FISWG Training

RMF and eMASS Tips for Success

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

John Forster, ISSP Team Lead
Southern Region

AGENDA

- RMF History
- Submitting an Acceptable Package
- Operational Issues
- eMASS Processing Items

RMF History

- August 24, 2016- DAAPM 1.0 requiring Risk Management Framework was released
- October 3, 2016- All expiring accreditations and new Authorizations for “Stand-Alone” systems required RMF
- March 31, 2017- DAAPM 1.1 was released
- May 19, 2017 – Notice that ALL information systems must follow RMF starting **January 1, 2018**
- November 17, 2017- DAAPM 1.2 was released
- June 4, 2018- DAAPM 1.3 was released
- May 6, 2019- DAAPM 2.0 was released (**eMASS transition**)
- February 6, 2020- DAAPM 2.1 was released
- August 31, 2020- DAAPM 2.2 was released

Controlled Unclassified Information (CUI)

- CUI will NOT be discussed during this presentation.
- Please refer to the DCSA website concerning any upcoming changes related to any upcoming CUI oversight.

www.dcsa.mil/mc/ctp/cui

Submitting an Acceptable Package- General

Help Documentation

Our eMASS help documentation has information for the latest version of eMASS, version 5.8.

Release Notes

Updates to eMASS and change log.

Helpful Links

DoD Cyber Exchange

Don't forget about the Help Section in eMASS

Organizational Artifact Templates, SOPs, and Guides

- Contingency Plan
  Contingency Plan Template
- Data Transfer Agent Authorization Form
  Data Transfer Agent Authorization Form Template
- Government to Contractor ISA Template
  Government to Contractor ISA Template
- Hardware List
  Hardware List Template
- Incident Response Plan
  Incident Response Plan Template
- IS Access Authorization and Briefing Form
  IS Access Authorization and Briefing Form Template
- IS Privileged Access Authorization and Briefing Form
  IS Privileged Access Authorization and Briefing Form Template
- ISSM Appointment Letter
  ISSM Appointment Letter Template
- Maintenance, Operating System and Security Software Change Log
  Maintenance, Operating System and Security Software Change Log Template
- Mobility System Plan
  Mobility System Plan Template
- Risk Assessment Report
  Risk Assessment Report Template
- RMF Security Plan Submission and Certification Statement
  RMF Security Plan Submission and Certification Statement Template
- Security Seal Log
  Security Seal Log Template
- Software List
  Software List Template
- System Diagram - Network Topology
  System Diagram - Network Topology Template
- Upgrade-Downgrade Procedure Record
  Upgrade-Downgrade Procedure Record Template
- DCSA Assessment and Authorization Process Manual Version 2.2

Submitting an Acceptable Package- General

- As ISSM, your KEY to submitting an "acceptable" authorization request package is to READ and FOLLOW the NISPOM, DAAPM, and the NISP eMASS Industry Operation Guide. These are the main references the ISSM will use to assess your plans. All of these guidance documents are available on the DCSA website. (https://www.dcsa.mil/Portals/91/Documents/CTP/tools/)
- A recent update to NISP eMASS replaced the "Comments" field with the "Implementation Narrative" field. All references to the Comments field in the NISP eMASS Industry Operation Guide are now applicable to the Implementation Narrative field. (Note: Although this isn't a required field for eMASS, it is for DCSA)
- Review the applicable SCGs to determine the classification level of system details (especially vulnerabilities). NISP eMASS is not approved for storing classified information. If system artifacts, information, or vulnerabilities are classified per the SCG, do not enter this data into eMASS. Follow guidance provided in the operation guide and contact the assigned ISSP.
- As ISSM, you are required employ a high level of attention to detail and conduct the initial assessment of the SSP prior to submitting it to DCSA for assessment. Details are outlined in DAAPM Ver. 2.2, Para 7.5.1.1, Task A-1.
- Notify your ISSP once you have transferred ALL security controls to CAC-2 in NISP eMASS. (Note- you can run a Reports>CAC history report to be sure all controls were included)

Submitting an Acceptable Package- Metadata

- There are many fields that need to be completed that tell DCSA “about” the system.
- Section 4.1 provides guidance for naming conventions and specific expected fields like “National Security System”, but one of the most important sections is the System Description. Include all fields identified in the guide. (note section 5.1.x requires more items)
- Section 4.2 covers Authorization information and need dates. (remember DCSA recommends submitting NLT **90 days prior to ATD or need date**)
- Section 4.3 covers roles- Select a DCSA field office instead of an individual ISSP or ISSP-TL, and select Southern Region vs. a specific AO.

