National Industrial Security Program (NISP) Enterprise Mission Assurance Support Service (eMASS) Industry Operation Guide

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

National Industrial Security Program Authorization Office

Version 1.0

13 August 2019

TABLE OF CONTENTS

1 INTRODUCTION

1.1 BACKGROUND

The NISP Enterprise Mission Assurance Support Service (eMASS) Operation Guide 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."

1.2 RESOURCES

In addition to this operation guide, key resources include:

- DoD 5220.22-M Change-2, *National Industrial Security Program Operating Manual* (NISPOM);
- DISA eMASS User Guide;
- DISA eMASS User Guide for System Administrators;
- DCSA Assessment and Authorization Process Manual (DAAPM);
- NISP eMASS Account; and
- Role Based Access as IAM

2 ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE

2.1 OVERVIEW

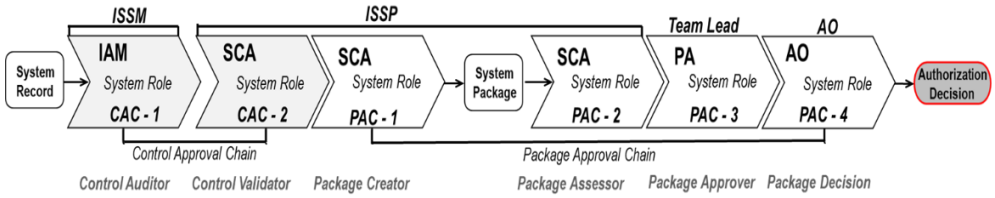
The Enterprise Mission Assurance Support Service (eMASS) is a government-owned, web-based application with a broad range of services for comprehensive fully integrated cybersecurity management. Features include dashboard reporting, controls scorecard measurement, and generation of a system security authorization package.

The Defense Information Systems Agency (DISA) manages eMASS's core functionality. DISA established an instance for Industry. The Industry eMASS instance is referred to as the National Industrial Security Program (NISP) eMASS instance. The DAAPM System Security Plan (SSP) templates will no longer be submitted via the ODAA Business Management System (OBMS) when requesting assessment and authorization of a classified system. The SSP is built in eMASS. All system security authorization packages must be submitted via the NISP eMASS instance at: https://nisp.emass.apps.mil/. Reference the NISP eMASS Information and Resource Center located on the DCSA Risk Management Framework (RMF) Web page.

The NISP eMASS instance is NOT APPROVED for storing classified information. If system artifacts, information, or vulnerabilities are classified per the Security Classification Guide (SCG), DO NOT enter this data into eMASS. Please follow guidance provided in this operation guide and contact the assigned Information System Security Professional (ISSP).

2.2 APPROVAL CHAINS

An approval chain is a series of users or user groups who must approve content before the deliverable can be finalized. When the last person in the chain approves the content, the deliverable is complete. The approval chain replicates the Risk Management Framework (RMF) process. The figure below provides an overview of the NISP eMASS Approval Chain from system record creation through authorization decision.



eMASS Approval Chain

Control Approval Chain (CAC): The primary vehicle through which the system security controls are approved and validated. eMASS privileges align with the system roles. As a standard, Industry users are assigned to the CAC – 1 Role. ISSPs are assigned to the CAC – 2 Role. Industry users have the following roles available in the CAC: IAM, Artifact Manager, and View Only. To register a system and edit security controls, Industry users must have the IAM role.

Package Approval Chain (PAC): The primary vehicle through which the system is assessed and authorized. DCSA users (e.g., ISSPs, Team Leads, and Authorizing Officials (AOs)) are assigned to the PAC.

Note: If the employment status of an employee changes (i.e., termination, retirement, etc.), the Facility Security Officer (FSO) or member of the Key Management Personnel (KMP) is responsible for notifying the DCSA NAO eMASS Team: dcsa.quantico.dcsa.mbx.emass@mail.mil.

3 SYSTEM REGISTRATION

The new system registration process consists of the following four major steps in eMASS:

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

Conduct the following actions:

1. Log in to NISP-eMASS: https://nisp.emass.apps.mil/;
2. Locate the Authorization Module Dashboard on NISP-eMASS Home screen;
3. Click the [New System Registration] to open the System Registration Module;
4. Select the Risk Management Framework (RMF) Policy option; and
5. Click [Next] in the lower right-hand corner to begin registering a new RMF System record.

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

Note: Systems with an ACTIVE Authorization to Operate (ATO) in the ODAA Business Management System (OBMS) are only required to complete New System Registration.

3.1 STEP 1 – SYSTEM INFORMATION

Registration Type: Select Assess and Authorize.

System Name: Enter the System Name.

The DCSA 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; and
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.

The DCSA 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.); and
3. Enter a System Name. *Note: The facility can choose how to best uniquely identify the system. It can be a unique name or number.*

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

Example 1 – 12345-SIPR-00001

Example 2 – 12345-00001

Information System Owner: Select the applicable Cage Code/Field Office from the drop-down menu. If the applicable Cage Code/Field Office does not appear, please inform the NAO eMASS Mailbox at: dcsa.quantico.dcsa.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 DCSA specific system types are not available options in eMASS. Thus, Industry must select IS Enclave 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).

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. Enter program/contract information, including contract vehicle's expiration date. The following details must also be included:

1. System Type (i.e., SUSA, MUSA, ISOL, C/S LAN, P2P, C2C, C2G, Unified WAN, eWAN);
2. Classification;
3. Categorization;
4. Formal Access Approvals;
5. CAVEATs;
6. Location (i.e., Closed Area, Restricted Area);
7. Type Authorization – List number of systems Type Authorized and include all System Acronyms;
8. Protected Distribution System (if applicable);
9. Operating System(s);
10. Mobility (if applicable); and
11. Interconnections (if applicable).

DITPR ID: Enter N/A.

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

Click SAVE to proceed to the next step.

3.2 STEP 2 – AUTHORIZATION INFORMATION

Security Plan Approval Status: Users will select the system's authorization status and corresponding assessment and authorization dates. Users also can 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:

1. 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), Requests for Proposals (RFPs), Requests for Information (RFIs), Rough Orders of Magnitude (ROMs), white papers, and other solicitations from Department of Defense (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:
     - Initiate and plan cybersecurity Assessment Authorization. Note: This should be selected for an initial registration/system);
     - Implement and validate assigned security controls;
     - Make assessment determination and authorization decision;
     - Maintain Authorization to Operate (ATO) and conduct reviews; and
     - Decommission. N*ote: 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 information system's operation or inherited controls that the system owner or common control provider must follow.

2. Approved (Valid Authorization to Operate (ATO) in OBMS/eMASS):

   - Security Plan Approval Status: 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. *Note: This date is located on the Security Assessment Report (SAR). If you are unable to locate this date, please use authorization date.*
   - Authorization Termination Date (ATD): Enter ATD.
   - RMF Activity: Choice is based upon where the system is within the RMF Process. Below are the options from the drop-down menu:
     - Initiate and plan cybersecurity Assessment Authorization. (Note: This should be selected for an initial registration/system.);
     - Implement and validate assigned security controls;
     - Make assessment determination and authorization decision;
     - Maintain ATO and conduct reviews; and
     - 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 information system's operation or inherited controls that the system owner or common control provider must follow.

3. Denied (Valid DATO in OBMS/eMASS):

- Security Plan Approval Status: 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 (Note: This date is located on the SAR. If you are unable to locate this date, please use authorization date).
- Authorization Termination Date (ATD): Enter ATD.
- RMF Activity: Choice is based upon where the system is within the RMF Process. Below are options from the drop-down menu:
  - Initiate and plan cybersecurity Assessment Authorization. (Note: This should be selected for an initial registration/system.);
  - Implement and validate assigned security controls;
  - Make assessment determination and authorization decision;
  - Maintain ATO and conduct reviews; and
  - 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 information system's operation or inherited controls that the system owner or common control provider must follow.

Click SAVE to proceed to the next step.

Note: Once the Authorization Information is entered and saved, it cannot be changed.

3.3 STEP 3 – ROLES

Users will assign specific personnel to each role of the PAC and 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. At this point in time, Industry must know their assigned DCSA Field Office. DCSA Field Offices can be found on the DCSA Web site.

Package Approval Chain: Personnel assigned to a role in the PAC are responsible for moving the system's RMF package through the Assessment and Authorization process. Conduct the following actions to assign users to the PAC:

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

2. Team Lead: Select the applicable DCSA Field Office in the Team Lead Available Users column and drag to the Assigned Users list box or double-click.
3. Regional AO: Select the applicable DCSA Region in the Regional AO Available Users column and drag to the Assigned Users list box or double-click.
4. IAM: The IAM Assigned Users list box will be prepopulated with the Industry eMASS user registering the system.

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. Conduct the following actions to assign users to the CAC:

1. IAM: Select the applicable users in the IAM Available Users column and drag to the Assigned Users list box or double-click. *Note: To allow other users within your container to view/edit the system package, add them here.*
2. SCA: Select the applicable DCSA 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.

