NISP Enterprise Mission Assurance Support Service (eMASS) Job Aid

Date: **March 25, 2019** **Version 1.0**

Overview

Purpose	This job aid was designed to assist NISP eMASS users navigate eMASS. **The *DISA eMASS User Guide* is an essential document and MUST be referenced throughout the process.** The *DISA eMASS User Guide* can be accessed by selecting the "Help" tab at the top of the eMASS screen. Please select the "RMF User Guide".
Required Resources	DISA eMASS User Guide DISA eMASS User Guide for System Administrators Defense Security Service Assessment and Authorization Process Manual NISP eMASS Account Role Based Access as IAM

Table of Contents

1.0 SYSTEM REGISTRATION

Overview

The *New System Registration* process consists of four major steps in eMASS as follows:

- Step 1. System Information
- Step 2. Authorization Information
- Step 3. Roles
- Step 4. Review and Submit

Reference the *DISA eMASS User Guide* (New System Registration Section).

Actions

Login to NISP-eMASS**:** **https://emass-nisp.csd.disa.mil/.**

Locate the *Authorization Module Dashboard* on NISP-eMASS *Home* screen.

Click the [New System Registration] to open the *System Registration Module*.

Select the *Risk Management Framework (RMF) Policy* option.

Click [Next] in the lower right-hand corner to begin registering a new RMF System record.

Step 1: System Overview

Registration Type: Select **Assess and Authorize.**

System Name: Enter the System Name. *(Note: The System Name must follow the DSS guidance for NISP eMASS System Naming.)*

The DSS guidance for NISP eMASS System Naming is as follows:

1. Enter the assigned Cage Code.
2. Enter the System Type (SUSA, MUSA, ISOL, P2P, C2G, C2C, etc.).
3. Enter a unique value for System Name.
4. If applicable, enter the Interconnected Government System Name (e.g., SIPRNet, MDACNet, SDREN, JTIC, etc.)

(CAGE Code)-(System Type)-(System Name)-(Interconnected Network)

Example 1 – 12345-C2G-INFINITY STONE-SIPR

Example 2 – 12345-SUSA-GAUNTLET

System Acronym: Enter the System Acronym. *(Note: The System Acronym must follow the DSS guidance for NISP eMASS System Acronyms.)*

The DSS guidance for NISP eMASS System Acronyms is as follows:

1. Enter the assigned Cage Code.
2. If applicable, enter the Interconnected Government System Name (e.g., SIPRNet, MDACNet, SDREN, JTIC, etc.)
3. Enter a unique System Identifier Value.

(CAGE Code)-(Interconnected Network)-(System Identifier)

Example 1 – 12345-SIPR-00001
Example 2 – 12345-00001

Information System Owner: Select the applicable Cage Code/Field Office from the Drop Down Menu. *(Note: If the applicable Cage Code/Field Office does not appear, please inform the NAO eMASS Mailbox at: dss.quantico.dss.mbx.emass@mail.mil).*

Version/Release Number: Enter the System Version/Release number specific to the facility's version or system control conventions.

System Type: Select **IS Enclave**. *(Note: The DSS specific system types are not available options in eMASS. Thus, Industry must select IS Enclave in order to have the ability to select the applicable baselines/overlays when creating the system record.)*

Acquisition Category: Select **N/A**

System Life Cycle/Acquisition Phase: Select **Post-Full Rate Production/Deployment Decision (Operations & Support)**. *(Note: Industry must select Post-Full Rate Production/Deployment Decision (Operations & Support)).*

National Security System: Check National Security System

Financial Management System: Uncheck Financial Management System

Reciprocity System: Uncheck Reciprocity System

Reciprocity Exemption Justification: Enter **N/A**

System Description: Provide a narrative description of the system, its function, and uses. Indicate if the system is stand-alone and/or interconnected. In addition, enter Program/Contract information, including contract vehicle's expiration date.

DITPR ID: Enter **N/A**.

DoD IT Registration Number: Not a required field – **Leave blank**.

Click SAVE to proceed to the next step.

Step 2: Authorization Information

Security Plan Approval Status: User will select the authorization status of the System and corresponding assessment and authorization dates. The user will also have the option to indicate if the System has been approved outside of eMASS. If the user indicates the System has been previously approved, the "Security Plan Approval Status Date" field is required. If the System is registered with an "Authorization Status" of anything other than "Not Yet Authorized," then the "Authorization Date" and the "Assessment Date" fields are conditionally required fields.

The Drop Down Options are the following:

Not Yet Approved *(Initial System Registration/New System without authorization in OBMS/eMASS)*

- **Authorization Status**: Select **Not Yet Authorized**

- **Need Date**: Enter the Need Date**.** These dates are based on contractually driven time frames, time needed to respond to Broad Agency Announcements (BAAs), Request for Proposals (RFPs), Requests for Information (RFIs), Rough Orders of Magnitude (ROMs), white papers, and other solicitations from DoD customers.

- **RMF Activity**: Choice is based upon where the system is within the RMF Process. The following are the options from the Drop Down Menu:
    1. Initiate and plan cybersecurity Assessment Authorization *(Note: This should be selected for an initial registration/system.)*
    2. Implement and validate assigned security controls
    3. Make assessment determination and authorization decision
    4. Maintain ATO and conduct reviews
    5. Decommission *(Note: This should not be an option for an initial registration/system.)*

- **Terms/Conditions for Authorization**: Provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

Approved (*Existing ATO in OBMS/eMASS*)

- **Security Plan Approval Status Date**: Enter authorization date.

