Risk Management Framework (RMF) Frequently Asked Questions (FAQ) June 2020

COMMON CONTROL PROVIDER (CCP)

1. **Question**: Can the process for NAO approved common controls be elaborated on? Is there a specific way to submit common controls?

   Answer: Yes. Industry users can submit a Common Control Provider (CCP) plan in the National Industrial Security Program (NISP) instance of Enterprise Mission Assurance Support Service (eMASS) and request authorization to allow systems to inherit the common controls. A CCP plan will enable a company to document their common controls. This will ensure consistency and streamline assessment and authorization processes. The CCP plan will be 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 or in hybrid fashion. The CCP plan will require reauthorization when common controls are modified or added. These controls cannot be inherited on any authorized system until authorization is granted by the Authorizing Official (AO).

   The requirements for the CCP plan are the same as other system security plans. Organizations will be required to address system details, control information [Implementation Plan, System Level Continuous Monitoring (SLCM)], test results [all control correlation identifiers (CCI)/assessment procedures (AP)], and upload all associated artifacts. Security controls that will not be addressed in the CCP plan will be marked as Not Applicable. In addition, organizations must include a digitally signed document detailing the commercial and government entity (CAGE) codes and locations of the facilities authorized to inherit from the CCP. This document will be used as a supporting artifact and will be uploaded into the Artifacts tab.

   The CCP plans created for a single location will be assigned to their local Defense Counterintelligence and Security Agency (DCSA) field office and the appropriate Regional Authorizing Official (RAO). If the CCP plan covers more than one facility within a region, Industry will contact their local Information Systems Security Professional (ISSP) to determine the appropriate field office assignment. If the CCP plan covers all DCSA regions, the plan will be assigned to the NISP Authorization Office (NAO) Headquarters staff and authorized by the NAO Office.

2. **Question**: During a presentation in March, you indicated the NAO would evaluate creating common controls based on the DAAPM that contractors could inherit. Has your office considered this request, and did it merit further action?

   Answer: Yes, the NAO is currently evaluating this request. We do not expect any decision before FY21.

3. **Question**: Is DCSA seeing many CCP packages being submitted by Industry?

   Answer: No. Industry has submitted a few CCP plans at both the local and national level.

4. **Question**: Are CCP packages and/or control inheritance allowed to be leveraged across different companies?

Answer: No. The security controls in a CCP plan can be inherited only within companies depending upon how the containers are built and limited to the container chain.

5. **Question**: If a company submits a CCP to the NAO, will this be reviewed and have the potential to be approved? Can the process be elaborated on?

   Answer: Reference #1.

6. **Question**: If a nation-wide company establishes over-arching policies and procedures that are applicable to all of its locations, can that be published as common controls set for inheritance by each locale?

   Answer: Reference #1.

7. **Question**: Is there a procedure defined for Industry for submitting a CCP (packages) for an organization at a corporate level for policies and procedures? Does an organization have to have a physical system registered in eMASS? Access only?

   Answer: Reference #1.

8. **Question**: Can PDS approval be part of the CCP or must be done with the assigned ISSP?

   Answer: PDS will be completed by the local assigned ISSP and approvals will be for a single facility only.

9. **Question**: If a CCP is approved by the NAO through eMASS for a contractor that spans all regions, will regional AOs and ISSPs "honor" that NAO approval?

   Answer: Yes, the NAO Office is a DCSA AO. Once the CCP plan is granted an authorization, the controls can be inherited by the CAGE codes listed in the plan.

10. **Question**: Does the CCP package have to be associated to a particular contract/DD Form 254 for the initial submittal, or can it be done ahead of required packages? Also, is it tailored specific to ISOL / P2P / multi-user standalone (MUSA) packages?

    Answer: No. The CCP package does not have to be associated to a particular contract/DD Form 254 for the initial submittal. CCP must be implemented in the same manner.

11. **Question**: If a Contractor has several facility locations, should a common control package be submitted to regional ISSPs before submitting to NAO?