3.4 STEP 4 – REVIEW & SUBMIT

The final step in the process 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.

Note: Systems with an ACTIVE ATO in the OBMS are only required to complete New System Registration. In addition to completing New System Registration, attach the following documents: Authorization to Operate (ATO), SAR, and Plan of Action and Milestones (POA&M). The documents will be added in the Artifacts section of eMASS. The next steps are for systems seeking authorization or re-authorization.

4 SYSTEM INFORMATION

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: Update system information populating the RMF Security Plan report.
- System – Categorization: Manage overlays and 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 (SLCM) Plan.
- 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. *Note: This section will NOT be used.*
- 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; and 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).

4.1 SYSTEM – DETAILS

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; and
- External Security Services.

Some of the data will be prepopulated based on information entered during System Registration. To enter all system information, select the Details sub-navigational tab within the system module. To add information to a particular section, click [Edit].

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

Reference the DISA eMASS User Guide (Details Section).

4.1.1 SYSTEM INFORMATION

Select System Information on the left-hand side menu. Click [Edit]. The following information must be completed in the System Information subsection:

Registration Type: Prepopulated from System Registration.

System Name: Prepopulated from System Registration.

System Acronym: Prepopulated from System Registration.

Information System Owner: Prepopulated from System Registration.

Version/Release Number: Prepopulated from System Registration.

System Type: Prepopulated from System Registration.

National Security System: Prepopulated from System Registration (Checked).

Financial Management System: Prepopulated from System Registration (Unchecked).

Reciprocity System: Prepopulated from System Registration (Checked).

Reciprocity Exemption Justification: Prepopulated from System Registration (N/A).

Public Facing Component/Presence: Select No.

COAMS System Affiliation: If not applicable, leave blank.

System Description: Prepopulated from System Registration.

DITPR ID: Prepopulated from System Registration (N/A).

DoD IT Registration Number: Prepopulated from System Registration (Blank).

DVS Site ID: If not applicable, leave blank.

System User Categories: Select applicable categories for the type of system users. The categories available are the following: Contractors, Coalition Partners, DoD Personnel, Fed/State/Local, Foreign Nationals, General Public, and Organization. More than one category can be selected. 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 use the Artifacts section.*

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 use the Artifacts section.*

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 use the Artifacts section.*

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 use the Artifacts section.*

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 used for information processing, transmission, and storage.

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). Industry Users will select Yes if they are using this system to Type Authorize identical copies of the system. If Industry Users are Type Authorizing identical systems, the following procedures must be followed:

1. Select the system being used to Type Authorize;
2. In the Artifacts section, upload the following for the system being Type Authorized:
    - Test Result Import/Export;
    - Hardware and Software Baselines ;
    - Facility/System Layout;
    - Record of Controlled Area (if applicable); and
    - Artifacts requested by the ISSP/AO.
3. In the System Description section (System>Details>System Information), update the Type Authorization information to include the number of systems Type Authorized and all System Acronyms.

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; and

Physical Location: Enter installation name and physical location information.

Click SAVE to complete.

4.1.2 AUTHORIZATION INFORMATION

Select Authorization Information on left-hand side menu. This data will be prepopulated based on information entered during System Registration. Validate Authorization Information.

Note: Once the Authorization Information is entered and saved, it cannot be changed.

4.1.3 FEDERAL INFORMATION SECURITY MANAGEMENT ACT (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.

4.1.4 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 Information Owner (IO) documentation/guidance;

Governing Mission Area: Choose applicable Governing Mission Area. Verify mission area with IO;

DoD Component: Office of the Secretary of Defense (OSD) is prepopulated;

Acquisition Category: Prepopulated from System Registration (N/A);

System Life Cycle/Acquisition Phase: Prepopulated 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; and

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

Click SAVE to complete.

4.1.5 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; and

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.

4.2 CATEGORIZATION

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:

1. Control Selection;
2. Overlays; and
3. Manage Security Controls.

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

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

Reference the DISA eMASS User Guide (Categorization Section).

4.2.1 CONTROL SECTION

In the Control Selection module, the user can 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 Selection 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 drop-down 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. However, the C-I-A must be based on the 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 drop-down menu.

1. Control Attributes: Enter Confidentiality-Integrity-Availability (C-I-A) and Impact (Recommended: Moderate);
2. Information Type Evidence: Upload evidence on how categorization of the system was determined (e.g., RAR);
3. 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;
4. 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 Global Information Grid (GIG) Connection Approval Process (CAP) identifier, ports, protocols, and services management.);
5. Additional Control Sets: Not Applicable;
6. Rebaseline Controls: Save Control Set Information will be checked. Resaving the control sets will rebaseline all controls;
7. Click [Save]. The Confirm Control Changes screen will appear; and
8. Review the security controls and scroll down to the bottom of the page.

Click SAVE to complete.

4.2.2 OVERLAYS

Select Overlays on left-hand side menu. In the Overlays section, the user can apply overlays to a system's baseline control set to address unique security requirements. The following overlays are available for application within eMASS:

1. DCSA Baseline (M-L-L);
2. SUSA (M-L-L);
3. MUSA (M-L-L);
4. ISOL-P2P (M-L-L); and
5. Classified Information (*Note: This Overlay will ONLY be selected if the Categorization is above M-L-L).*

To apply the SUSA, MUSA, or ISOL-P2P Overlay, users must ALSO apply the DCSA Baseline (M-L-L) Overlay. Once an overlay is applied, eMASS will retain the control information. If an overlay is applied in error, users cannot go back and rebaseline the controls. The user will need to delete the system and start again.

To apply an available overlay to a system's baseline security controls, conduct the following actions:

1. Select the hyperlinked [Overlay Name] within the Overlays section in Categorization;.
2. Within the Overlay pop-up window, complete the questionnaire to determine if the overlay will be applied to the system;
3. Click SAVE; and
4. If an overlay is successfully applied to the system, the Status column will state "Applied."

4.2.3 SECURITY TECHNICAL IMPLEMENTATION GUIDES

eMASS allows users to identify applicable DISA Security Technical Implementation Guides (STIGs) based on the technologies present within the system's authorization boundary.

THIS SECTION WILL NOT BE USED.

4.2.4 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:

1. Select Controls search for the desired control to add to the system record's baseline security control set by clicking [Search];
2. Select the [+] button next to each control that will be added to the system's baseline control set.
3. Provide justification for adding the security controls;
4. Click [Apply]. The selected controls will now be displayed;
5. Review the controls that will be included in the system's baseline security control set; and
6. Click SAVE.

4.3 CONTROLS

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).

4.3.1 LISTING

Select Controls on the top menu. To filter controls for a registered system, select one or many options in the Control Filters listing. Filter options include Non-Compliant (NC) and Not Applicable (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.

1. 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;
2. Import/Export Control Information: Control Import/Export is a feature of eMASS which allows users to import/export a system's Implementation Plan, SLCM Strategy, and Risk Assessment information for selected security controls using a defined Microsoft Excel template;
3. 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.
4. 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 drop-down 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; and
    - The section on the right side of the screen is where test results are recorded.
5. Multiple Test Results: Users 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; and
- The four required fields appear for each AP. Once all the fields have been completed, click [Save].

Test Results: Test results consist of the following required fields.

1. Status: "Compliant," "Not Applicable," or "Non-Compliant."
2. Test Date: The default date is today's date, but can be changed to any date in the past.
3. 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.
4. Test Results: The test results are required and used to document Industry's self-assessment of the security controls and provide confirmation that the security controls are applied and meet the security requirements for the system.

If annotating the non-compliance status of a Security Control is determined to be classified as per the SCG, mark the Security Control as "Not Applicable".

"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].

If System vulnerabilities are determined to be classified, the Control will be set as "Not Applicable". In the "Comments" field, indicate that details will be maintained on-site. Ensure ongoing communication is conducted with the assigned ISSP regarding the authorization package.

Organizational Values from Control Details: In order to view the organizational specific Assignment Values for security controls set by DCSA, navigate to the Control Details view. Conduct the following actions:

1. From Control Details on the System Main screen, click the desired [Control Acronym] to navigate to the Control Details view.
2. Select the [Assignment Value] hyperlink to view Assignment Values that were set for each specific parameter within the Security Control text.
3. The Assignment Values Information tooltip will appear. Select Assignment Values assigned from [NISP] to view within the Security Control text.
4. The NISP Assignment Value will now be displayed within the Security Control text.