- **Authorization Status**: Select the applicable Authorization Status (Available Options: Authorization to Operate (ATO), Authorization to Operate w/ Conditions, Decommissioned, Denial of Authorization to Operate (DATO), Interim Authorization to Test (IATT), and Not Yet Authorized)

- **Assessment Completion Date:** Enter date assessment completed.

- **Authorization Termination Date:** Enter ATD.

- **RMF Activity**: Choice is based upon where the system is within the RMF Process. The following are the options from the Drop Down Menu:
    1. Initiate and plan cybersecurity Assessment Authorization
    2. Implement and validate assigned security controls
    3. Make assessment determination and authorization decision
    4. Maintain ATO and conduct reviews
    5. Decommission

- **Terms/Conditions for Authorization**: Provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

Denied (*Existing DATO in OBMS/eMASS*)

- **Security Plan Approval Status Date**: Enter date authorization issued.

- **Authorization Status**: Select the applicable Authorization Status (Available Options: Authorization to Operate (ATO), Authorization to Operate w/ Conditions, Decommissioned, Denial of Authorization to Operate (DATO), Interim Authorization to Test (IATT), and Not Yet Authorized)

- **RMF Activity**: Choice is based upon where the system is within the RMF Process. The following are the options from the Drop Down Menu:
    1. Initiate and plan cybersecurity Assessment Authorization
    2. Implement and validate assigned security controls
    3. Make assessment determination and authorization decision
    4. Maintain ATO and conduct reviews
    5. Decommission

- **Terms/Conditions for Authorization**: Provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

Click SAVE to proceed to the next step.

Step 3: Roles

Users will assign specific personnel to each role of the Package Approval Chain (PAC) and Control Approval Chain (CAC).

To assign a user to a specific role, drag the user's name from the *Available Users* list box to the *Assigned Users* list box or double-click on the user's name in the Available Users list box. Multiple personnel can be selected for each step.

Package Approval Chain: Personnel assigned to a role in the PAC will have responsibility for moving the system's RMF package through the Assessment and Authorization process. DSS users (e.g., ISSPs, TLs, and AOs) are assigned to the PAC.

At this point in time, Industry must know their assigned DSS Field Office. DSS Field Offices can be found on the DSS website.

- **SCA**: Select the applicable DSS Field Office in the *SCA Available Users* column and drag to the *Assigned Users* list box or double-click.

- **Team Lead**: Select the applicable DSS Field Office in the *Team Lead Available Users* column and drag to the *Assigned Users* list box or double-click.

- **Regional AO**: Select the applicable DSS Region in the *Regional AO Available Users* column and drag to the *Assigned Users* list box or double-click.

- **IAM**: The IAM Assigned Users list box will be pre-populated with the Industry eMASS user registering the system. Do not add additional Assigned Users. *(Note: This only applies to IAM under the PAC.)*

Control Approval Chain: Personnel assigned to a role in the CAC are responsible for assessing and validating Security Controls, adding and managing the System's POA&M, and adding Artifacts and scans. As a standard, Industry users are assigned to the CAC – 1 Role only. ISSPs are assigned to the CAC – 2 Role.

- **IAM**: Select the applicable users in the *IAM Available Users* column and drag to the *Assigned Users* list box or double-click.

- **SCA**: Select the applicable DSS Field Office in the *SCA Available Users* column and drag to the *Assigned Users* list box or double-click.

Click SAVE to proceed to the next step.

Step 4: Review & Submit

The final step in System registration allows the user to review the data and submit the System registration. This screen displays *System Information, Authorization Information, and Roles.* If corrections are needed, click on the System registration navigation menu on the left to return to the step.

Click [Submit System] to complete the registration. The newly created System will now be displayed in the list of available Systems.

2.0 SYSTEM INFORMATION

Overview

The *System* module enables the user to manage and update System information. At the top of the *System* screen is a series of links to take the user to specific modules for the System:

- **System – Dashboard**: Overview of high-level System information.

- **System – Details:** Ability to update System information populating the RMF Security Plan report.

- **System – Categorization:** Manage Overlays, manually tailor-in Security Controls, and a system's categorization.

- **Controls – Listing:** Access the assigned Security Controls, Control Information Import/Export, Test Result Import/Export, and Bulk Control Processing modules.

- **Controls – Implementation Plan:** Create a plan concerning the implementation of System's Security Controls and system-level Continuous Monitoring Plan (SLCM).

- **Controls – Risk Assessment:** Update information surrounding the risk of individual Security Controls along with recommendations for remediation/mitigation.

- **Assets:** Upload asset scan results to map findings to a System's Security Controls. View/Act on prioritized actions (Add Test Results, Open/Close POA&M Items) for Security Controls based on ingested scan results.

- **POA&M:** Add, modify, and delete POA&M Items. Access POA&M Import/Export module.

- **Artifacts**: Add, modify, and delete System and Control level artifacts.

- **Package:** Initiate the authorization workflow approval process, comment in the collaboration boards, view comments and System snapshots from past reviews within the *Historical Package Listing*, receive Security Plan Approval, POA&M Approval, Assess Only Approval (Assess Only System records), Change Request Approval (certain eMASS instances only), and Authorization Extensions.