    Answer: The answer depends on where the facilities are located. If all facilities are in the same region, i.e., the facility (CAGE code) specific common control packages should be reviewed by the regional staff. If the facility is corporate (covers multiple CAGE codes across all regions) the CCP should be submitted to NAO.

AUTHORITY TO OPERATE

12. **Question**: Can an approved plan in eMASS be transferred from one CAGE code to another?

    Answer: Yes, but only under limited circumstances. An authorized plan can only be transferred to another CAGE code within eMASS when the facility’s classified operations, including authorized systems, are officially transferred to a different CAGE code [example: Facility A (CAGE code 12345) is merging with Facility B (CAGE code 54321) and all classified operations will fall under CAGE code 54321]. Industry will follow the Transferring Systems in the NISP eMASS Job Aid located on the eMASS [HELP] page. Prior to conducting the actions detailed in the Job Aid, Industry is required to work with their assigned ISSP who will advise on the National Industrial Security Program Operating Manual (NISPOM) requirements that must be met prior to conducting the transfer.

13. **Question**: Why isn't there a process to buy a fully RMF accredited system for single user stand alone and MUSA. Of course, there would be some information that would need to be added but it would be minimal. This would speed up the process and reduce the cost for industry.

    Answer: DCSA will not consider a process to allow industry to buy or obtain through other means an RMF authorized system. One of the tenets of maintaining an authorized system is the level of experience of the ISSM. If an ISSM if not capable of identifying the RMF requirements, DCSA would be concerned of the ability to adequately manage and monitor the system.

14. **Question**: Will any authorization inspections be done remotely for IS that are unclassified prior to authorization?

    Answer: DCSA may consider authorization based on scan results. DCSA does not have the ability to access systems remotely at this time.

15. **Question**: Will DCSA still support authorizing new wide area networks that are required without being able to conduct an on-site?

    Answer: DCSA may consider waiving on-sites on a case by case basis. Reference #14.

16. **Question**: Do you have any idea when DCSA will be able to conduct onsite reviews? Any idea when this will change?

    Answer: Currently, DCSA is under COVID-19 restrictions and the time frame to resume on-sites has not been determined.

17. **Question**: We have a system that being registered into eMASS for the first time, and authority to operate (ATO) deadline is July 26. Will we get an extension for our ATO?

    Answer: The assigned ISSP is in the best position to provide advice on specific authorization actions or specific systems.

18. **Question**: Are there going to be any ESU extensions due to COVID-19?

    Answer: No. Microsoft Windows 7 ESU extensions will not be granted past December 31, 2020.

19. **Question**: We have completed the Bulk Processing feature in eMASS to submit all controls to the ISSP for review. How long before they review?

    Answer: The assigned ISSP plus their field and Regional leadership are in the best position to advise companies on the project quality of their submissions, specific timelines and workload projections.

ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (eMASS)

20. **Question**: Our Government Customer doesn't want the systems information in eMASS for classification reasons. What do we need to have from the Government customer so that this is not an issue for security vulnerability assessments/reviews?

Answer: If system vulnerabilities are deemed classified by the Government customer/information owner, it should be documented in the security classification guide (SCG). Instructions are provided in the NISP eMASS Industry Operation Guide for addressing vulnerabilities determined to be classified.

21. **Question**: Are we going to be loading POAM entries into eMASS? Would there be any concern with loading all those entries into a single system that could potentially be compromised? Even if POAM entries are unclassified, it seems like this could be problematic.

Answer: The NISP instance of eMASS requires a plan of action and milestones (POA&M) item for Non-Compliant 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.

22. **Question**: The Industry Operation Guide references a DCSA overlay, but in eMASS it's still "DSS" - are they the same?

Answer: Yes, the overlays are the same. NAO is working with the Defense Information Systems Agency (DISA) to update the overlay name.

23. **Question**: Will ISSO-type containers be created in eMASS for ISSOs to aid in the CM process?

Answer: No. For clarification, the NISP eMASS containers are based on CAGE codes. Your question is related to roles. The roles available in eMASS are determined by the application owner, DISA. The only roles available to Industry are Information Assurance Manager (IAM), Artifact Manager, and View Only. The IAM role provides the ability to register systems, build security plans, edit security controls, and submit for review in the CAC. Artifact managers have view-only permissions but can also create, edit, and delete artifacts related to an assigned system. The View Only role provides view only permission for the assigned system.