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

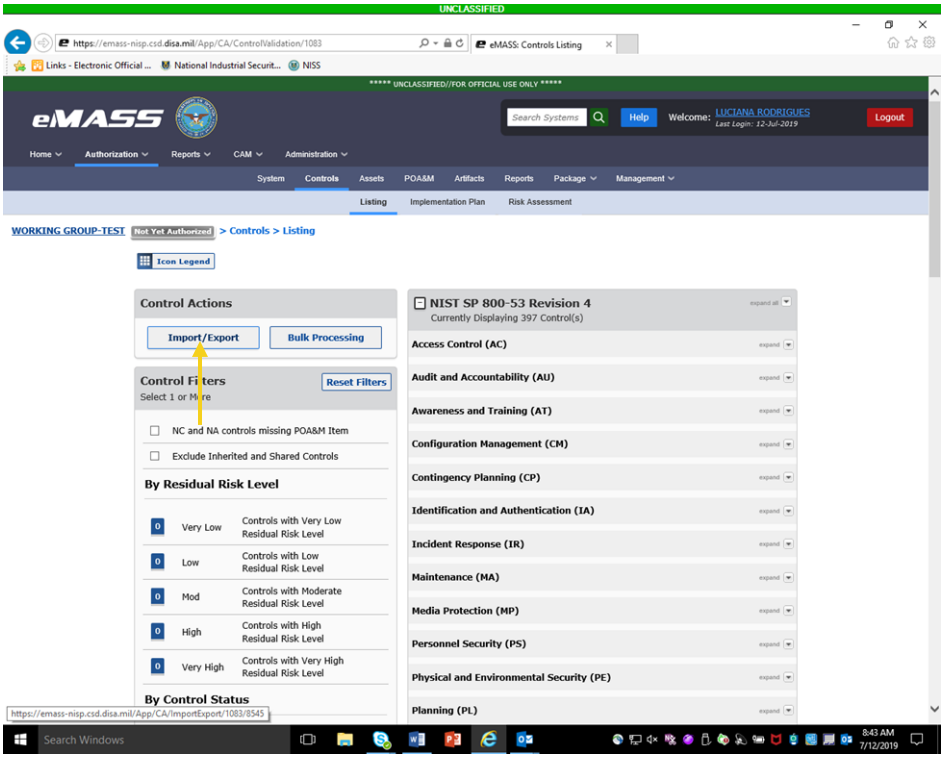
4.3.2 IMPORT/EXPORT

DCSA strongly recommends utilizing the Test Result Import/Export and Control Import/Export. Rather than addressing the test results, implementation plan, SLCM Strategy, and risk assessment for each control individually, the Test Result Import/Export and Control Import/Export feature allows users to address all system requirements within the eMASS generated templates.

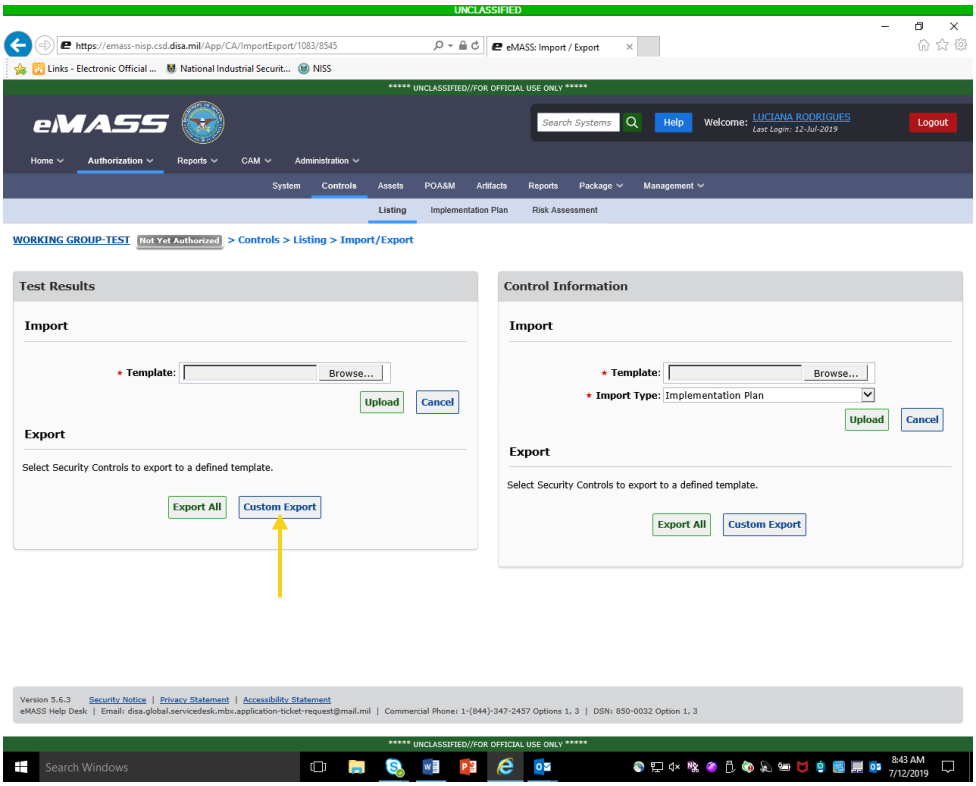
Note: Only eMASS generated templates can be imported.

Test Result Import/Export

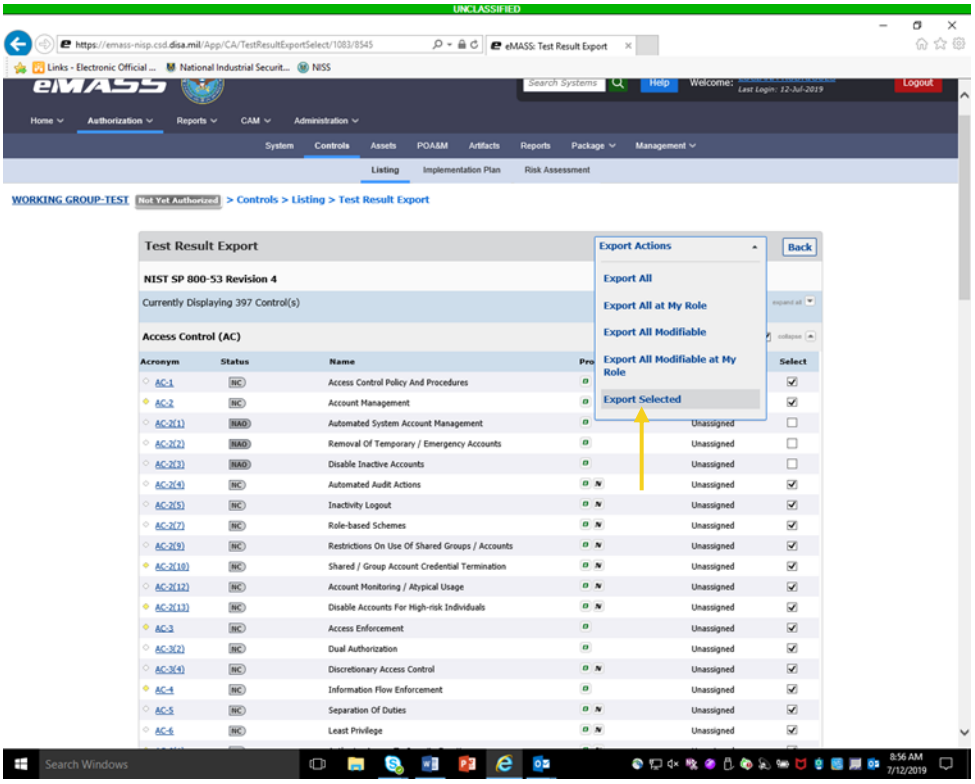
1. To begin the process, click [Import/Export] under Control Actions on Controls – Listing view.



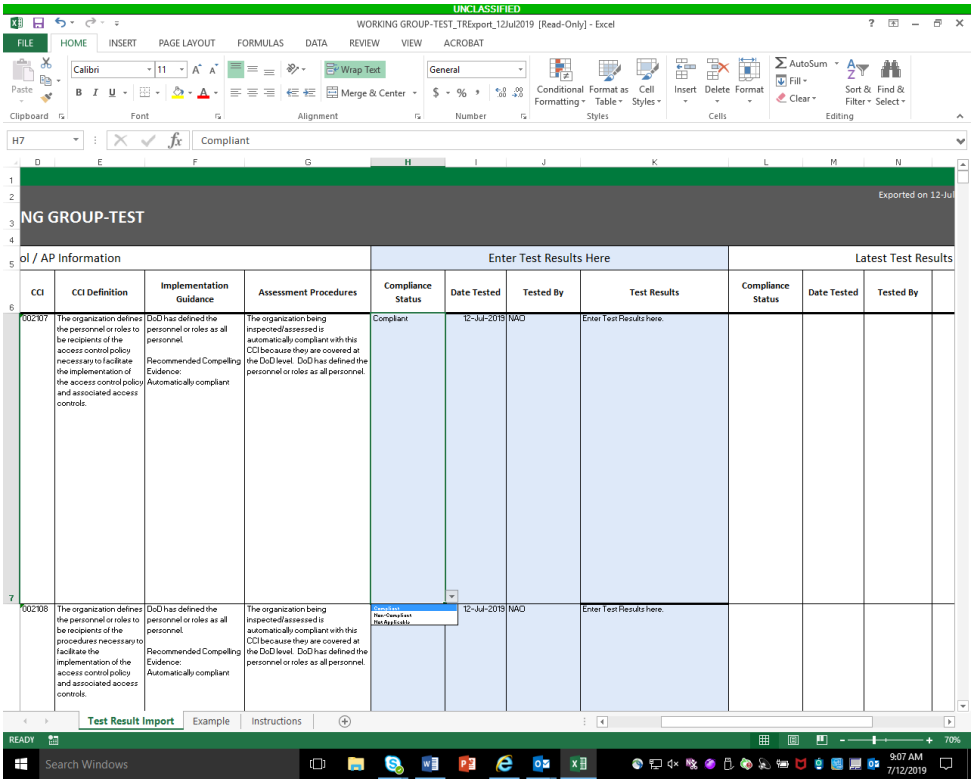
2. From the Import/Export home page, click [Custom Export]. Test Result Export allows users to export to a defined custom template.



