MARINE CORPS SYSTEMS COMMAND

SYSTEMS ENGINEERING, INTEROPERABILITY, ARCHITECTURES AND TECHNOLOGIES

RISK MANAGEMENT FRAMEWORK PROCESS GUIDE

Version 1.0
25 May 2016

CLEVENGER.JIMMY.M.1131133380

Digitally signed by CLEVENGER.JIMMY.M.1131133380
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USMC, cn=CLEVENGER.JIMMY.M.1131133380
Date: 2016.10.06 08:49:52 -04'00'

Jimmy Clevenger
Director Systems Security Engineering Division
Systems Engineering, Interoperability, Architectures and Technologies (SIAT)
Marine Corps Systems Command

THIS PAGE IS INTENTIONALLY LEFT BLANK.

RECORD OF CHANGES

The table below identifies revisions to this document. The version number, date, and description of change for each revision are noted in the table.

Version Number	Date of Issue	Section(s)	Change Code*	Brief Description of Revision

*__A__ – Added **M** – Modified **D** – Deleted

Direct any questions and concerns about this guide to the Marine Corps Systems Command SIAT Systems Security Engineering Division, Cybersecurity Engineering Branch. People submitting comments should complete the comment resolution matrix (Appendix L) and send it to SIAT SSE via the C&A Manager ticketing system.[1]

[1] https://mcscviper.usmc.mil/sites/SIAT/Architecture/CE/CAM/SitePages/Home.aspx

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

DoD Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), implements the RMF for DoD IT, adopts the related National Institute of Standards and Technology (NIST) RMF guidelines, and provides the framework to manage life-cycle cybersecurity risk to DoD IT. The RMF uses a risk-based cybersecurity approach for authorization of IT systems and services. The RMF establishes and enforces a tailored set of security controls, and focuses on security as an integral part of a system's overall lifecycle.

1.1 Purpose

This guide describes Marine Corps Systems Command's (MCSC) processes to properly manage the risk of US Marine Corps (USMC) IT in accordance with the DoDI 8510.01 (reference (a)), taking into account USMC-unique operational and environmental needs. This guide also establishes the roles and responsibilities for RMF stakeholders and provides USMC Program Managers and the cybersecurity workforce with a practical guide for implementing RMF to facilitate Assessment and Authorization (A&A) and to operate IT with an acceptable level of risk.

This guide is not intended to duplicate existing NIST and DoD policy, directives, or guidance beyond what is required to define the MCSC process for RMF A&A. As this process evolves, SIAT SSE will update this guide.

1.2 Scope

The MCSC RMF Process Guide provides an overview and a process for MCSC IT to be assessed and authorized for MCSC IT that will receive, process, store, display, or transmit DoD information at the secret and below levels. These technologies are defined by the DoD as Information Systems (IS); Platform IT (PIT), including its sub-categories of PIT components, PIT systems, and standalone PIT systems; IT services; IT products; and stand-alone systems. (The USMC has chosen not to classify any of its DoD IT as PIT.) This guide also describes the roles and responsibilities of the stakeholders in the six steps of the RMF process. It is written for users with a basic knowledge of USMC cybersecurity and A&A, and can help the cybersecurity workforce with the concepts and requirements incorporated into the Marine Corps Certification and Accreditation Support Tool (MCCAST).

Consistent with the DoD RMF policy, the USMC will require an Information System Continuous Monitoring (ISCM) Strategy as part of every IT's Security Authorization Package, which section 4.2.3 addresses. The monitoring strategy describes the plan to continuously monitor the effectiveness of security controls employed within or inherited by the system and to monitor changes to the system and its operational environment. A DoD directive on ISCM is forthcoming, and as the USMC defines its ISCM requirements, this information will be incorporated into the guide.

The initial release of this process guide is limited to the process steps that will enable A&A under RMF, given the constraints associated with the current USMC operating environment. Future releases of this guide will include additional expansion of the RMF process as it applies to

the USMC. This guide, along with the USMC Enterprise Cybersecurity Directive (ECSD) 018 (reference (m)) and the MCCAST training guidance, forms the authoritative source to implement the RMF process within Marine Corps Systems Command.