- **Management:** Access to ATC (certain eMASS instances only), Personnel, Associations (Inheritance), System Migration, Workload Tasks, and Administration functions.

- **RMF/DIACAP Policy Toggle**: Toggle to view information associated with the RMF and DIACAP policy views.

Reference the *DISA eMASS User Guide* (System Information Section).

2.1 System – Details

Overview

Once the system is registered, the package creator (IAM) will build the system package. Under the *System* tab, select *Details*. The following subsections will display:

- System Information
- Authorization Information
- FISMA
- Business
- External Security Services

Some of the data will be pre-populated based on information entered during System Registration.

Reference the *DISA eMASS User Guide* (Details Section).

Actions

To enter all System information, select the *Details* sub-navigational tab within the *System* module.

To add information to a particular section, click [Edit].

ALL REQUIRED FIELDS (RED STARS) MUST BE COMPLETED. If all required fields are not complete, the package cannot be successfully submitted.

System Details – System Information

Click [Edit]. Add information not entered during System Registration.

The following information must be completed in the *System Information* subsection:

- **Registration Type:** Pre-populated from System Registration.
- **System Name:** Pre-populated from System Registration.
- **System Acronym:** Pre-populated from System Registration.
- **Information System Owner:** Pre-populated from System Registration.
- **Version/Release Number:** Pre-populated from System Registration.
- **System Type:** Pre-populated from System Registration.

- **National Security System:** Pre-populated from System Registration (Checked).
- **Financial Management System:** Pre-populated from System Registration (Unchecked).
- **Reciprocity System:** Pre-populated from System Registration (Checked).
- **Reciprocity Exemption Justification:** Pre-populated from System Registration (N/A).
- **Public Facing Component/Presence:** Select **No**.
- **COAMS System Affiliation:** If not applicable, leave blank.
- **System Description:** Pre-populated from System Registration.
- **DITPR ID:** Pre-populated from System Registration (N/A).
- **DoD IT Registration Number:** Pre-populated from System Registration (Blank).
- **DVS Site ID:** If not applicable, leave blank.
- **System User Categories:** Select applicable user categories. After checking the applicable user categories, enter relevant information.
- **Ports, Protocols, & Services Management (PPSM) Registry Number:** If applicable, enter PPSM Registry number. If not applicable, enter N/A.
- **System Authorization Boundary:** Provide a description of the System Authorization Boundary and attach supporting artifacts. *(Note: Only one artifact can be added here. If additional artifacts need to be uploaded, please see Section 2.6 – Artifacts.)*
- **Hardware/Software/Firmware:** Provide details and attach supporting artifacts (e.g., hardware baseline, software baseline, etc.). *(Note: Only one artifact can be added here. If additional artifacts need to be uploaded, please see Section 2.6 – Artifacts.)*

- **System Enterprise and Information Security Architecture:** Describe system architecture and attach supporting artifacts. *(Note: Only one artifact can be added here. If additional artifacts need to be uploaded, please see Section 2.6 – Artifacts.)*

- **Information Flow/Paths:** Describe information flow/paths and attach supporting artifacts. *(Note: Only one artifact can be added here. If additional artifacts need to be uploaded, please see Section 2.6 – Artifacts.)*

- **Network Connection Rules:** Describe Network Connection Rules. If not applicable, enter N/A.

- **Interconnected Information Systems and Identifiers:** Enter Interconnected Information Systems and Identifiers. If not applicable, enter N/A.

- **Encryption Techniques:** Enter Encryption Techniques.

- **Cryptographic Key Management Information:** Enter Cryptographic Key Management Information.

- **System Location:** Select applicable location type *(Single or Multiple).*

- **Type Authorization:** Select applicable choice *(Yes or No).*

- **Deployment Locations:** Select applicable deployment location *(Options: (1) Cleared Contractor Facility – Mobility Plan must be attached, (2) Government Site – Mobility Plan must be attached, (3) Both Cleared Contractor Facility & Government Site – Mobility Plan must be attached, and (4) Not Applicable – System and/or components are not mobile).*

- **Baseline Location:** If the user assigns only one deployment location to the System, then "Baseline Location" is NOT a required field.

- **Physical Location:** Enter Installation Name and Physical Location information.

Click SAVE to complete.

System Details – Authorization Information	Select *Authorization Information* on Left Hand Side Menu. This data will be pre-populated based on information entered during System Registration. Validate Authorization Information. If updates are needed, Click [Edit]. *Click SAVE to complete.*
System Details – FISMA	Select *FISMA* on Left Hand Side Menu. Click [Edit]**.** **This section is NOT APPLICABLE.** However, user must select **NO** for all Drop Down Menu options. *Click SAVE to complete.*
System Details – Business	Select *Business* on Left Hand Side Menu. Click [Edit]**.** The following information must be completed in the *Business* subsection: • **Mission Criticality:** Choose applicable mission criticality. Verify criticality via IO documentation/guidance. • **Governing Mission Area:** Choose applicable Governing Mission Area. Verify mission area with IO. • **DoD Component:** OSD is pre-populated. • **Acquisition Category:** Pre-populated from System Registration (N/A). • **System Life Cycle/Acquisition Phase:** Pre-populated from System Registration. *(Note: Industry must select Post-Full Rate Production/Deployment Decision (Operations & Support) during System Registration.)* • **Software Category:** Enter applicable Software Category.