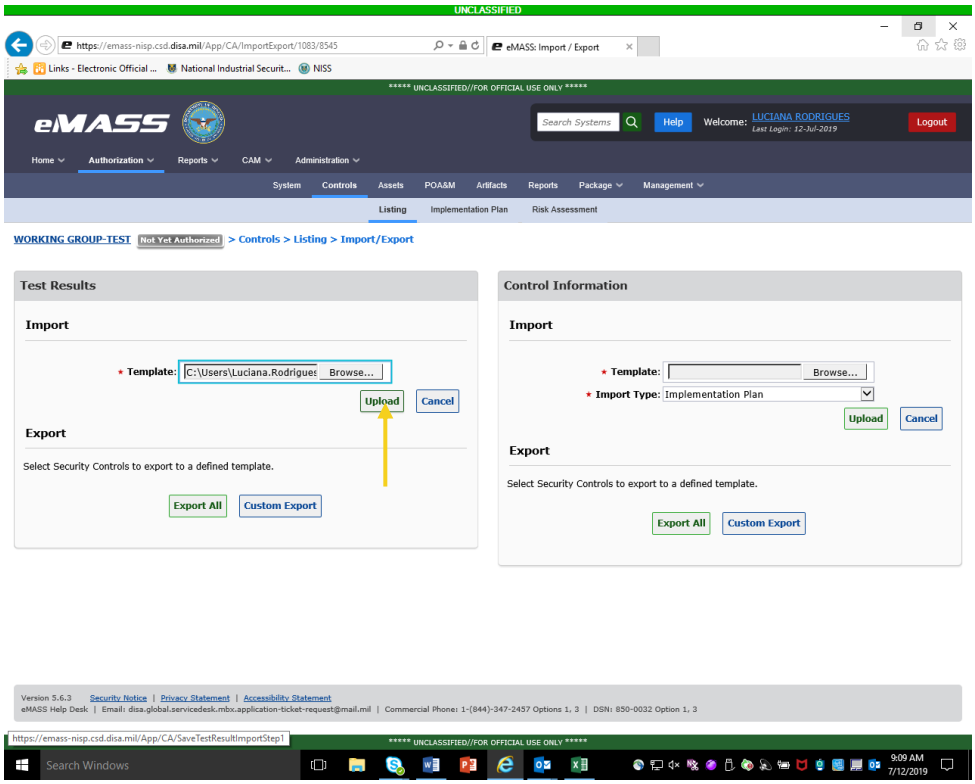
3. Place a checkmark in the checkbox of the security controls that will be exported. **Ensure that controls marked Not Applicable Official (NAO) due to application of an overlay are NOT selected.** Select [Export Selected] from the drop down.



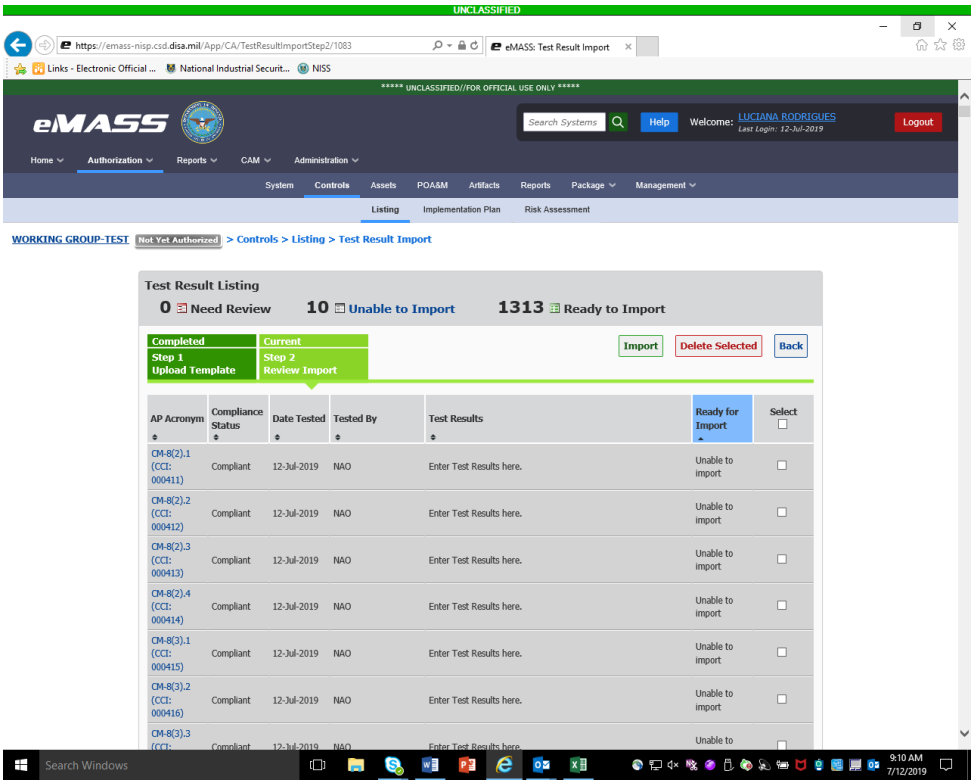
4. An eMASS template will generate. Complete all sections highlighted in blue. **The test results are required and used to document Industry's self-assessment of the security controls and provide confirmation that the security controls are applied and meet the security requirements for the system.** The template includes instructions and examples.



5. When the template is complete, return to the Import/Export home page. Click [Browse] to upload the completed eMASS-generated Test Result Export template. Click [Upload].



6. The user will be taken to Step 2 – Review Import to verify that the imported test result information is correct.

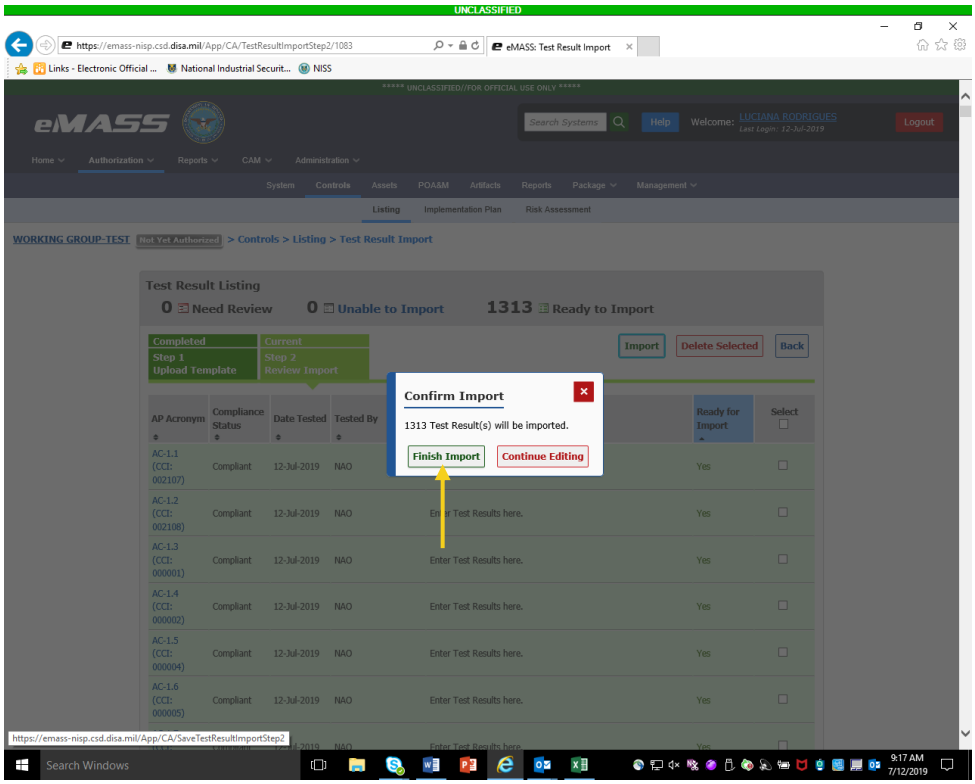


Test results that are ready to be imported will be highlighted green and do not require updates. If test results are highlighted in red, there are errors and the controls are not ready to import. Test results highlighted in grey are unable to be imported into the system.

