NISP eMASS Facilitates Successful Package Submission

This article provides guidance for, and examples of, the National Industrial Security Program (NISP) Enterprise Mission Support Service (eMASS) capabilities for cleared industry to facilitate an effective cybersecurity program. This information is intended as a work aid for security managers, information systems security managers (ISSM), and other cybersecurity staff. Security managers and ISSMs should work together with their security officer and other pertinent staff skilled to ensure eMASS is being used in a holistic, cost- effective, and strategic manner. Use of these features should be part of an overall risk management strategy that considers the full range of system features available for creating and sustaining a healthy, enterprise cybersecurity program.

First, when submitting systems in the NISP eMASS for Assessment and Authorization, ISSMs must submit complete system security packages addressing all security controls applicable to the system. This includes system description, control implementation language, risk assessments, control assessment procedures, and Plans of Action and Milestones (POA&M) for any non-compliant or partially implemented controls. System packages submitted without all security controls fully addressed will no longer be accepted for review.

Three key features that enable organizations to expedite the authorization of Risk Management Framework (RMF) security packages are: Authorized Common Control Provider package, Control Bulk Import/Export, and Control Inheritance. ISSMs are highly encouraged to make use of the RMF-specific features within eMASS when creating system security packages. Here is an explanation of these key features:

An authorized Common Control Provider (CCP) plan enables organizations to document enterprise processes to ensure consistency and streamline Assessment and Authorization processes. CCP packages include the organization's approach to enable standardized RMF implementation across multiple NISP programs. The CCP package is used to identify the common controls and all the associated procedures and artifacts. In addition, it will specify if the common controls provide the required protection fully (with nothing further needed from the system) or in hybrid fashion (partially by the alternative, with the remainder provided by the system).

The Control Bulk Import/Export allows users to export/import a System's Implementation Plan, System Life Cycle Management (SLCM) Strategy, Risk Assessment information and Assessment Procedures (AP) and Control Correlation Identifiers (CCIs). Bulk Import/Export provides flexibility to users in situations where security control assessment activities may have already been performed outside of eMASS.

The Control Inheritance identifies authorization boundaries and creates relationships (i.e., Parent/Child, Provider, or Co-System) between interconnected systems registered in eMASS, allowing for establishing system hierarchy or information management. Users can establish an inheritance relationship where an individual security control/AP is provided from one or multiple

systems. With full inheritance, a receiving system will have visibility into all the test results, POA&M items, and artifacts from the originating system(s). With hybrid inheritance, 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.

To reiterate, a timely authorization decision is contingent upon users submitting a complete and accurate security plan. DCSA highly recommends submitting security plans, initial or a reauthorization, at least 90 days before the need date. A complete security plan has all the required system details, supporting artifacts, and security control information (including test results) needed to support authorization activities. This timeframe will allow for a complete plan review to include the on-site assessment, interaction between the ISSM and the DCSA information systems security professional (ISSP), and the opportunity to address any potential updates or changes to the security plan.

Industry users should ensure the following is complete:

a. Required system details are populated.
b. Implementation Plan and System-level Continuous Monitoring Plan is completed for all security controls.
c. Risk assessment is addressed for all non-compliant security controls.
d. All artifacts needed to support authorization activities are included.
e. Assessment Procedures and Control Correlation Identifiers (CCI), assigned to a security control, are tested and the test results applied for all security controls.
f. POA&M is accurate and addresses all non-compliant controls…worth repeating.

In addition, a completed system security plan must include supporting artifacts. For more information on supporting artifacts, see DCSA Assessment and Authorization Process Manual (DAAPM) Version 2.1, section 7.5 found here: https://www.dcsa.mil/Portals/91/Documents/CTP/tools/DCSA_Assessment_and_%20Authorization_Process_Manual_Version_2.1.pdf

Finally, the DAAPM and its associated appendices (contains templates and overlays for download) should be the ISSM's first stop for answers to questions regarding the assessment and authorization of systems and contains specific guidance outlining DCSA expectations for the successful approval of system packages. The DAAPM Version 2.1 was released in February and becomes effective on March 9, 2020. It supersedes all previous versions.

Another important document is the NISP eMASS Industry Operation Guide Version 1.1, which was created to assist industry users in navigating the system. The operation guide provides detailed instructions on account management, registering a system, completing required fields in the RMF Security Plan, submitting controls, and management and inheritance. Industry can gain proficiency with eMASS by using the operation guide and referencing the NISP eMASS Information and Resource Center: https://www.dcsa.mil/mc/ctp/tools

The NISP Authorization Office acknowledges that these features and capabilities alone will not solve all of cleared industry's cybersecurity or eMASS challenges. Furthermore, these items might require expending resources on training, qualified personnel, or even equipment to fill in gaps identified as a result of implementing these features. We do know, however, that by reading the DAAPM, becoming proficient with NISP eMASS, and following the guidelines posted, your facility will be well on its way to an effective cybersecurity program.

This article is provided for NISP Cleared Contractors from Karl Hellmann, Authorizing Official, NISP Authorization Office, Defense Counterintelligence and Security Agency.