Submitting an Acceptable Package- Controls

- Collaborate with the Government Information Owner regarding categorization and control selection. (CIA of Moderate/Low/Low is the starting point. See if contractual documentation sheds light.)
- Do not select the "Classified Information" overlay unless you are required to have above MLL. Then you and the IO would need to reference CNSSI-1253 for required additional controls.
- Choose the correct Overlay for your system based on system type. If you choose the wrong one it is difficult to recover. (Note: A Client Server LAN requires 388 controls to be addressed)
- Seek formal documentation from the IO for tailoring due to contractual obligations or cost, Ref: DoDM 5220.22, Vol. 2.
- Ensure implementation details address ALL aspects of the control requirements.
- Make sure the ISSP can find your implementation information. (The best place is within the control. Do not make the ISSPs search through supporting artifacts to gather information.)

Submitting an Acceptable Package- Controls

- Pay attention to implementation details.- For example don't have a control status of "Applicable" while details indicate "Not Applicable".
- Understand the difference between control Types.
  - Common- Controls that will be "inherited"
  - System Specific- Controls that stand on their own.
  - Hybrid- Controls that are only fully described by both of the above
- Understand the difference between Not Applicable (NA) and Non-Compliant (NC).
  - NA Controls: (are not subject to ConMon and continued testing)
    - Controls that are part of an Overlay
    - Controls that have been covered by formal documentation provided by the Government IO
    - Controls that are justified by the ISSM and validated by the ISSP as not applicable for the system, and passes the common sense test (e.g., consider "external" type controls when you have an isolated LAN)
  - NC Controls: (require POAM entries and risk level)
    - Controls that are "applicable" but not fully implemented.

Submitting an Acceptable Package- ConMon

- Continuous Monitoring (ConMon) is an important aspect of the overall security because it communicates to DCSA how controls are going to be assessed for continued effectiveness over time.
- ConMon strategies should include details related to steps that “will be” taken by the defined frequency to check on controls.
- Frequencies that differ from the recommended DAAPM Appendix A timeframes should be justified. Don’t expect to be able to make all checks an annual event.
- The ISSP will validate your documented ConMon activities against the verbiage in the SLCM during CMEs and eSVAs. Deviations from documented SLCM activities will likely result in vulnerabilities being documented/cited during the CME/eSVA.

Submitting an Acceptable Package- POA&M

- All Non compliant security controls must be included on the POA&M.
- Items should include specific steps required in support of particular Milestone events.
- Realistic dates should be provided as supported by the underlying and documented steps.
  (Note: Don't include items on the POA&M and simply set a date for three years from when it was entered.)
- POA&M items are approved as a part of the IS authorization package. A separate approval is not needed unless the POAM needs revised.

Submitting an Acceptable Package- Test Results

- Test Results are not Implementation Narrative details or ConMon
- Test Results are a summary of the actions that have already taken place to validate that controls has been effectively implemented.
- Bad Example:
  - Annually user accounts are reviewed.
  - DOD automatically compliant
- Good Example:
  - User accounts on the system **have been reviewed** and it was confirmed that there are no existing group accounts.
- Test results should address each CCI. If you reference SCAP results make sure the STIG check applies to the specific CCI.
- Avoid Referring to additional artifacts that contain test results.

Submitting an Acceptable Package- Final Checks

- The operations guide states (Section 5.6),
  - "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.
    - 4. Risk Assessment for all NC controls.
  - *Note: Security controls 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."*

Submitting an Acceptable Package- Final Checks

- Artifacts:
  - Make sure all necessary Artifacts are provided (see Task A-5 of the DAAPM)
    - Apply common sense
      - Make sure diagrams are legible, show all components and information flow, and make the proposed authorization boundary clear.
      - You always need some type of Government sponsorship/contract. (don't forget to ensure your CAGE is listed as a Performing Location)
      - You don't need a mobility plan if there is no mobility.
      - Associate artifacts related to specific controls within eMASS.
  - *Note: One artifact not on the list is the Security Classification Guide(s), but if it is Unclassified include it. (and make sure you read it before uploading information in eMASS so you don't create a Spill)*