Users may apply the following options to imported test result: (1) Edit test results by clicking on the hyperlinked cell or row; (2) delete test results by placing a checkmark in a checkbox for a test result and clicking [Delete Selected]; and(3) update test results by clicking on a hyperlinked row with errors.

Note: If there are any test results with errors, eMASS will prompt the user to review those entries before proceeding to the next step.

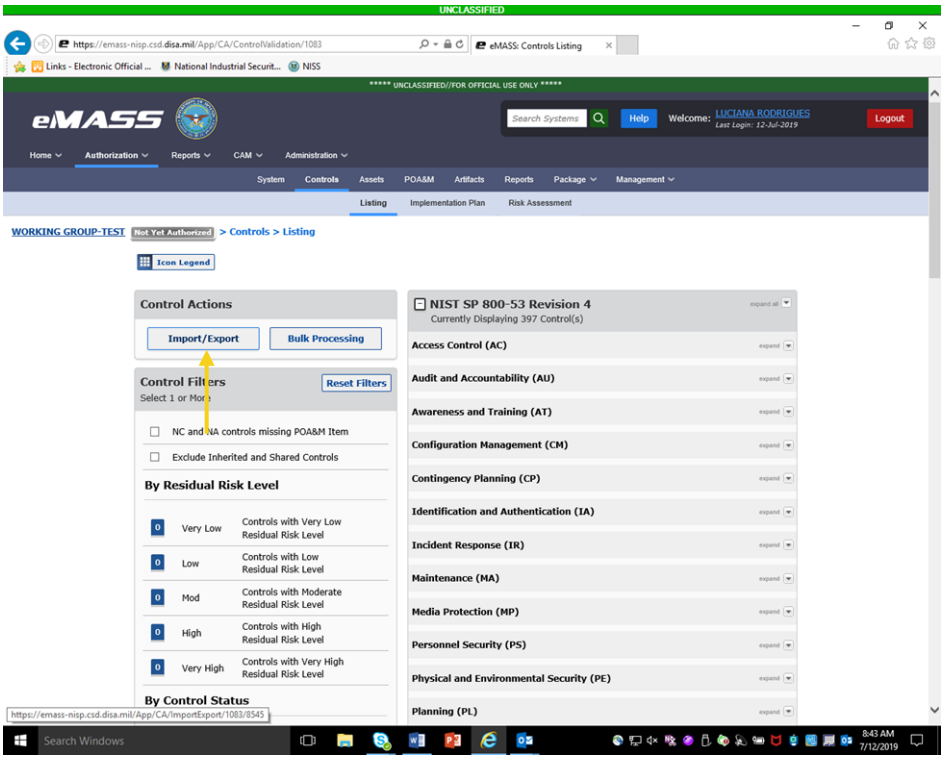
7. After confirming all of the test results are ready for import, click [Import]. Review the summary information and click [Finish Import].



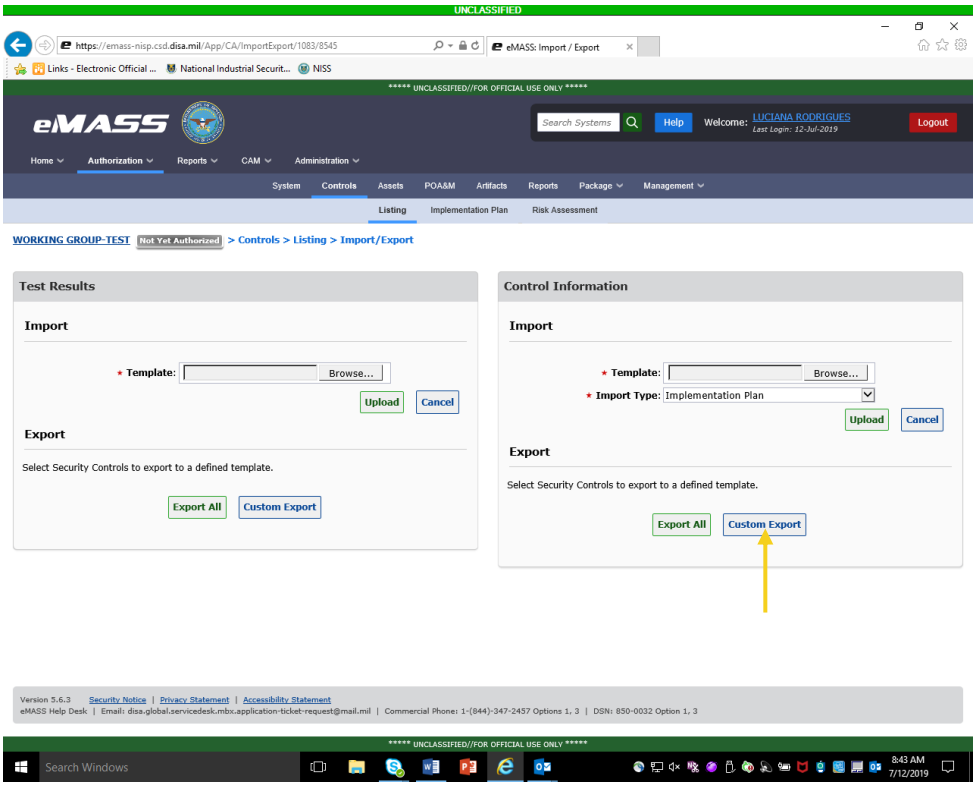
The newly imported test results will be added to the Test Result History table for the associated APs. The Control/AP compliance status will be updated automatically based upon the imported test results.

Control Import/Export

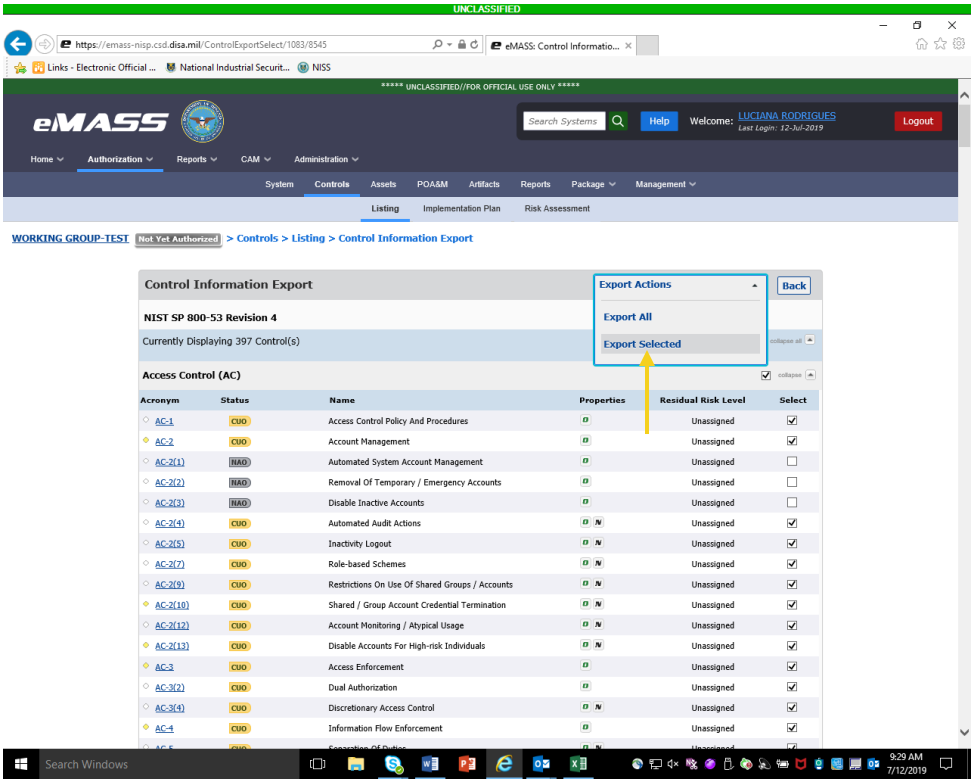
1. To begin the process, click [Import/Export] under Control Actions on Controls – Listing view.