1.3 Background

DoDI 8510.01 and DoDI 8500.01 (references (a) and (b), respectively) define the transition from Certification and Accreditation (C&A) under the DoD Information Assurance Certification and Accreditation Process (DIACAP) to the RMF A&A process. These DoD instructions point to compliance with overarching Federal guidelines, including the Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems (reference (c)); Federal Information Processing Standard Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems (reference (f)); and multiple NIST Special Publications 800 series.

While RMF for DoD IT provides a framework for achieving A&A, it leaves several key implementation aspects to the DoD components to define. Examples of component-specific details include the following:

- Roles and responsibilities
- Process for assessing IT services and IT products for inclusion in authorization boundaries
- Identification of common controls that are component-wide, or applicable to a subset of the components, and how those controls may be inherited
- Process for inter/intra-component reciprocity, using a centralized Authorizing Official (AO)
- Definition of risk tolerance levels
- Assignment of organizationally defined control values

1.4 How to Use This Guide

This guide provides a two-part approach to presenting the RMF process. The first part depicts the overall RMF process in a single Responsible, Accountable, Supportive, Consulted, and Informed (RASCI) table, Table 4-1. The table gives a high-level outline of the six steps of RMF according to the USMC approach to the A&A. The reader will gain an understanding of the minimum activities required for the RMF process. The second part will then explain in more detail what happens during each step, who is responsible, what tools should be used, and what the input and output expectations are for each RMF step.

The remainder of this guide is devoted to an in-depth discussion of the major areas and deliverables that comprise the RMF process and Security Authorization Package. These include the following:

- System Security Categorization
- Security Plan (SP)

- ISCM Strategy
- Security Assessment Plan (SAP)
- Risk Assessment Report (RAR)
- Security Assessment Report (SAR)
- Plan of Action and Milestones (POA&M)

The USMC RMF stakeholders should rely on the Headquarters Marine Corps (HQMC) Command, Control, Communications, and Computers (C4) C&A/A&A website[2] for the most up-to-date USMC-specific policy and guidance and the SIAT Cyber-Engineering Division website[3] for MCSC-related guidance. The RMF Knowledge Service (KS)[4] hosts wider DoD policy, and the USMC C&A/A&A portal may reference it as required to maintain consistency with the DoD's evolving policy and guidance.

Table 1-1 identifies the minimum documentation required to prepare a complete Security Authorization Package as required by RMF policy and includes an overview of the MCSC RMF Process Guide terminology. While this documentation should be generated by MCCAST, the tool's capability is still evolving to support the creation of all this RMF documentation. If MCCAST is not able to generate the specific RMF document in a USMC-approved format, an uploaded artifact in MCCAST will be accepted until such time as the tool can generate the necessary RMF documentation. Specific guidance will be provided to the cybersecurity workforce via meetings and emails.

Table 1-1: RMF Required Documentation

DoD RMF Term	Description	USMC Term (Acronym)	Reference
Security Authorization Package	The set of required documents developed for authorizing officials. The base package contains (1) the security plan, (2) the security assessment report, and (3) the plan of action and milestones. The security authorization documentation is maintained throughout a system's lifecycle, includes the authorization decision document, and is the minimum information necessary for the acceptance of an IS by a receiving organization.	Security Authorization Package	DoDI 8510.01; NIST Special Publication 800-37; RMF KS

[2] The HQMC C4 C&A/A&A site at https://eis.usmc.mil/sites/c4/cy1/default.aspx
[3] SIAT Cyber Engineering site at https://mcscviper.usmc.mil/sites/SIAT/Architecture/CE/SitePages/Home.aspx
[4] The RMF KS at https://rmfks.osd.mil