- **System Ownership/Controlled:** Select the applicable option.

- **Other Information:** If applicable, enter additional information. If not applicable, leave blank.

- **Cybersecurity Service Provider:** If applicable, select appropriate Cybersecurity Service Provider. If not applicable, leave blank.

Click SAVE to complete.

System Details – External Security Services

Select *External Security Services* on Left Hand Side Menu.

Click [Edit].

The following information must be completed in the *External Security Services* subsection:

- **External Security Services:** Provide the security service name and identify the provider. These are security services provided by external sources (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, CSSP, and/or supply chain arrangements.) If not applicable, enter N/A.

- **Services Description:** List all of the security services provided by external providers, include specific source (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, CSSP, and / or supply chain arrangements.) If not applicable, enter N/A.

- **Security Requirements Description:** Describe how the external services are protected in accordance with the security requirements of the organization. If not applicable, enter N/A.

- **Risk Determination:** Document that the necessary assurances have been obtained stating the risk to organizational operations and assets, individuals, other organizations, and the nation arising from the use of the external services is accessible. Is the external provider compliant with federal laws, or is the external service provider under contract to provide a security level commensurate with the system's security categorization. If not applicable, enter N/A.

Click SAVE to complete.

2.2 Categorization

Overview

Until the System's Categorization is completed with the identified appropriate Control Attributes, the System will not have Security Controls. The following subsections must be completed:

- Control Selection
- Overlays
- Manage Security Controls

Reference the *DISA eMASS User Guide* (Categorization Section).

Actions

To manage the System's Control Set, navigate to the *Categorization* sub-navigational tab within the *System* module.

ALL REQUIRED FIELDS (RED STARS) MUST BE COMPLETED. If all required fields are not complete, the package cannot be successfully submitted.

Categorization – Control Selection

In the *Control Selection* module, the user will have the ability to search for and associate NIST SP 800-60 Information Types with the System record to receive an overall recommended System security categorization.

The following information must be completed in the *Control Section* subsection:

- **Applied Information Types:** Select [Edit Information Types]. From the *Information Types* page, users can search for Information Types by using the drop-down or text field in the top left section. Once the user has entered in search data, click [Search]. Information Types may be searched by "Information Type Category," or "Information Type Name." All applicable Information Types will be listed in the *Search Results* section. Add individual Information Types by clicking the green [+] button to the right of the result. Additionally, the user can click [Add Visible] to select all search results.
    - Selected Information Types: The *Selected Information Types* will be shown. Use the dropdown menus to select the applicable Confidentiality, Integrity, and Availability (C-I-A) for each Information Type. *(Note: eMASS will automatically populate the recommended C-I-A levels for some of the*

Information Type as established by NIST SP 800-60 Vol. 2. Please update C-I-A based on Risk Assessment results.)

Click Save to Complete.

- **Primary Security Control Set:** Select [Edit Control Selection]. Select latest version of NIST SP 800-53 from the dropdown menu.
  - Control Attributes: Enter Confidentiality-Integrity-Availability (C-I-A) and Impact (Recommended: Moderate).
  - Information Type Evidence: Upload evidence on how categorization of the system was determined (e.g., RAR).
  - Rationale for Categorization: NISP will be entered if the system has been categorized at the Moderate-Low-Low (M-L-L) level. Justification needs to be provided for anything other than M-L-L.
  - Additional Authorization Requirements: Identify any additional authorization requirements beyond the A&A process (e.g., privacy, special access requirements, cross security domain solutions, Non Classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), or GIG CAP identifier, ports, protocols, and services management.)
  - Additional Control Sets**:** Not Applicable.
  - Re-baseline Controls**:** Save Control Set Information will be checked. Re-saving the control sets will re-baseline all controls.
  - Click [Save]. The Confirm Control Changes screen will appear.
  - Review the Security Controls and scroll down to the bottom of the page.

Click SAVE to complete.

Categorization – Overlays

Select *Overlays* on Left Hand Side Menu.

In the *Overlays* section, the user has the opportunity to apply Overlays to a System's Baseline Control Set to address unique security requirements. The following Overlays are available for application within eMASS:

- DSS Baseline (M-L-L)
- SUSA
- MUSA
- ISOL-P2P

- Classified Information *(Note: If one of the above DSS Overlays are applied, this Overlay is NOT required. This Overlay will be selected if the Categorization is above M-L-L and the system is not a SUSA, MUSA, or ISOL-P2P.)*

IMPORTANT: In order to apply the SUSA, MUSA, or ISOL-P2P Overlay, you must ALSO apply the DSS Baseline (M-L-L) Overlay.

To apply an available Overlay to a System's baseline Security Controls, select the hyperlinked [Overlay Name] within the *Overlays* section in *Categorization*.

Within the *Overlay* pop-up window, complete the questionnaire to determine if the Overlay will be applied to the System.

Click SAVE to complete.

If an Overlay is successfully applied to the System, the *Status* column will state "Applied."

Categorization – Manage Security Controls

Select *Manage Security Controls* on Left Hand Side Menu.

The Controls listed in the *Manage Security Controls* page will be directly associated with the selections that the user made in the *Control Selection* page. The *Manage Security Controls* page allows users to add additional (i.e., tailor in) Controls to the System's Baseline Security Controls.