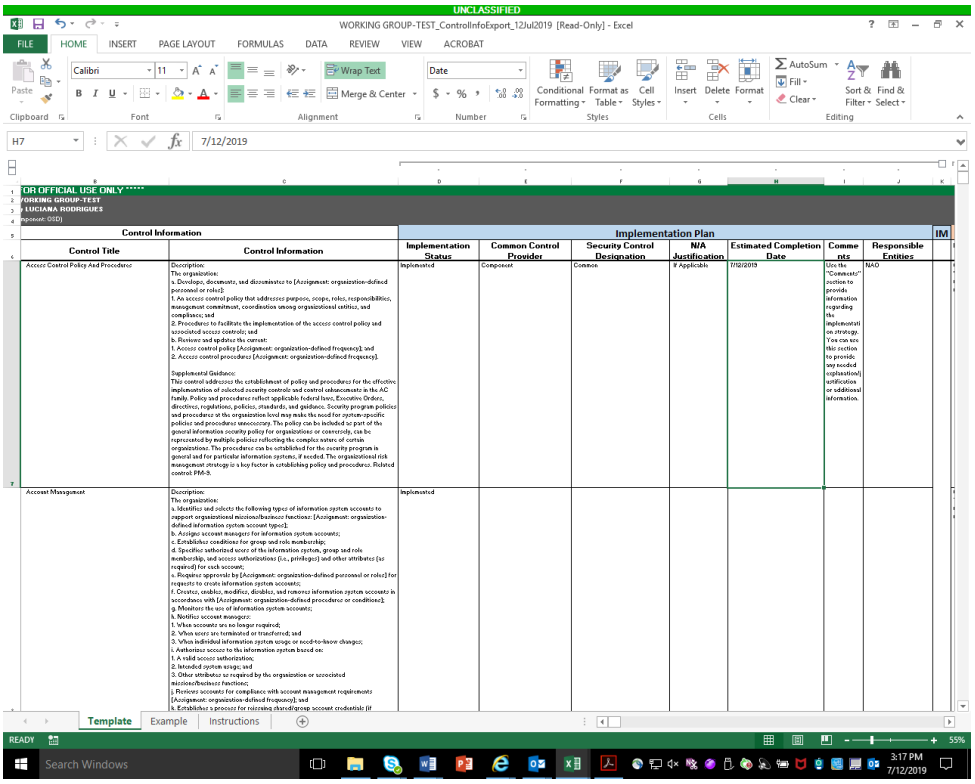
2. Control Export allows users to select security controls to export to a defined custom template. From the Import/Export home page, click [Custom Export].



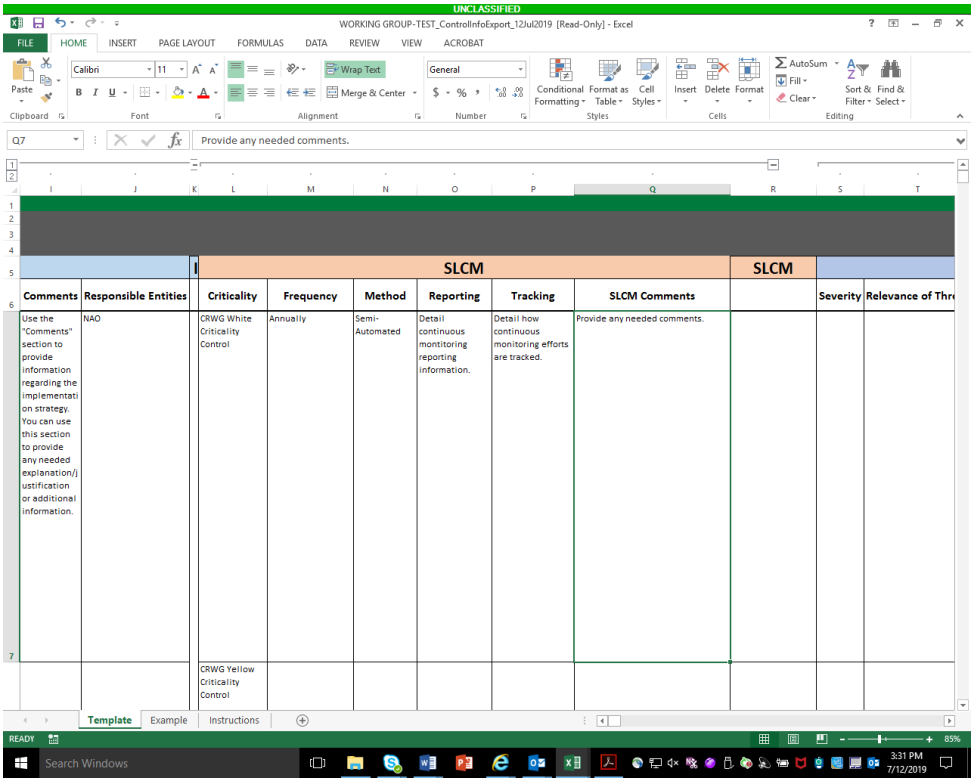
3. Place a checkmark in the checkbox of the security controls that will be exported. **Ensure that controls marked NAO due to application of an overlay are NOT selected.** Select [Export Selected] from the drop down.



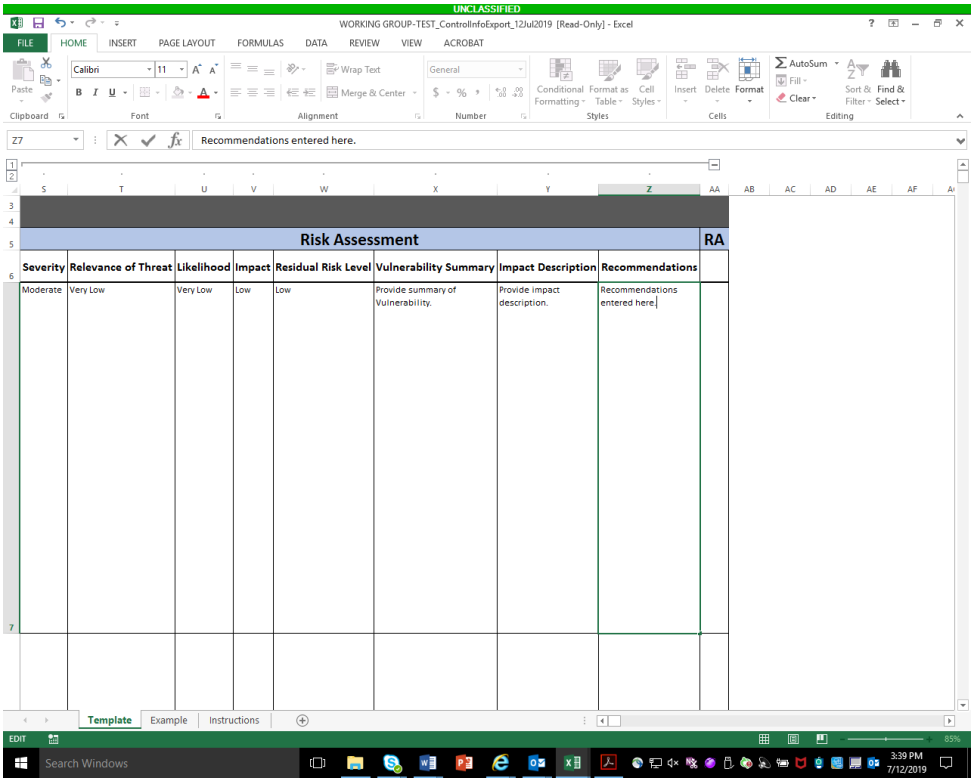
4. An eMASS template will generate with Implementation Plan, SLCM Strategy, and Risk Assessment. Complete all required fields in the Implementation Plan section. **Use the "Comments" section to provide information regarding the implementation strategy and functional description of security control Implementation (including planned inputs, expected behavior, and expected outputs). This section will include any additional information necessary to describe how the security capability is achieved. Users can also use this section to provide any needed explanation/justification.** When referencing an artifact to support the implementation of a security control, provide the following: artifact name, description, type, template (if applicable), category (e.g., Implementation Guidance, Evidence, and Other), expiration date, last reviewed date, page number, and artifact owner (if applicable).



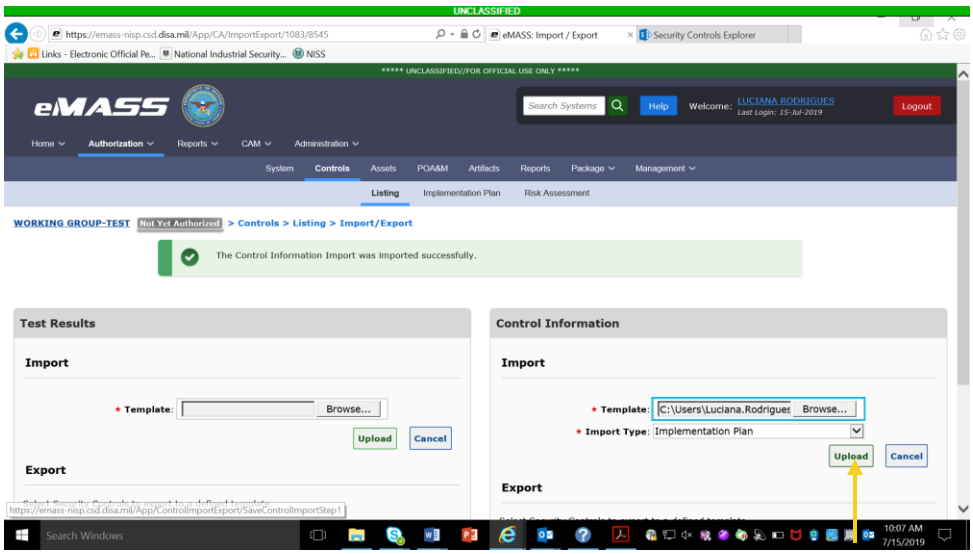
5. Complete all required fields in the SLCM section.