DoD RMF Term	Description	USMC Term (Acronym)	Reference
Security Plan	Provides an overview of the security requirements for a system and describes the security controls in place or planned for meeting those requirements and implementation status.	Security Plan (SP)	DoDI 8510.01; NIST Special Publication 800-37, 800-18; RMF KS
Security Assessment Plan	Describes the objectives of the security control assessment and provides a detailed roadmap for conducting the assessment.	Security Assessment Plan (SAP)	NIST Special Publication 800-53A; RMF KS
Security Assessment Report	Describes the results of the security control assessment to determine the effectiveness of the security controls employed within or inherited by the information system, including recommendations for correcting any weaknesses in the controls.	Security Assessment Report (SAR)	NIST Special Publication 800-37; RMF KS
Risk Assessment Report	Provides risk assessment of Non-Compliant (NC) security controls and addresses vulnerabilities displayed in the SAR after the security control assessment has been completed.	Risk Assessment Report (RAR)	RMF KS
Plan of Action and Milestones	Addresses the residual vulnerabilities in the system. The POA&M lists the tasks to be accomplished, resources required, milestones for meeting the tasks, and scheduled completion dates for the milestones.	Plan of Action and Milestones (POA&M)	SIAT CE C&A website; RMF KS

2 USMC RMF ROLES AND RESPONSIBILITIES

Dedicated and qualified personnel are the most important aspect to ensure USMC systems adequately implement RMF cybersecurity requirements. This section describes the roles, responsibilities, and required qualifications for each role under the USMC RMF process.

Table 2-1 identifies the USMC-assigned RMF roles by appointment, consistent with DoDI 8500.01 (reference (b)), as well as the MCSC RMF Process Guide terminology for each role. MCCAST identifies these roles as stakeholders.

Table 2-1: MCSC RMF Roles/Stakeholders

DoD RMF Role	USMC Term	Appointed By[5]
Authorizing Official (AO)	AO	USMC Chief Information Officer (CIO)
-----	AO Cybersecurity Analyst (AO CSA)	AO
DoD Component Senior Information Security Officer (SISO)	SISO	Department of Navy (DON) CIO
Security Control Assessor (SCA)	SCA	AO
-----	SCA Analyst	SCA
-----	Security Control Validator (SCV)	AO
-----	Information Owner (IO)	<Program-specific>
Program Manager (PM)	PM	CG Marine Corps Systems Command
-----	Information System Security Engineer (ISSE)	<Program-specific>
Information System Security Manager (ISSM)	ISSM	SCA
Information System Security Officer (ISSO)	ISSO	ISSM
User Representative (UR)	UR	CG Marine Corps Combat Development Command (MCCDC)

[5] *Appointed by* is the authority who appoints the individual to the role.

2.1 RMF Personnel Qualifications

The PM for the system being assessed is responsible for identifying the RMF stakeholders within MCCAST. For roles assigned by the PM, qualified cybersecurity support personnel must be identified (e.g., SCVs fully qualified by the AO). Personnel serving in RMF roles must meet the suitability and fitness requirements established in DoDI 5200.02 (reference (d)). RMF personnel must also meet the cybersecurity workforce qualification standards in accordance with the latest DoD and USMC policy. (Refer to ECSD 024 (reference (u)) for the USMC cybersecurity workforce standards.) Personnel supporting RMF should have a commitment to and knowledge of the system(s) to which they are assigned. The PM must ensure RMF activities are planned and resourced for continued cybersecurity sustainment throughout the system lifecycle.

2.2 Role Descriptions

The following role descriptions briefly describe the USMC RMF stakeholder responsibilities as they relate to RMF. USMC ECSD 018 (reference (m)) is the authoritative source with more details of USMC cybersecurity roles and responsibilities and other specific qualifications required for stakeholder roles.

2.2.1 Authorizing Official (AO)

The USMC has one Service AO who is responsible for implementing the RMF. The USMC CIO is responsible for appointing the AO. The AO function is resident in HQMC C4 Cybersecurity Division.

The AO is responsible and accountable for system-related security risks. The AO makes an authorization decision based on the system-related security risks that may impact organizational operations and assets, individuals, other organizations, or the nation.