Click [Add Additional Controls] to open the *Add Additional Controls* screen. Conduct the following actions:

- Select Controls search for the desired Control to add to the System record's baseline Security Control Set by clicking [Search].
- Select the [+] button next to each Control that will be added to the System's Baseline Control Set.
- Provide justification for adding the Security Controls.
- Click [Apply]. The selected Controls will now be displayed.
- Review the Controls that will be included in the System's Baseline Security Control Set.

Click SAVE to complete.

2.3 Controls

Overview

Control Details within the Controls view displays all the Security Controls assigned to the System. Each Control lists the "Acronym," "Status," "Name," "Properties," and "Residual Risk Level." By default, all the Controls are grouped by Control Family, but each Control Family can be collapsed or expanded by clicking [expand all] or [expand] to display associated Security Controls. *Control – Listing* will default to display the last custom filters the user applied per System record.

Reference the *DISA eMASS User Guide* (Controls Section).

Controls – Listing

Select *Controls* on the Top Menu.

In order to filter Controls for a registered System, select one or many options in the *Control Filters* listing. Filter options include *NC and NA Controls missing POA&M Item, Exclude Inherited and Shared Controls, Residual Risk Level, Control Status, Control Family, Control Property,* and *Control Criticality Rating*. Users can reset the selected filters by clicking [Reset Filter].

Control Actions: Users can apply a variety of actions against the Security Controls assigned to their Systems at either an individual level or in bulk.

- **Import/Export Test Results**: Test Result Import/Export is a feature of eMASS 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 of eMASS 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 of eMASS 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 eMASS and to track future Control assessments within eMASS.

Security Control Testing and Validation: Validating Security Controls within eMASS is a three-step process: (1) All of the Assessment Procedures (APs) assigned to a Security Control must be tested and the results must be recorded as test results. (2) The package is reviewed and submitted by the first role in the CAC (Industry). (3) The package is reviewed and validated by the last role in the CAC (DSS).

- **Individual Test Results**: Users can add individual test result to an Assessment Procedure (AP) by navigating to the *Assessment Procedures Details* screen.
    - From the *Control Details* page on the *System Main – Controls* view, click the [+] sign next to the desired Control and the view will expand to show all the APs for the Control. Click on the desired AP to display the *Assessment Procedures Details* screen.
    - At the top and bottom of the page are navigation tabs that allow the user to move to the previous or next AP. The dropdown menu in the center allows the user to move to other APs within the same Control.
    - The left side of the display provides information on how to test the AP and what the result of the test should be (derived from the RMF Knowledge Service).
    - Within the *Artifact and POA&M Items* table, users can view existing and add new AP-level artifacts and POA&M Items.
    - The section on the right side of the screen is where test results are recorded.

- **Multiple Test Results**: User can add test results to all APs of a particular Control from a single view by navigating to the *Control Details* view.
    - From *Control Details* on the *System Main* screen, click the desired [Control Acronym] to navigate to the *Control Details* view. Each Security Control AP is displayed within the *Assessment Procedure List*.
    - Users have the option to [Enter Test Results] for an individual AP or click [Expand All APs] to enter multiple test results simultaneously.

  - The left side of the display provides information on how to test the AP and what the result of the test should be (derived from the RMF Knowledge Service).
  - Within the *Artifact and POA&M Items* table, users can view existing and add new AP-level artifacts and POA&M Items.
  - The section on the right side of the screen is where test results are recorded.

- **Test Results Fields**: Test results consist of four required fields.
  - **Status:** "Compliant," "Not Applicable," or "Non-Compliant"
  - **Test Date:** The default date is today's date, but can be changed to any date in the past.
  - **Tested By:** The default value is the person entering the AP test results, but the value can be edited to enter a different name. This is useful if the actual test was conducted by someone other than the person entering the data.
  - **Test Results:** Provide a summary of and a justification for any findings encountered during testing.

- **"Not Applicable" Security Control:** If it is deemed that a baseline Security Control is Not Applicable (NA), the user can set the Control as "Not Applicable" from the *Control Information and Actions* section on the *Control Details* page.
  - If "Not Applicable" is selected from the dropdown menu, a comment box appears. The "Comments" text field is mandatory and is used to provide justification for this status.
  - Enter comments and click [Save].

Organizational Values from Control Details: In order to view the organizational specific Assignment Values for Security Controls set by DSS, navigate to the *Control Details* view. From *Control Details* on the *System Main* screen, click the desired [Control Acronym] to navigate to the *Control Details* view.

- Select the [Assignment Value] hyperlink to view Assignment Values that were set for each specific parameter within the Security Control text.

- The Assignment Values Information tooltip will appear. Select Assignment Values assigned from [NISP] to view within the Security Control text.

- The NISP Assignment Value will now be displayed within the Security Control text.

Users are required to reference the DAAPM Appendix A for Security Control implementation requirements, organizational values, supplemental guidance, as well as DSS specific guidelines.

Controls – Implementation Plan

Select *Implementation Plan* on the Top Menu.

The *Implementation Plan* sub-navigational tab displays *Assigned Security Controls* and lists the following information: *Control Acronym, Implementation Status, Security Control Designation, Responsible Entities, and Estimated Completion Date*. The information here populates the *Implementation Plan* and *DoD System-level Continuous Monitoring (SLCM) Strategy*.

To edit the Implementation Plan, select the Control(s) to edit in the "Select Visible" column and click [Edit Selected]. To edit the implementation plan for all Controls, place a check in the checkbox located in the "Select Visible" column header and click [Edit Selected]. Once the user clicks [Edit Selected], the *Edit Implementation Plan* screen will display.

