long will it take until my account is approved?** Once you have completed all prerequisites, please allow 3 to 5 days for account approval.

7. **I receive an error when accessing eMASS. How do I proceed?** The NISP eMASS application is owned by DISA. The DCSA NAO eMASS team are system administrators for container and account creation. If you are experiencing application issues, you must contact the DISA eMASS Help Desk:
   Email: disa.global.servicedesk.mbx.ma-ticket-request@mail.mil
   Commercial Phone: 1-(844)-347-2457 Options 1, 3
8. **I have completed my control review and I am ready to submit my package to my ISSP. How do I submit? I do not have permissions to initiate a workflow.** In order to submit a package for approval into the next stage of the Control Approval Chain (CAC) (CAC Role 2 - DCSA), you do not need to initiate a workflow. This is not required when submitting a package. Prior to Submitting for Review, Industry must ensure the following is complete:
   - Test Results, Implementation Plan, and System-Level Continuous Monitoring (SLCM) are entered for all Security Controls.
   - Risk Assessment is completed for all applicable Security Controls (Non-Compliant).

   Use the Bulk processing feature in eMASS to submit controls to the ISSP in the CAC-2 role for control validation. Bulk Processing can be accessed by clicking [Bulk Processing] on the Controls - Listing screen. Bulk processing has the following options: "Add Test Results," "Set as Not Applicable," "Submit for Review," "Validate," or "Skip Validation." You will select "Submit for Review." This is detailed in Section 10.1.3 of the DISA eMASS User Guide.
9. **Are Industry consultants allowed access into the eMASS application? If so, what forms are required and what roles are applicable?** In order for a consultant to gain access to the eMASS instance, the company's designated Information Systems Security Manager (ISSM) must have an active eMASS account for the CAGE Code being requested by the consultant. The requested role will be determined by the facility's designated ISSM/FSO.
   To request a NISP-eMASS account, cleared consultants must complete the following:
   - DISA eMASS Computer Based Training (CBT)
   - DISA Cyber Awareness Challenge (CAC) training
   - DCSA IO (pre-populated) System Authorization Access Request (SAAR) form
   - Submit all artifacts to DCSA NAO eMASS mailbox at: dss.quantico.dss.mbx.emass@mail.mil
   - Access NISP eMASS instance (https://nisp.emass.apps.mil) and register user profile.
10. **I have an eMASS account, but I need to request access to additional CAGE Codes and/or add a role to my account. What should I do?** In order to gain access to additional Cage Code containers, please resubmit your Industry SAAR and include the additional Cage Codes in Block 13. Please have the FSO from the additional Cage Codes sign the SAAR.
11. **Can I import the previous DAAPM 1.3 SSP Template into eMASS?** The previous DAAPM 1.3 SSP Template cannot be imported into eMASS. As stated in the NISP eMASS Job Aid (Located on the NISP eMASS Information and Resource Center: https://www.dss.mil/ma/ctp/io/nao/rmf/) and DISA eMASS User Guide (Accessed by

clicking the "Help" Tab in eMASS), users can apply a variety of actions against the Security Controls assigned to their Systems.

- Import/Export Test Results: Test Result Import/Export is a feature which allows users to export/import a System's Assessment Procedures (CCIs) and latest test results simultaneously utilizing a defined template. Test Result Import/Export provides flexibility to practitioners in situations where Security Control assessment activities may have already been performed outside of eMASS.
- Import/Export Control Information: Control Import/Export is a feature which allows users to import/export a System's Implementation Plan, DoD System-level Continuous Monitoring (SLCM) Strategy, and Risk Assessment information for selected Security Controls utilizing a defined Microsoft Excel template.
- Bulk Processing: Bulk processing is a feature which enables the user to assess or validate multiple Controls simultaneously. Bulk processing may be appropriate in situations where an ATO already exists under a different authorization scheme (e.g., OBMS), a RMF package was done manually outside of eMASS, or the System has been imported into eMASS. Bulk processing does not eliminate the need to test and validate each applicable RMF Control. Bulk processing provides flexibility to practitioners in situations where authorization activities may have already been performed outside of the system to track future Control assessments within eMASS.