The AO has the following cybersecurity responsibilities:

- Performing all required and approved AO RMF process steps discussed in Section 4 of this guide
- Making a risk-based authorization decision for systems to operate in the USMC
- Rendering a final determination of risk to DoD operations and assets, individuals, other organizations, and the nation from the operation and use of the system
- Making a risk-based authorization decision to accept and use a DoD system through cybersecurity reciprocity, promoting reciprocity to the maximum extent possible
- Making a risk-based authorization decision for cloud solutions that meet the NIST definition of cloud computing and are subject to cloud policy (e.g., Federal Risk and Authorization Management Program).
- Approving system security categorizations and final security control sets for systems
- Establishing guidance for and overseeing system-level risk management activities
- Approving the SP, SAP, and system-level ISCM Strategy submitted by the PM and establishing reauthorization requirements based on the ISCM Strategy

- Monitoring and tracking overall execution of POA&Ms
- Establishing minimum qualifications for SCVs
- Authorizing SCVs per USMC-established requirements
- Issuing Authorization to Operate (ATO) (and Authorization to Connect [ATC] to the Marine Corps Enterprise Network [MCEN]); Interim Authorization to Test (IATT); Interim Authority to Build (IATB); or Denial of Authorization to Operate (DATO) for every system assessed and authorized through the RMF process
- Appointing RMF stakeholders as identified in Table 2-1.

2.2.2 Authorizing Official Cybersecurity Analyst (AO CSA)

To perform the AO function in the most efficient manner, the USMC will use a team of AO Cybersecurity Analysts (CSAs) to assist with AO responsibilities. AO CSAs reside in HQMC C4 Cybersecurity Division and report directly to the AO.

The AO CSA has the following cybersecurity responsibilities:

- Reviewing and concurring with system security categorization decisions
- Reviewing final security control sets for DoD systems and providing recommendation to AO
- Reviewing the SP and system-level ISCM Strategy submitted by the PM and providing recommendation to AO
- Ensuring RMF process steps are followed and adhered to by RMF stakeholders
- Establishing and/or providing guidance to RMF stakeholders on RMF processes and procedures
- Ensuring AO authorization decisions are supported by sufficient documentation and risk assessments
- Ensuring authorization recommendations comply with higher level policy as defined by DoD/USMC policy
- Providing technical analysis of RMF artifacts to inform the authorization decision, in support of the AO

2.2.3 Security Control Assessor (SCA)

The MCSC SCA provides oversight and technical expertise to conduct RMF assessment activities throughout a system's lifecycle. Assessment activities are based on security requirements outlined in DoDI 8510.01 and ECSD 018 (references (a) and (m), respectively). For MCSC, the Director SIAT, System Security Engineering (SSE) Division is the MCSC SCA.

The SCA maintains oversight of the cybersecurity risk assessment process within the overall RMF A&A process, assists with the assessment of the security controls, and certifies the residual risk in support of an RMF authorization. To determine the overall effectiveness of the security controls, the SCA conducts an independent, comprehensive assessment of the managerial,

operational, and technical controls employed within or inherited by a USMC system (i.e., an independent verification and validation). To help perform the SCA function, the USMC uses SCA Analysts and SCVs to assist with SCA responsibilities.

The SCA has the following cybersecurity responsibilities:

- Performing SCA RMF process steps, as provided in Section 4 of this guide
- Assessing and quantifying aggregate cybersecurity risk
- Documenting the SCA's determination of compliance with the assigned security controls
- Conducting a threat and vulnerability-based cybersecurity risk assessment. The risk assessment evaluates threats, vulnerabilities, and potential impacts as well as existing and planned risk mitigation. The risk assessment must address the impact of all NC controls, and must clearly communicate the SCA's conclusion on system cybersecurity risk, and any recommendations for special instructions to accompany the authorization decision.
- Preparing the RMF risk determination via the SAR, and making a recommendation to the AO for system authorization
- Preparing the SAR Executive Summary as the final and official document that certifies the risk as part of A&A
- Providing guidance on the MCSC RMF process, in alignment with USMC RMF guidance
- Supporting DoD and USMC continuous monitoring requirements
- Appointing RMF stakeholders as identified in Table 2-1.

2.2.3.1 SCA Analyst

The SCA has a team of analysts to help execute the SCA responsibilities. The SCA Analyst will act as the SCA's representative and will interface with the PMs, ISSMs/ISSOs, ISSEs, SCVs, as directed. The SCA Analyst should be considered a risk assessment subject matter expert and provide support and assistance in the A&A effort.