Submitting an Acceptable Package- ISSM Reminders

- The cleared contractor will appoint, in writing, an **employee** as the ISSM. Each site is required to have an ISSM capable of effectively handling **day-to-day operations** and responding to security instances.
- ISSMs are to conduct the initial assessment. The DCSA guidance within the CA-2 Control states,
  "*The initial security assessment is performed by the ISSM and determines the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements*."
- Remember that the ISSM needs to sign a Certification Statement **every time** a package is submitted.
- Remember that the ISSM is certifying:
  - Security controls and protection measures as described in the submitted package have been implemented.
  - Any items that don't meet all NISPOM and DAAPM requirements are on a POA&M.
  - Making willful false official statements or concealing a material fact is a felony.
- If an acceptable plan has been submitted correctly, all an ISSP should have to do is check your homework…

Operational Issues- Contractual Evidence

- Task A-5 in the DAAPM requires some type of sponsorship artifact in support of the IS.
- Please ensure that both the FSO and ISSM are familiar with the contractual documentation and the requirements contained within.
- Ensure any new contractual efforts for an existing system are considered a potential change needing reviewed by the CCB.
- Things to look for:
  - Make sure the CAGE requesting the system is identified in the performing location block. (for DD-254s)
  - Ensure that the applicable SCGs are on hand and have been reviewed regarding the classification of IS details.
  - Read and implement the system/data disposition instructions.
  - Security Impact Analysis considerations for the CCB (for new work).
    - TEMPEST requirements
    - Information Assurance certification requirements
    - Additional guidance related to incident response
    - Guidance related to IS Categorization
    - Information related to required formal access approvals or handling caveats

Operational Issues- Federal Information Systems

- DAAPM Section 9.8 discusses FIS and points the reader to DOD Manual 5220.22 Volume 2.
- Volume 2 (section 11.4) indicates that a Federal Information System should be:
  - Located in Federal space under a formal agreement with the contractor.
  - Or…Granted an exception to policy (by OUSD (I&S)) for continuing to operate in Contractor Space overseen by DCSA.
- In some instances, an alternative option is for the contractor to acquire the necessary security information, oversight, & administration of the system for DCSA to be able to authorize it.
- Any FIS discovered during DCSA reviews (which don't follow Vol 2 section 11.4) will be assessed a vulnerability. (Reference NISPOM 8-100.d, DAAPM 9.8)

Operational Issues- Unsupported System Components

- These have previously been referred to as “Legacy” OSs, but SA-22 applies to any “unsupported” component.
- Unsupported system components should be completely described under the SA-22 Control.
- There are only two options for Unsupported Components.
  - Establish a POAM with realistic dates to migrate to a supported component.
  - Obtain contractual documentation iaw DODM 5220.22 Volume 2 to justify continued use. (see section 11.3)
- Risks associated with unsupported components must be documented in the Risk Assessment Report (RAR).

Operational Issues- Area Type (PE controls)

- An early system question often involves Area type.
- Closed areas are needed for unattended processing or items that can't be secured in a GSA-Approved container.
  - Requires specific physical attributes
  - Requires approval by DCSA Industrial Security Rep
  - Is documented on a DCSA Form 147
- Restricted Areas can be used but require additional considerations.
  - Coordination with the FSO
  - Upgrade/Downgrade procedures and logs
  - Security seals may be necessary (a diagram is helpful)
  - User training is key to detect any tampering **prior** to use

Operational Issues- System Changes

- Address the proposed change with the CCB first.
  - Conduct a Security Impact Analysis and present the results to the CCB for consideration.
- Document the CCB minutes as part of the CM-3 ConMon record.
- Coordinate with your ISSP regarding:
  - The controls, ConMon, and Tests that will be revised
  - Resubmitting the package in eMASS using the bulk upload for impacted controls, ConMon, and Tests.
  - When requested changes can be implemented (some may be able to start immediately while others need to wait until eMASS validation is completed).
- The ISSP will determine if the system needs a reauthorization and a new ATO letter prepared for signature. If not, controls will change from the "unofficial" to the "official" status after validation. (There is a risk that controls can be returned for rework as well)