12. **How can I delete a system entered into eMASS?** Systems can only be deleted by the DCSA NAO eMASS System Administrators. If you would like a system deleted, please send an email to the eMASS Mailbox (dss.quantico.dss.mbx.emass@mail.mil) with the System ID, System Name, and confirmation that you want the system permanently deleted.
13. **How can I confirm whether or not my system has been submitted to CAC Role 2 (DCSA)?** Industry users can use the "Report" feature. Create the following report: Reports > CAC History Report > Select the System Acronym from the drop down menu > Generate Report. This report provides the status of all controls within the Control Approval Chain.
14. **Which STIGs are required for DSCA authorized classified systems?** In order to streamline the onsite validation of a system, DCSA will use the DISA STIG, associated benchmark and STIG Viewer to assess the controls documented within the system security authorization package. Industry is not required to STIG their systems. However, they must identify their baseline standards within their system security authorization package (e.g. NIST, NSA, STIG). DCSA 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. If the system cannot be assessed use the specified scanning tools, Industry must document the justification and process for assessing the system in the system security authorization package. The assessment will then be conducted in accordance with the system security authorization package.

    The ISSP (SCA) and Authorizing Official with oversight of the system can utilize any STIG deemed applicable in their official assessment of the NISP system, however the compliance or non-compliance of each individual control must be validated against any STIG findings. There is no "requirement" for a specific set of STIGs to be implemented,

they serve as a benchmark from which the SCA's assessment of security controls can begin. All applicable security controls (according to the security categorization and risk assessment) must be addressed, and residual risk from vulnerabilities mitigated to the satisfaction of the Authorizing Official.

15. **Is Industry required to address all Control Correlation Identifiers (CCIs)?** Industry was never required to address them in the past. DCSA requires CCIs be addressed for each control. The previous DAAPM 1.3 DCSA SSP allowed a high level statement to address all aspects of the control (CCIs). The eMASS provides users with the ability to breakdown the security controls to address all aspects of control compliance separately. If an overall statement adequately demonstrates proper implementation/justification for all CCIs, it can be used in each of the CCI required fields. Work with your assigned ISSP in order to satisfy assessment requirements.
16. **Are my OBMS systems with a valid ATO going to be imported into eMASS?** No. In order to create an eMASS System Record for OBMS Systems with a valid Authorization to Operate (ATO), Industry users will complete the New System Registration process outlined in The NISP eMASS Job Aid (Located on the NISP eMASS Information and Resource Center: https://www.dss.mil/ma/ctp/io/nao/rmf/).
17. **What is required from Industry if a user with an active eMASS account leaves the company?** Industry is required to contact the DCSA NAO eMASS System Administrators immediately. It is the responsibility of Industry to properly maintain their eMASS Containers and inform DCSA of any changes in personnel status (i.e. termination, retirement, military deployment, etc.).
18. **My eMASS account deactivated due to inactivity. How to I reactivate my account?** If a user's eMASS account has been expired less than 90 days, the user will need to contact the DCSA NAO eMASS mailbox and request account reactivation. If a user's account has been expired for more than 90 days, the user is required to submit a new DD2875 SAAR form along with the required training completion certificates. Visit the NISP eMASS Information and Resource Center: https://www.dss.mil/ma/ctp/io/nao/rmf/.
19. **If a package was approved in OBMS and a user needs to register the valid authorized system in eMASS, are users required to answer all Security Control information?** If a package was authorized in OBMS and has a valid authorization, the user is required to complete the New System Registration in eMASS and upload the authorized Security Assessment Report (SAR), Authorization to Operate (ATO), and Plan of Action and Milestones (POA&M) in the Artifacts section. Control information will need to be addressed for reauthorization and/or administrative edits. Consult with the designated ISSP form more information.