24. **Question**: The job aid for transferring systems appears to have a very limited scope, could the transfer function also be used by a centralized company location that builds and accredits classified systems, then transfers and deploys them to other company locations?

Answer: No, the Transferring System Job Aid was written to be specific and should only be used when a facilities classified operations, including authorized systems, are being transferred to another CAGE code. As stated in the Job Aid, Industry must work with their assigned DCSA representatives prior to performing any action in order to ensure all NISPOM requirements are met.

25. **Question**: Our company has multiple locations with multiple CAGE codes. Can I access eMASS instances for systems created by the ISSM at our other location? Currently, I can only see systems in eMASS that I have created within my own CAGE code.

Answer: In the NISP eMASS instance, containers are created based on CAGE codes. In order to view systems under additional CAGE codes, an Industry user must first have access to the applicable eMASS container/CAGE code. Industry users can request to modify an existing user account by following the guidance in Section 3.1 of the NISP eMASS Industry Operation Guide. In addition to having access to each applicable eMASS container/CAGE code, an Industry user must be assigned to a system. Roles are assigned to systems during “New System Registration”. If a user needs to be assigned to a system, the IAM associated with the system will need to conduct the following:

- Select the System
- Click the Management Tab
- Select Personnel
- Click Edit in the CAC/Package Approval Chain (PAC)
- Select the applicable users in the IAM Available Users column and drag to the Assigned Users list box

Reference the NISP eMASS Industry Operation Guide Version 1.1 located on the eMASS [HELP] page.

TRAINING

26. **Question**: Is instructor-led eMASS training available?

    Answer: Instructor led eMASS training is provided by DISA and some commercial vendors for a fee.

27. **Question**: Is there any DCSA or STEPP training courses to help us learn more about the RMF process? I’m aware that Udemy does offer some courses that are available for a fee.

    Answer: Center for Development of Security Excellence provides an on-line RMF course for ISSMs/ISSOs.

28. **Question**: Can you provide a recommendation for training materials or a class that would be an executive summary type training delivered to senior management that covers RMF, eMASS, and CMMC that covers the complexities and requirements?

    Answer: NAO does not make training recommendations. DISA eMASS training must be accomplished in order to obtain a NISP eMASS account and NAO provides a link to that training. Industry users also have the option of designing and building their own training using NAO products, tools, and artifacts.

MISCELLANEOUS

29. **Question**: Due to the amount of data that has to go into both spreadsheets, is there any possibility that the two workbooks could be combined? Test results are similar to Comments and SLCM comments.

    Answer: No. The information entered in the Control Information and Test Results templates are NOT the same. These templates were customized by DISA to support the eMASS RMF workflow process. Each template has unique values that are critical in supporting Assessment and Authorization (A&A) activities.

30. **Question**: I've started this process recently - my executives would like to know how many man hours we should expect it to take to submit a package for one MUSA?

Answer: The time necessary to complete submission of an RMF package in eMASS heavily depends on the skill set of the individual performing the task and the proficiency the individual has with the eMASS tool. Creation, preparation, and submission of a complete RMF package in eMASS can be efficiently streamlined by organizations leveraging the CCP option. A CCP is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (e.g., security controls inherited by systems). Industry is strongly encouraged to leverage CCP to significantly reduce the time necessary to submit eMASS packages. Training for the eMASS tool is available at https://www.dcsa.mil/mc/ctp/tools/ and https://rmfks.osd.mil/rmfresources/eMASS/CBT/index.html

31. **Question**: During a presentation in March, you stated the NAO would be releasing guidance that system upgrades from Windows 7 to Windows 10 would NOT need AO reaccreditation or a full eMASS package submission. Has that guidance been released?

    Answer: No. Contact your assigned ISSP for guidance regarding upgrading from Windows 7 to Windows 10 and any required authorization actions.