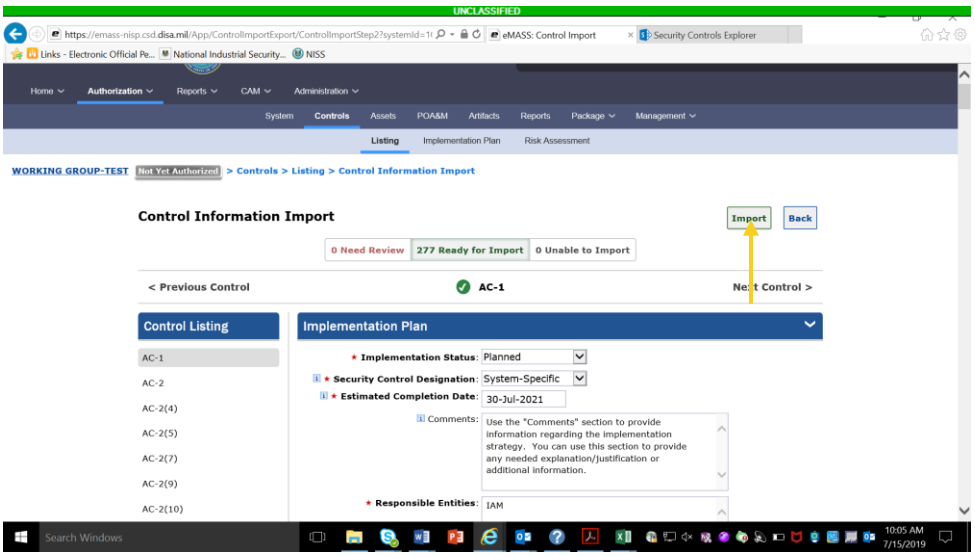
6. For all NC security controls, users must complete the fields in the Risk Assessment section.



7. When the template is complete, return to the Import/Export home page. Click [Browse] to upload the completed eMASS-generated Control Export template. Click [Upload]. From the "Import Type" drop down, users may select to import "Implementation Plan" information, "Risk Assessment," information, or "Implementation Plan & Risk Assessment" information. Click [Upload].



8. The user will be taken to the second step of Control Import to verify that the imported information is correct. Control information that is ready to be imported and does not require updates will be located within the green [# Ready to Import] section. Control information that is not ready to import will be located in the red [# Need Review] section. Control information that is unable to be imported will be located in the grey [# Unable to Import] section.



Users have the following options for imported Security Controls:

- Edit Security Control information by clicking on the Control within the “Need Review” and/or “Ready for Import” sections of the Import. If any information is modified, the user must click [Save Control] to ensure the changes are recorded before proceeding. [Save Control] will only appear once all required fields have been completed; and
- Users can completely remove imported information per Security Control by clicking [Delete Control] within the “Need Review” and/or “Ready for Import” sections of the Import.

4.3.3 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 SLCM Strategy.

Note: The instructions below are for adding Implementation Plan information individually. If the user has used the Control Import/Export feature to import Implementation Information, this information will be prepopulated.

To edit the Implementation Plan, conduct the following actions:

1. Select the Control(s) to edit in the "Select Visible" column and click [Edit Selected]; and
2. 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:

<u>Implementation Plan</u>

1. Implementation Status: Select Applicable Option;
2. Security Control Designation: Select Applicable Option;
3. Estimated Completion Date: Enter projected completion; and
4. Responsible Entities: Personnel responsible for implementing each control.

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

1. 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 NC. Please reference the Control Statuses Section of the DISA eMASS User Guide.);
2. Frequency: Indicate the frequency with which the Control is monitored;
3. Method: Indicate the method of monitoring the Control;
4. Reporting: Provide a short narrative explaining who reports what to whom by when;
5. Tracking: Provide a short narrative explaining how security controls found to be non-compliant or ineffective will be tracked; and
6. SLCM Comments: Provide a short narrative further explaining any other details not appropriate for the other fields.

Reference the DISA eMASS User Guide (Implementation Section).

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

4.3.4 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 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 can 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 users 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 can enter risk assessment information from the Control Details page.

1. On Control Details, click [View/Edit];
2. The Edit Risk Assessment Information pop-up displays;
3. 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; and
4. Enter information and click [Save].

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

Note: Risk Assessment information must be completed for NC controls prior to submitting for review.

4.3.5 SUBMIT FOR REVIEW

Prior to submitting for review, Industry must ensure the following is complete:

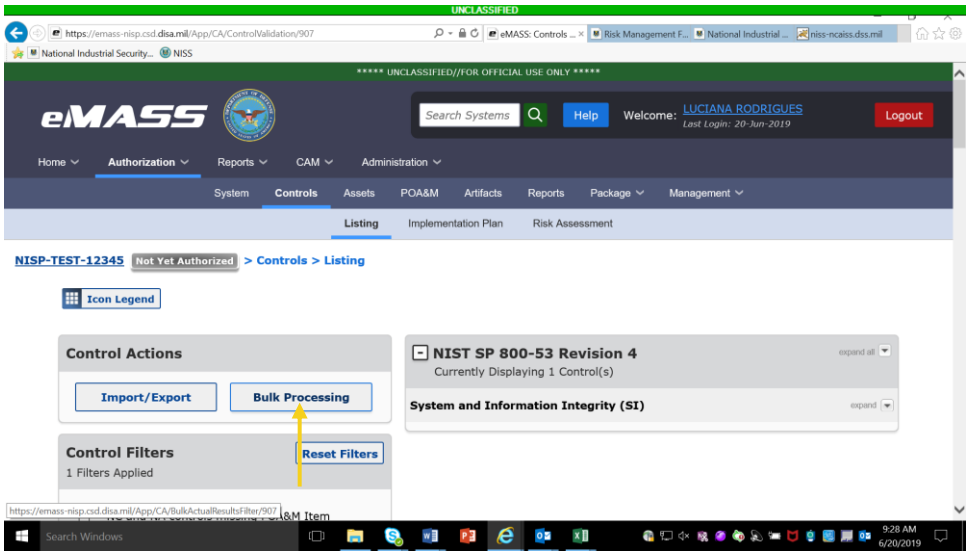
1. Test Results for all security controls;
2. Implementation Plan for all security controls;
3. SLCM for all security controls; and
4. Risk Assessment for all NC controls.

Note: System packages must contain acceptable responses for Test Results, Implementation Plan, SLCM, and Risk Assessment (if applicable). If the responses are not acceptable and the documentation is insufficient, the system package review will take additional time and the ISSP may recommend a DATO.

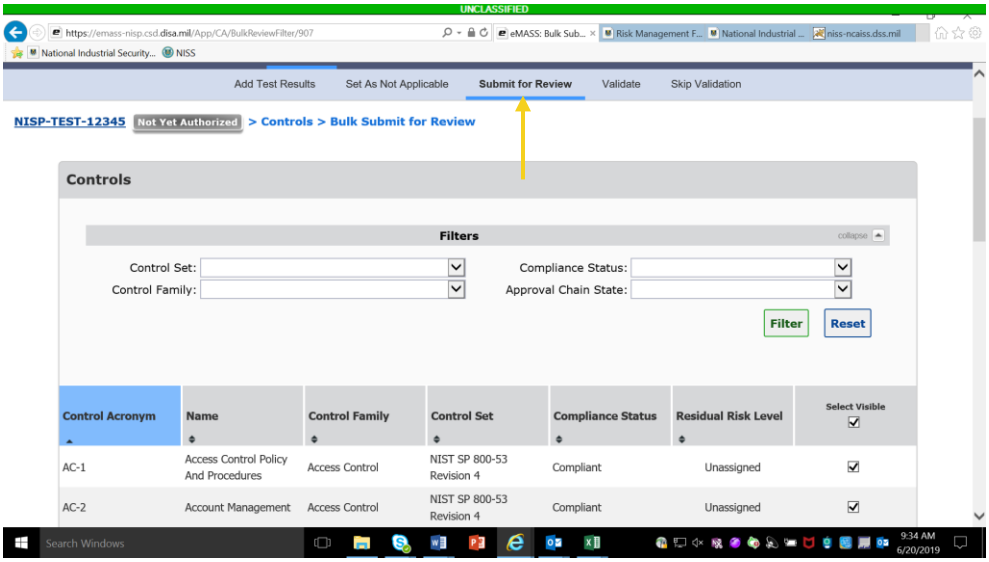
Industry/CAC – 1 Actions: Once all the information listed above is complete, the security controls are ready to move to the next stage of the CAC (CAC – 2/ISSP). **Industry users are NOT required to initiate a workflow to submit.** The ISSP will complete the control validation/assessment. When the validation process is complete, the ISSP will initiate the Package Approval Chain workflow.