The SCA Analyst has the following cybersecurity responsibilities:

- Assisting the SCA in executing SCA RMF process steps, as provided in Section 4 of this guide
- Assessing technical and non-technical security features of a system to address known threats and vulnerabilities. The analyst must consider and identify impacts as well as consider existing risk mitigation strategies.
- Acting as an independent and impartial assessor to determine and certify aggregate cybersecurity risk for recommendation to the SCA
- Reviewing the SAP for quality assurance and providing initial concurrence on behalf of the SCA for the SAP, and ensuring all appropriate security controls were assessed for compliance

- Providing SAR analysis to the SCA and the PM
- Auditing RMF authorization packages
- Ensuring RMF A&A packages are correctly entered into MCCAST
- Guiding SCVs with the following:
    - Understanding of the RMF risk assessment process
    - Applicability of security controls
    - Use of appropriate test procedures and tools
    - Recommending mitigation measures for specific vulnerabilities
    - Completing residual risk assessment
    - Traceability of test results to system components and the risk assessment, as reflected in the relevant RMF documentation
    - Understanding of cybersecurity policies and the effects of specific policies to the risk of a system

2.2.4 Security Control Validator (SCV)

The SCV, who is appointed by the AO, is an independent[6] third party assessor who verifies and validates the system has implemented the approved security control baseline. The SCV acts as a trusted agent to the SCA; so while the PM funds the SCV, the SCV must remain independent of the design or development of the system in order to conduct an impartial assessment. The SCV should use the SCA Analyst as an advisor to assist in all matters of validation, documentation, vulnerability mitigation, and residual risk determination.

A program management office may hire a government or contractor support to act as the SCV for that program management office's portfolio. However, that SCV must meet the definition of independence as shown in the footnote below.

SCVs must complete the USMC validator training requirements, which include the following, before they are added to the AO-approved list of SCVs:

- HQMC C4 Cybersecurity Cyber Assessment Methodology Course
- CNSSI 4016 Risk Management
- MCCAST training
- Information Assurance Technical Level II (or greater)

The SCV has the following cybersecurity responsibilities:

- Performing all required and approved SCV RMF process steps, as provided in Section 4 of this guide

[6] The term "independent" in this context means the validator is free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system. (See NIST SP 800-53A, Section 3.1.)

- Preparing and submitting the SAP with program assistance
- Assisting with required MCCAST data entry requirements
- Conducting a complete security control assessment of technical and non-technical security features of a system to address known threats and vulnerabilities. The assessment must identify impacts and consider existing risk mitigation strategies.
- Completing a SAR in conjunction with the ISSM based on the security control assessment results
- Developing the initial RAR and POA&M based on the assessment results. For a security control assessment, the SCV will complete those portions of the POA&M to identify weakness, affected device, raw CAT, control, mitigated CAT, mitigation, source identifying weakness, status and comments.
- Ensuring traceability of all vulnerabilities from raw assessment results to the POA&M
- Conducting required vulnerability analysis to support mitigation and residual risk determination
- Completing the SAR Executive Summary, with all assessment results, for SCA Analyst review and SCA certification and signature
- Coordinating with the SCA Analyst in all matters of risk determination should questions or issues occur
- Supporting the execution of the continuous monitoring strategy to support continuing authorization requirements or ongoing authorizations

2.2.5 Program Manager (PM)

The PM represents the interests of the system throughout its lifecycle (acquisition, lifecycle schedules, funding responsibility, system operation, system performance, and maintenance). The PM leads the organization that has been assigned system lifecycle management and ensures the appropriation of funds to support cybersecurity standards through the lifecycle of the system. The PM integrates security requirements into the system solution, thereby ensuring an acceptable level of risk is maintained within the operational environment. This must be accurately documented in the RMF package.

Note: NIST Special Publication 800-37 Rev 1 (reference (g)) states the "Information System Owner (or Program Manager)" is the "official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system." However, DoDI 8510.01 (reference (a)) states the term ISO is not synonymous with PM as indicated in Reference NIST Special Publication 800-37. This guide uses the term PM.