32. **Question**: Is there written guidance that indicates how to complete/submit a re-authorization package for a system that was previously authorized in the Office of the Designated Approving Authority (ODAA) Business Management System (OBMS)?

    Answer: Yes. The process for submitting a system authorized within OBMS for re-authorization within eMASS is the same as submitting a new system for authorization, and is described in full within the NISP eMASS Industry Operation Guide Version 1.1, located here: https://www.dcsa.mil/Portals/91/Documents/CTP/tools/NISP%20eMASS%20Industry%20Operation%20Guide%20Version%201.1.pdf

    NOTE: Pay special attention to the "System Information" process within the NISP eMASS Industry Operation Guide Version 1.1, as this is where the current authorization information will be entered. If the system was manually migrated from OBMS to eMASS and already has an eMASS system record, the re-authorization process will still be the same as for a new system, minus creation of a new eMASS system record.

33. **Question**: Can you please detail the process for approving Hibernation beyond 180 days?

    Answer: Hibernation beyond 180 days is permitted only with AO approval. Contact your assigned ISSP to determine requirements to obtain AO approval for the hibernation request.

34. **Question**: For a single laptop computer that will have multiple users (MUSA) is there a streamline process?

    Answer: No. A single laptop with multiple users falls under the "MUSA" category and must address all security controls within the Moderate-Low-Low baseline and "MUSA" Overlay. See the NISP eMASS Industry Operation Guide Version 1.1, section 5.2 (Categorization).

35. **Question**: At the spring Computer-Assisted Information Support System Working Group (CAISSWG), you announced that DCSA would soon be releasing a memo allowing Industry to upgrade their systems from Windows7/WinServer 2008 to Windows 10/WinServer 2016 WITHOUT seeking reauthorization. What is the status of this?

Answer: DCSA has not yet released a memo. Please contact your assigned ISSP for guidance regarding upgrading from Windows 7 to Windows 10 and any required authorization actions. Reference #31.

36. **Question**: Is DCSA responsible for A&A for DFARS 7012 or NIST 800-171?

Answer: No.

37. **Question**: I thought DCSA was responsible for assessing/inspecting controlled unclassified information (CUI) data. Now that Cybersecurity Material Model Certification (CMMC) is required, are they no longer responsible for CUI data or is another agency responsible for it?

Answer: Currently, DCSA is not responsible for CUI assessments.

38. **Question**: How does DCSA define/determine the demarcation for corporate system compliance for companies that have cleared and uncleared business units that share enterprise IT infrastructure for functions like Human Resources (HR), Accounting, etc.?

Answer: DCSA does not have cognizance for industry owned and operated unclassified human resource management systems or unclassified corporate accounting systems. Industry enterprise IT infrastructure that stores, transmits, processes, or receives CUI must comply with the security requirements defined in the contract with the government contracting authority (GCA) and information handling procedures defined by the government information owner of the data.

39. **Question**: I've been working a document with our sponsor to get SIPRnet for our company as own/operate, and we are first filling out a template provided online and a PowerPoint. Is that still accurate or should the process for SIPR start on eMASS?

Answer: The first step in the process to receive authorization to operate a SIPRNet circuit in an industry facility is approval from the DoD Chief Information Officer (CIO) Mission Partner Validation Office. This office requires the government sponsor of the SIPRNet circuit to submit a Mission Partner DISN Connection request package. This package consists of a PowerPoint questionnaire and DoD Contractor DISN Validation memo. After a complete Mission Partner DISN Connection request package is submitted by the government sponsor to the DoD CIO Mission Partner Validation Office, that office issues an approval or denial letter for connection to SIPRNet. The DoD CIO Mission Partner Validation approval letter is a required artifact in the eMASS package submission to request authorization of a SIPRNet circuit in an industry facility.

40. **Question**: Some regions require ISSPs to STIG their isolated systems. This seems to be in conflict with earlier NAO guidance. Are isolated systems required to be STIG'd?