The following information must be completed in the Implementation Plan:

- **Implementation Status:** Select Applicable Option.
- **Security Control Designation**: Select Applicable Option.
- **Estimated Completion Date:** Enter projected completion.
- **Responsible Entities**: Personnel responsible for implementing each Control.

System-Level Continuous Monitoring (SLCM) Strategy (a/k/a Continuous Monitoring Strategy)

- **Criticality**: Indicate the criticality of monitoring the Control as Red, Yellow, or White. *(Note: The DoD Continual Reauthorization Working Group (CRWG) Criticality Ratings (Red, Yellow, and White) are associated with Security Controls (NIST SP 800-53 Priority 1 = Red, NIST SP 800-53 Priority 2 = Yellow, and NIST SP 800-53 Priority 3 = White). Control Criticality Rating is annotated for each control on the Control Listing page. Security Controls identified with a Red or Yellow Criticality icon contain*

rationale surrounding the actions that need to be taken when assessed and validated as Non-Compliant. Please reference the Control Statuses Section of the DISA eMASS User Guide.)

- **Frequency**: Indicate the frequency with which the Control is monitored.
- **Method**: Indicate the method of monitoring the Control.
- **Reporting**: Provide a short narrative explaining who reports what to whom by when.
- **Tracking**: Provide a short narrative explaining how Security Controls found to be non-compliant or ineffective will be tracked.
- **SLCM Comments**: Provide a short narrative further explaining any other details not appropriate for the other fields.

Implementation Plan information must be complete prior to Submitting for Review.

Reference the *DISA eMASS User Guide* (Implementation Section).

Controls – Risk Assessment

Select *Risk Assessment* on the Top Menu.

The *Risk Assessment* sub-navigational tab displays the *Risk Assessment Summary* and the *Security Control Distributions*. The information here populates the Security Assessment Report (SAR).

Threat Source Assessments: Allows for assessments of a System's exposure and associated risk to specific threat sources that are formally identified by the Organization. Threat sources that are determined to be applicable can be evaluated for overall likelihood, impact, and risk level.

Control Details/Threat Risk Assessment: Organizations can map threat sources to the NIST SP 800-53 Security Controls to provide additional information when conducting Control assessments. If an organizationally-defined threat source has been mapped to a Security Control, users have the ability to document the threat risks directly from the *Control Details* page. On *Control Details*, click on the hyperlinked threat source name to produce an identical pop-up as in the *Risk Assessment* tab.

Risk Assessment Summary: Allows the user to document the assessed risk for the System's Security Controls. The *Security Control Distributions*

section displays risk assessment information surrounding the number of Non-Compliant Controls per Residual Risk Level and number of Non-Compliant Controls per Severity.

Risk Assessment Information: Users have the ability to enter risk assessment information from the *Control Details* page.

- On *Control Details*, click [View/Edit].
- The *Edit Risk Assessment Information* pop-up displays.
- Users can populate/edit the same Control risk fields as the *Risk Assessment Summary* (adjusting a value in one location will be automatically reflected in the other.) As such, the same auto-calculations and recommended value displays for the "Likelihood" and "Residual Risk Level' fields are applied to the *Edit Risk Assessment Information* pop-up.
- Enter information and click [Save].

Risk Assessment information must be completed prior to Submitting for Review.

Reference the *DISA eMASS User Guide* (Risk Assessment Section).

Controls – Submit for Review

Prior to Submitting for Review, Industry must ensure the following is complete:

- Test Results are entered for all Security Controls.
- Implementation Plan and Risk Assessment is completed for Security Controls.

Select *Control Details* on the Top Menu.

Industry/CAC – 1

- Once all of the APs assigned to a Control have been tested and test results have been applied, the Control is ready to move through the CAC in order to finally validate the Control.
- The active role (CAC – 1/Industry) in the CAC will be highlighted in blue and there will be a [Submit and add comments] button.
- Clicking [Submit and add comments] reveals a Comments box.

- Fill out the optional comments box and click [Submit].

- A Workload Task notification will be generated for the second role in the CAC (CAC – 2/ISSP).

ISSP/CAC – 2

- The assigned ISSP will log in to eMASS and go to the *Control Details* screen for the Control requiring validation.

- The CAC – 2 role will be highlighted in blue and an [Approve/Return] button will be listed.

- The ISSP has two options: (1) Add a test result before approving the Control or (2) Continue the approval process.
    1. Add a Test Result before approving the Control – If the ISSP adds a test result before approving the Control, the status of the Control will change from Compliant Unofficial (CUO), Non-Compliant Unofficial (NCUO), or Not Applicable Unofficial (NAUO) to Compliant Validated (CV), Non-Compliant Validated (NCV), or Not Applicable Validated (NAV). This feature allows the validator to retest and verify a submitted test result.
    2. Continue the approval process – The ISSP will click [Approve/Return]. This action will reveal the *Approve/Return* screen. The ISSP has two options: "Approve" or "Return for Rework." "Return for Rework" returns the Control back to the CAC – 1/Industry. Both options require the ISSP to complete the "Comments" text field. Once saved, the Control is given a final validation status of Compliant Official (CO), Non-Compliant Unofficial (NCO), or Not Applicable Official (NAO).