Use the Bulk Processing feature in eMASS (Section 10.1.3 of the DISA eMASS User Guide) to submit controls to the ISSP in the CAC – 2 Role for validation.

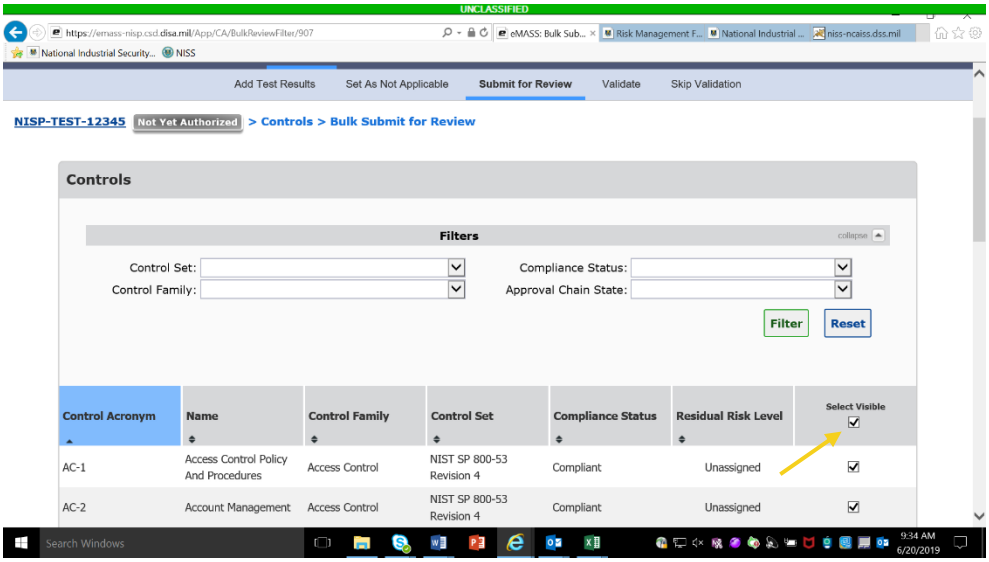
1. Select [Bulk Processing] on the Controls – Listing screen.



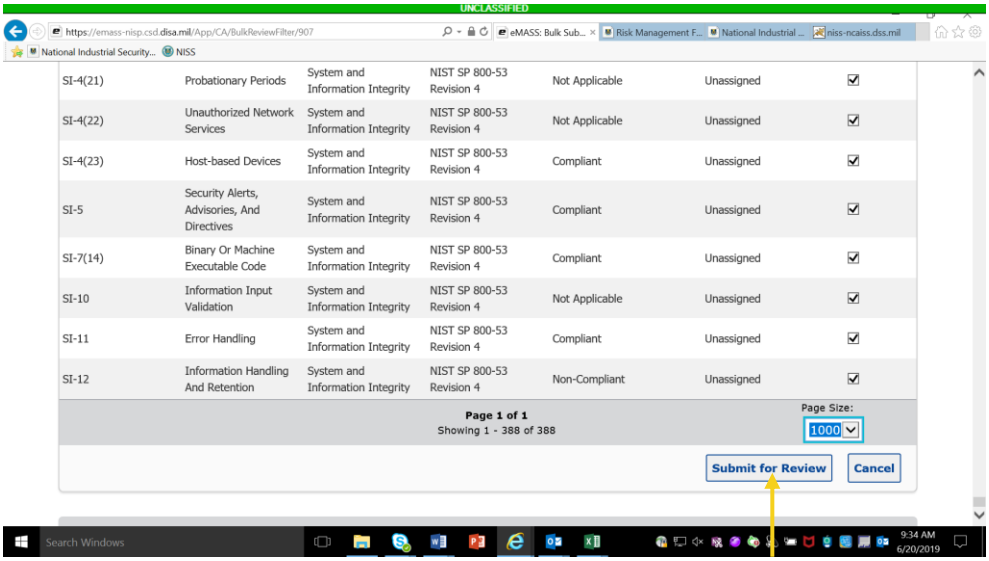
2. Bulk Processing has the following options: "Add Test Results," "Set as Not Applicable," "Submit for Review," "Validate," or "Skip Validation." Select “Submit for Review.”



3. Place a check in the “Select Visible” checkbox next to all the security controls. *Note: Scroll down to the bottom of the page and expand page size to 1000 to view/select all.*



4. Select “Submit for Review.”



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

5. To check the security controls status in the CAC, IAM users that either registered the system or have an assigned IAM role for a system package can run a CAC History Report. This report allows users to see the system’s package status within the CAC.

   Reports > CAC History Report > Select the System Acronym from the drop-down menu > Generate Report.

<u>Industry/CAC – 2 Actions</u>: 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. If the ISSP adds a test result before approving the control, the control’s status 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; and
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 receives a final validation status of Compliant Official (CO), Non-Compliant Unofficial (NCO), or Not Applicable Official (NAO).

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

4.4 ASSETS

The Assets module allows users to manually document the system's hardware and software components and increases the system's security posture visibility by mapping asset scan results to security controls.

THIS SECTION WILL NOT BE USED.

4.5 PLAN OF ACTION AND MILESTONES (POA&M)

eMASS allows users 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. eMASS requires a POA&M for NC controls. If annotating a system vulnerability is determined to be classified as per the SCG, indicate in eMASS that details will be maintained on site.

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 can view details of locked POA&M Items in the System POA&M, but can only 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.

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

Note: A POA&M Template is available in the "Help" section of eMASS.

4.6 ARTIFACTS

The user can 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.

To add artifacts, conduct the following actions:

1. Select Artifacts on the top menu;
2. Click [Artifacts] to open the Artifacts screen;
3. Click [Add Artifact] and the Add Artifact screen opens;
4. Search for the desired control and/or AP associated with the artifact 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;
5. 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;

6. 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 e tracking of any artifact that requires periodic reviews and updates; and
7. Enter the artifact information. The "Category" drop-down 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; and
    - Click [Save] to complete the process of adding the artifact and to return to the Control Details screen.

Reference the DISA eMASS User Guide (Artifacts Section).

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

4.7 PACKAGE

DCSA will submit packages through the 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:

1. Assess and Authorize;
2. Authorization Extension;
3. POA&M Approval; and
4. Security Plan Approval.

Note: Industry completes the package in the CAC. The actions below are conducted by DCSA.

Package Workflow: DCSA users have the ability to "initiate" a workflow to the first PAC role. Once a workflow is initiated, all systems' progress can be tracked at each step in the RMF workflow. Within the workflow, Collaboration Boards facilitate communication between system personnel. The ISSP will conduct the following actions to initiate a workflow:

1. Navigate to the Package Status tab located within the Package main tab;
2. Choose the workflow type that will be submitted into the PAC;
3. On the Create New page, enter the "System Name" and enter optional "Comments." Click [Initiate Workflow] to initiate the Workflow;
4. A confirmation message will appear stating that the workflow was successfully initiated; and
5. PAC users can now 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, the ISSP/PAC – 1 role will submit the initiated package.

1. 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; and
2. Select [Submit] from the "Action" drop down, 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.

1. Click [Updates to System] from the Package Status screen;
2. 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; and
3. 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 the following information and notifications:

1. 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;
2. The "Assessment Recommendations" section shows any special artifacts and comments added by Package Reviewers;
3. 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; and
4. 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.

1. "Return for Rework" option is selected from the "Select Action" drop-down menu;
2. Select the appropriate role in the drop-down menu; and
3. Provide comments and click [Return for Rework].

Applying an Assessment Decision: For authorization package types, the DCSA roles can 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 recommend an Authorization Termination Date (ATD). After applying the assessment decision to the active package, the DCSA PAC roles will automatically be taken to the Package Reports view to apply a digital signature to the SAR.

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

1. Once an "Authorization Determination" for the package is selected, the "Authorization Date," "Terms/Conditions for Authorization," "Authorization Termination Date," and "ADD Classification" fields appear;
2. The "ATD" field will display a list of preset dates based on the "Authorization Status" the user selected;
3. The AO will enter information for all required fields and select [Authorize]; and
4. 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).

4.8 MANAGEMENT

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

Users can 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).

5 DECOMMISSIONED SYSTEMS

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

1. Decommissioned systems remain in the eMASS instance repository but no longer appear on any reports, metrics, or general system searches;
2. New inheritance relationships cannot be requested with systems that have an "Authorization Status" of "Decommissioned";
3. Setting an "Authorization Status" as 'Decommissioned' will automatically update the "RMF Activity" field to "Decommissioned";
4. Setting the "RMF Activity" field to "Decommissioned" will automatically update the "Authorization Status" to "Decommissioned"; and
5. Systems of any Registration Type can be set to "Decommissioned."

The following procedures will be used to decommission a system:

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

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

6 REPORTS

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).