Operational Issues- Assured File Transfers (AFT)

- When is AFT needed?
  - A form of it is needed if your system is authorized for Secret/CNWDI but you need to extract Secret.
  - Anytime you need to extract Unclassified information from the system.
- Where should procedures be documented?
  - The DAAPM (Appendix O) has basic requirements that can be referenced
  - Controls such as AC-3(2), AC-4, AC-16 can address specifics and reference additional artifacts as necessary.
- What about Alternate AFT?
  - Any deviations from the DCSA provided procedures need to be highlighted and approved as part of the Authorization.
- Don’t forget about the required Two Person Integrity (TPI)

Operational Issues- Externally Connected IS

- Interconnected systems have a greater potential for risk to classified information. For these IS make sure you:
  - Read the DAAPM (Section 9.6) regarding whether or not an Interconnection Security Agreement will be needed. (There is a sample template in DAAPM Appendix U)
  - Highlight the connections on the system diagram and information flow path
  - Adequately address CA-3 and SC-7 controls along with their applicable enhancements.
    - The direct connection of any system to an external network is prohibited. (boundary protection device required)- ref CA-3 DCSA supplemental guidance
    - Identify the boundary protection and how information flow is enforced. (encryption by itself doesn't manage information flow)
    - Document how deny-all, permit by exception is implemented.

Operational Issues- Protected Distribution Systems

- Addressed in Controls SC-8, SC-8(1), refer to CNSSI 7003 and www.dcsa.mil/mc/ctp/nao.
- A Protected Distribution System (PDS) must be formally approved by the DCSA Authorizing Official.
- PDS Reminders:
  - Submit your PDS "plan" prior to purchasing materials and/or actually building it.
  - Don't try to define Limited Access Areas as Controlled Access Areas. DCSA defines the CAA as the Closed Area.
  - Pay attention to construction requirements and "inspect-ability".
    - How is the PDS marked?
    - How will joints be sealed?
    - How will "voids" include inspection ports?
  - Alarmed PDS have some different requirements to consider like response time.

Operational Issues- Spill Cleanup Reminders

- Overarching things to consider:
  - Do you have an approved Company Incident Response Plan (IRP) or are you following your version of DAAPM Appendix Q?
  - Have you reviewed DAAPM Appendix R (Spills) and S (Sanitization)?
  - Does the spill involve information that DCSA doesn't have oversight for? Let DCSA know anyway and we can work with the CSO if they need assistance.
  - Do your processes involve remote cleanup with remote workers? Remote aspects of your cleanup should be clear in the submitted IRP.
  - DCSA expects cleanup to follow DAAPM guidance at a minimum as documented in your IRP. IO approval is required for spills in case the IO wants additional action. (No answer within 30 days implies concurrence with DCSA procedures).
  - IRPs are approved in conjunction with the Information System unless a separate one was submitted and approved at the corporate level.

Operational Issues- Spill Cleanup Specifics

- Be ready to provide the following to your ISSP:
  - Any checklists you utilize to confirm effective cleanup activities.
  - Documentation for any non-volatile memory that was destroyed or Sanitized. (Note that destruction is expected for Solid State Drives based on the type of memory.)
  - Logs related to overwriting activity for magnetic drives. (Note that a 3 pass overwrite is required)
  - Concurrence by either the GCA or IO if less than the DCSA procedures are used. (Note: Ensure you tell them what DCSA requires.)

Operational Issues- AI Final Report Reminders

- Refer to the DAAPM to ensure that you have covered all of the aspects of Appendix R.
- Include a list of all affected Infrastructure components and a summary of how cleanup was accomplished on each component.
- Make it clear how long classified information was at risk.
- Identify any controls that provide additional insight regarding risk mitigation. (e.g. limited file access by userid)
- Make sure the report draws a conclusion, addresses potential culpability, and discusses how any corrective actions can prevent a reoccurrence.

Operational Issues- Audit Variances

- Variances are appropriate for proposal systems, periodic company shutdowns, etc.. Not to simply avoid audit analysis.
- There is NO longer a separate audit variance approval or a Holiday Shutdown letter.
- Audit variance information should be referenced in your AU controls as appropriate.
- Section 12 of the DAAPM requires the use of an SOP that:
  - Identifies physical protections.
  - Limits hibernation to less than 180 days.
  - Identifies any technical controls. (e.g., encryption)
  - Discusses how updates will be accomplished upon returning the system to service.
- Remember that end of day checks are still required.