DO NOT SKIP VALIDATION UNLESS AUTHORIZED BY YOUR ISSP/AO

Reference the *DISA eMASS User Guide* (Security Control Testing and Validation Section).

2.4 Assets

Overview

The Assets module provides users the ability to manually document their System's hardware and software components of their Systems and increased visibility of the System's security posture by mapping asset scan results to Security Controls.

THIS SECTION WILL NOT BE USED.

Reference the *DISA eMASS User Guide* (Assets Section).

2.5 Plan of Action and Milestones (POA&M)

Overview

eMASS provides the ability to create and edit POA&M Items, add additional milestones, review and modify the POA&M, provide the AO with risk assessments, and ensure transparency to corrective actions and mitigation efforts.

Reference the *DISA eMASS User Guide* (Plan of Action and Milestones Section).

Actions

Select *POA&M* on the Top Menu.

While a package is under review, all *POA&M Items* (both Control-level and System-level) existing at package creation will be locked in the live System POA&M. Users will be able to view the details of locked *POA&M Items* in the System POA&M, but will only be able to edit the risk analysis fields for a POA&M Item that is included within an active package.

Users are responsible for updating a POA&M "Completion Status" based on actions taken against a Control (e.g. Control status change).

The user can choose to view the *POA&M Items for Controls, APs, and System* table in a "Table View" or "Card View" format. Click the [Card View] hyperlink to toggle the table to Card View. The *POA&M Items for Controls, APs, and System* table will be displayed in the "Card View" format.

2.6 Artifacts

Overview

The user has the ability to upload artifacts into eMASS to support authorization activities. Artifacts can be documents, diagrams, Visio charts, spreadsheets, etc. These artifacts may be associated at the System level or the Control and/or AP level.

Reference the *DISA eMASS User Guide* (Artifacts Section).

Actions

Select *Artifacts* on the Top Menu.

Click [Artifacts] to open the Artifacts screen. If the user would like to add an artifact, click [Add Artifact] and the *Add Artifact* screen opens.

The following are the procedures for adding an artifact:

- First, search for the desired Control and/or AP that the artifact will be associated by clicking [Search]. Security Controls may be searched by "Control Family," "Control Acronym/Control Name," and "Include APs." If a user does not select "Include APs," only Controls will be returned in the search results.

- A list of Controls and/or APs will be displayed based off of the search criteria. Select the [+] button to associate an individual Security Control and/or AP to the artifact.

- Complete all required artifact information. The "Artifact Owner" field will only appear if the System has established a manual inheritance relationship. The optional "Artifact Expiration Date" allows for the tracking of any artifact that requires periodic reviews and updates.

- Enter the artifact information. The "Category" dropdown menu has the following choices:
    - Implementation Guidance: Specific guidance for implementation of the System.
    - Evidence: Artifacts that are related to the System, but not specifically guidance for that System's implementation.
    - Other: Digitally signed reports from packages.
    - Click [Browse] to select the location of the artifact to upload.
    - Click [Save] to complete the process of adding the artifact and to return to the Control Details screen.

Note: The maximum file size for downloading artifacts is 100 MB.

2.7 Package

Overview

DSS will submit packages through the Package Approval Chain (PAC) for review and approval. Each package type will be captured and tracked historically within the Historical Package Listing for a System record. The following package types are available for submission into the PAC:

- Assess and Authorize
- Authorization Extension
- POA&M Approval

- Security Plan Approval

Note: Industry will not have a role in the PAC. Industry completes the package in the CAC.

Reference the *DISA eMASS User Guide* (Package Section).

Actions

PAC users will select *Package* on the Top Menu.

Package Workflow: PAC users have the ability to "initiate" a workflow to the 1st role of the PAC. Once a workflow is initiated at by a member of the PAC, the progress of all Systems can be tracked at each step in the RMF workflow. Within the workflow, Collaboration Boards facilitate communication between System personnel.

- To initiate a workflow and create a new package, navigate to the *Package Status* tab located within the *Package* main tab.
- Choose the workflow type that will be submitted into the PAC.
- On the *Create New* page, enter a unique "Package Name" and enter optional "Comments." Click [Initiate Workflow] to initiate the Workflow.
- A confirmation message will appear stating that the workflow was successfully initiated.
- PAC users will now be able to use the Collaboration Boards to comment/collaborate and upload artifacts as the package is processed through the workflow.

Package Submission: From the *Package Status* page, users with the PAC – 1 role may submit the initiated package.

- The active role is highlighted in dark blue in the PAC bar and a user with that highlighted role will have the ability to act on the workflow.
- Select [Submit] from the "Action" dropdown, enter in required "Comments" and click [Submit] to submit the package to the next role.

Updates to System: PAC users reviewing a package can view updates made to the live System since the package was submitted into the PAC.

- Click [Updates to System] from the *Package Status* screen.

- The *Updates to Current System* pop-up window will display a count of POA&M Items (grouped by Completion Status) that have been added to the live System since package creation.

- To view any changes to Control compliance status since package creation, click the [Updated Controls] tab.

Package Review: PAC users reviewing a package can "Approve," "Disapprove and Move Forward," or "Return for Rework."

Package Status: The *Package Status* sub-tab of an active workflow displays information and notifications.

- The Package Progress Bar shows the location of the package in the approval chain and the elapsed time spent at the current and each previous package reviewing role.

- The "Assessment Recommendations" section shows any special artifacts and comments added by Package Reviewers.