Answer: No. The security requirements for processing government owned information on isolated systems at industry facilities should be defined in the contract with the government customer. If the government customer states in the terms of the contract, contract security classification specification (DD Form 254) and/or other security guidance that systems processing the government owned data must be in compliance with Security Technical Implementation Guide (STIG) requirements; then the isolated system must be configured in compliance with STIG requirements. If the contract documents listed above do not state the isolated systems are required to be in compliance with STIG configuration requirements, then it is not necessary to configure the system for compliance to STIG configuration requirements.

41. **Question**: You indicated NAO systems did not have to be STIG'd but certain tools used in the process leverage the STIG. The tool that comes immediately to mind is the SCAP. Is there wiggle room here for an ISSP decision to mandate STIGs?

Answer: No. Security Compliance Automation Protocol (SCAP) tools automate the process of validating the technical security configuration of a computing asset. Manually reviewing the technical security configuration of a computing asset is extremely resource intensive and can consume many hours of time. Leveraging a SCAP tool significantly reduces the time required to review the technical security configuration of a computing asset. Automating actions which are manually resource intensive reduces the overall time required to authorize a system to process classified information. Please review the answer to question 40 regarding STIG compliance.

42. **Question**: Is the SCAP tool required for a Secret MUSA?

Answer: No. There is no policy-based requirement for industry to utilize the SCAP tool on authorized information systems. If the SCAP tool is present on the system, it will be utilized by DCSA personnel conducting Security Control Assessor actions. If not, then a complete manual review of all technical security controls and configurations will be required. As such, industry is highly encouraged to utilize the SCAP tool on all systems that support the application in order to expedite SCA review and package approval. The exception to the aforementioned position is if industry indicates use of the SCAP tool in the control implementation language of the system security package and thus makes the SCAP tool a requirement.

43. **Question**: Is there any update on an overlay from DCSA for a client/server isolated local area network Information System?

Answer: No. DCSA does not provide an overlay for Client/Server Isolated LAN systems (C/S ISOL). C/S ISOL systems will utilize the DCSA Baseline (M-L-L) Overlay within eMASS, and all security controls in the Moderate-Low-Low baseline must be addressed. See NISP eMASS Industry Operation Guide Version 1.1, Section 5.2 (Categorization).

44. **Question**: Are non-DODIN authorized systems required to go through the DSAWG for CDS approval?

Answer: Yes. DoD Instruction 8540.01 Cross Domain (CD) Policy, Section 2.a (2) specifically states the instruction applies to all cross domain capabilities to, from, within, or between DoD information systems (IS) to include mission partner information systems and defense contractor IS. DoDI 540.01, Section 8.u.(1) specifically states a Cross Domain Solution Authorization (CDSA) is issued by DoD Information Security Risk Management Committee (ISRMC) or Defense Security/Cybersecurity Accreditation Working Group (DSAWG) before allowing a CDS to access or transfer information between different interconnected security domains. A CDSA is required for use of a CDS. The CDSA is issued by ISRMC or the DSAWG.

45. **Question**: Do encryption passwords have to meet all password length, complexity, and history requirements?

Answer: Yes. The security controls and protection of encryption passwords must be commensurate with the classification level of the system the information being encrypted is processed on. For example, encryption passwords used to encrypt information being processed on a Collateral Secret level system must use the same length, complexity, and history requirements as the passwords used to access the Collateral Secret system.

46. **Question**: Can Karl please clarify for Industry how the passcode/password to encrypted media should be treated from a classification stand point?

    Answer: The security controls and protection of encrypted media passwords must be commensurate with the classification level of the system the information was extracted from. For example, encrypted media passwords used to encrypt information extracted from a Collateral Secret level system must be protected and safeguarded as Collateral Secret information. Reference #45.

47. **Question**: Follow up to the passcode/password question, are encryption keys for encrypting media (CD/DVD, etc.) treated at classification of the system? Could the encryption passphrase be treated as unclassified as long as it's handled separately from the media?

    Answer: The security controls and protection of encryption keys for encrypting media (CD/DVD, etc.) must be commensurate with the classification level of the information being encrypted on the media. For example, encryption keys used to encrypt Collateral Secret level information stored on a CD must be protected and safeguarded as Collateral Secret information. The encryption keys used to encrypt or decrypt classified information cannot be treated as unclassified information.