Operational Issues- Miscellaneous

- When you submit for a re-Authorization you should change the system's Version Number (e.g. 1.0 to 2.0).
- SCGs should be routinely uploaded as an artifact for Package submission unless they are classified. (and noted as such)
- Read DODM-5220.22 Volume 2!
  (There are many sections you should be aware of…Special Category-11.3.d, Cost/Operational considerations-11.3.f/g, Spill cleanup approval-11.3.j, Disassociation, etc.)

eMASS Processing- Triage Review of the Package

- DCSA headquarters personnel conduct a package review shortly after packages are submitted (this started a couple months ago).
- The review is designed to assess the completeness of the package based on compliance with the eMASS Industry Guide and the DAAPM.
- Personnel conducting the review respond directly to the Company on behalf of the ISSP, but the ISSP is not coordinated with.
- If the package is considered INCOMPLETE it will be returned to the ISSM for rework and a report uploaded as an artifact.
- All packages will go through this Triage by headquarters personnel.

eMASS Processing- POA&M Updates

- At the end of March there were 1361 systems that had at least one overdue POAM item (404 systems in the Southern region).
- Future plans anticipate the ability for ISSMs to create a POA&M workflow in eMASS….but until that occurs:
  - Update POAM items as they are completed.
  - Identify any necessary extensions with a justification for review.
  - Add any additional items as a result of continuous monitoring efforts or DSCA assessments.
  - Return all controls impacted by changed POA&M items to the SCA for Assessment (notify the ISSP via email **summarizing why the package is being submitted**).
  - The SCA/ISSP will assess the controls and Revised POAM.
  - The SCA will either validate the controls and process a workflow for an authorization (with or w/o a new ATO) which will approve the POA&M or return items for rework.

eMASS Processing- Decommissioning a System

- Considerations should be made during the creation of your system package. You need to know in advance how you are going to disposition classified material. (MP-6 is a good place to start)
- DAAPM (Task M-6) states,
  "A decommission plan addresses the approach used to securely transition the system and system elements into a decommissioned state. The plan determines approaches, schedules, resources, specific considerations of decommission, and the **effectiveness and completeness** of decommission actions."
- The ISSM must initiate the Decommission workflow in eMASS.
- The ISSP will review the Decommission plan and assess compliance with established sanitization procedures or retention authorities.
- The workflow ends ones the Authorizing Official signs.
- **Don't** use the System Details>Authorization information> RMF Activity> "Decommission" field in eMASS (This is reserved for the AO). A decommission workflow is required to be initiated by the ISSM.

eMASS Processing- CCPs

- Common Control Plans can't realistically include all 388 controls.
- CCPs will not be approved with "planned" controls.
- If a system with an inherited control is found to be NC, it will impact the CCP as well as ALL systems inheriting that control.
- Relevant controls must be marked as "common" and be made "inheritable".
- Subsequent systems that inherit the controls have to identify the common control provider.

Acronyms

- AFT- Assured File Transfer
- ATD- Authorization Termination Date
- ATO- Authorization to Operate
- CAC- Control Approval Chain
- CCB- Configuration Control Board
- CCP- Common Control Plan
- ConMon- Continuous Monitoring
- CUI- Controlled Unclassified Information
- DATO-Denial of Authorization to Operate
- eMASS- Enterprise Mission Assurance Support Service
- FIS- Federal Information System
- GCA- Government Contracting Agency
- IO- Information Owner (Government)
- IRP- Incident Response Plan
- ISA- Interconnection Security Agreement
- ISSM- Information System Security Manager
- ISSP- Information System Security Professional
- OUSD (I&S)- Office of the Under Secretary of Defense for Intelligence and Security
- PAC- Package Approval Chain
- PDS- Protected Distribution System
- POA&M/POAM- Plan of Actions and Milestones
- RAR- Risk Assessment Report
- RMF- Risk Management Framework
- SCA- Security Controls Assessor
- SCAP- Security Content Automation Protocol
- SCG- Security Classification Guide
- SLCM-System-Level Continuous Monitoring

Questions

?