- The "Collaboration Board" displays all actions performed by Package Reviewers and the date the action occurred. Additionally, it shows all user posts and replies since the workflow initiation.

- Package notifications will potentially display on the *Package Status* sub-tab depending on the information contained within the package or certain events in the live system. Package notifications can appear as yellow warnings (informational) or red warnings (package cannot proceed forward until the issue has been addressed).

Package Overview: *Package Overview* mimics the *Controls – Listing* page and displays information on the compliance status of Security Controls and allows the reviewer to drill down to view specific information on each Security Control. The *Package Control Summary* view can be expanded or collapsed simultaneously or by an individual Control Family.

Package Risk Assessment: *Risk Assessment* allows the reviewer to view and edit the package *Risk Assessment Summary*. Any changes made to the risk information in the package will be reflected in the live System *Risk Assessment*.

Package POA&M: Package *POA&M* allows the reviewer to view and to edit the package *POA&M* (risk analysis fields only). Any changes made here will be reflected in the live System *POA&M*.

- To add or modify a package POA&M Item's risk analysis fields, click the hyperlinked "Vulnerability Description" and then [Edit].

Package Categorization: The System's security categorization can be viewed in package *Categorization*. The package *Categorization* displays the overall categorization (Confidentiality, Integrity, and Availability values), applied Information Types, rationale for categorization, and any additional authorization requirements.

Package Artifacts: Artifacts attached to the package can be viewed in package *Artifacts*.

Package Reports: *Reports* associated with the active package can be viewed and downloaded in package *Reports*.

Return for Rework: Throughout the review and approval process, the PAC user has the option to return a package for rework.

- "Return for Rework" option is selected from the "Select Action" Drop Down Menu.
- Select the appropriate role in the Drop Down Menu.
- Provide comments, and click [Return for Rework].

Applying an Assessment Decision: For authorization package types, the DSS roles have the ability to assess the submitted package and provide the AO with authorization recommendations. When assessing the package, these roles can document an Executive Summary describing the overall System cybersecurity risk and can also recommend an Authorization Termination Date (ATD).

- After applying the assessment decision to the active package, the DSS PAC roles will automatically be taken to the package *Reports* view to apply a digital signature to the Security Assessment Report.

Applying an Authorization Decision: For authorization package types, the AO will be prompted to select the appropriate authorization decision for the System.

- Once an "Authorization Determination" for the package is selected, the "Authorization Date," "Terms/Conditions for Authorization,"

"Authorization Termination Date," and "ADD Classification" fields appear.

- The "ATD" field will display a list of pre-set dates based off the "Authorization Status" the user selected.
- Enter information to all required fields and select to **[Authorize]**.
- After applying the authorization decision to the active package, the AO will be automatically redirected to the package *Reports* view to apply a digital signature to the Security Plan Report and Authorization Decision Document.

Reference the *DISA eMASS User Guide* (Package Section).

2.8 Management

Overview

Inheritance identifies authorization boundaries and creates relationships (i.e. Parent/Child, Provider, or Co-System) between interconnected information Systems registered in eMASS, allowing for an establishment of System hierarchy or information management.

Users have the ability to establish an inheritance relationship wherein an individual Security Control/Assessment Procedure is provided from one or multiple Systems. When full inheritance is established, a receiving System will have visibility into all the test results, POA&M Items, and artifacts from the originating System(s). When hybrid inheritance is established, a receiving System will have visibility into the latest test results, POA&M Items, and artifacts from the providing System(s) but must still enter local assessments to that Control/AP. Users can manage any Common Control Provider relationships and System associations within the Associations Summary.

Reference the *DISA eMASS User Guide* (Management Section).

3.0 DECOMMISSIONED SYSTEMS

Overview

According to the RMF, the last phase of a System's life cycle is the Decommission phase. eMASS has several rules governing decommissioned Systems:

- Decommissioned Systems remain in the eMASS instance repository but no longer appear on any reports, metrics, or general System searches.

- New inheritance relationships cannot be requested with Systems that have an "Authorization Status" of 'Decommissioned.'
- Setting an "Authorization Status" as 'Decommissioned' will automatically update the "RMF Activity" field to 'Decommissioned.'
- Setting the "RMF Activity" field to "Decommissioned" will automatically update the "Authorization Status" to 'Decommissioned.'
- Systems of any Registration Type can be set to Decommissioned.

Reference the *DISA eMASS User Guide* (Decommissioned Systems Section).

Actions

The following procedures will be used to decommission a system:

- To decommission a registered System, navigate to *System Details* and then *Authorization Information*. Click [Edit].
- Set the RMF Activity dropdown menu to "Decommission." The Authorization Status and RMF Activity status will then change to "Decommission." Click [Save].
- The System will now be decommissioned in eMASS.

Decommissioned Systems remain in the eMASS instance repository but no longer appear on any reports, metrics, or general System searches.

4.0 REPORTS

Overview

Reports can be accessed from the eMASS tool bar or from the eMASS *Home* screen. The user can generate System and package reports from the *Reports* and *Package* tab respectively on the System Main screen.

Reference the *DISA eMASS User Guide* (Reports Section).

NISP eMASS Questions & Concerns	Contact the DSS Information Systems Security Professional (ISSP) assigned to your facility and/or the NAO eMASS Mailbox at: dss.quantico.dss.mbx.emass@mail.mil