The PM has the following cybersecurity responsibilities:

- Performing, or having a designated PM representative perform, all required and approved PM RMF process steps, as provided in Section 4 of this guide
- Implementing the RMF security controls for the PM's systems
- Enforcing AO authorization decisions for hosted, standalone, or interconnected systems

- Coordinating system security requirements, including inheritance agreements, with receiving organizations early and throughout system development to support reciprocity
- Complying with statutory law, such as (1) the Federal Information Security Modernization Act (FISMA), which is tracked in DITPR-DON, and (2) the Clinger-Cohen Act, of which the Cybersecurity Strategy is a component
- Assisting with development, maintenance, and execution of the SP
- Ensuring POA&M development, execution, and maintenance
- Assigning resources, milestones, resource funding, and estimated completion dates to the POA&M
- Implementing continuous monitoring in accordance with the ISCM Strategy
- Maintaining Information Assurance Vulnerability Alert (IAVA), Information Assurance Vulnerability Bulletin (IAVB), and Communications Task Ordering (CTO) compliance and reporting (reference (n)).
- Managing risk

2.2.6 Information Owner (IO)

The IO represents the end users of the system in the intended operational environment. As such, the IO has overall ownership of the information transmitted, processed, and stored by the system.

The IO has the following cybersecurity responsibilities:

- Performing all required and approved IO RMF process steps, as provided in Section 4 of this guide
- Assisting the user representative with system security categorization
- Maintaining the security posture of the fielded system in accordance with the ISCM Strategy and instructions from the PM

2.2.7 User Representative (UR)

The UR represents the operational interests of the user community and is the stakeholder who formally defines and clarifies requirements to ensure the IS meets the user needs. In the USMC this responsibility is fulfilled by MCCDC. The UR must provide cybersecurity requirements to the PM so that the A&A record is accurate and the development effort can properly integrate cybersecurity into the system lifecycle. The UR identifies any security controls that could potentially interfere with mission execution.

The UR has the following cybersecurity responsibilities:

- Performing all required and approved UR RMF process steps, as provided in Section 4 of this guide
- Providing input to the security control selection process

- Identifying the Defense-in-Depth Functional Implementation Architecture (DFIA) defense level at which the system resides
- Identifying the system security categorization
- Identifying the system's Cybersecurity Safety (CYBERSAFE) grade

2.2.8 Information System Security Manager (ISSM)

The ISSM is responsible for the planning and execution of the cybersecurity requirements of DoD IT and for ensuring adherence to the USMC RMF process. The ISSM must be a government employee or uniformed service member. The ISSM supports a PM in delivering a Program of Record (POR) with cybersecurity integrated throughout the system development lifecycle and for implementing RMF within the program. Often the ISSM will delegate authorities during A&A to an ISSO or ISSE, but the ISSM retains overall responsibility.

The ISSM has the following cybersecurity responsibilities:

- Performing all required and approved ISSM RMF process steps, as provided in Section 4 of this guide
- Supporting implementation of the RMF for assigned programs, organizations, systems, or enclaves
- Maintaining and reporting system's A&A status and issues
- Ensuring the SP is developed and maintained for assigned systems
- Supporting the PM for the continuous monitoring of assigned systems
- Performing annual security reviews, annual testing of security controls, and annual testing of the contingency plan to maintain FISMA compliance
- Managing POA&M entries and ensuring vulnerabilities are properly tracked and mitigated or remediated. Specific POA&M entries the ISSM will complete on the initial POA&M received from the SCV include POC, resources, scheduled completion date, and comments. Throughout the POA&M lifecycle, the ISSM will also update the status and comments.
- Assisting with identification of the security control baseline set and applicable overlays
- Managing cybersecurity testing
- Assessing the initial control set to ensure controls are properly documented for AO review
- Assembling the Security Authorization Package
- Registering the system in MCCAST
- Planning and performing cybersecurity testing to assess security controls and recording security control compliance status during sustainment
- Appointing RMF stakeholders as identified in Table 2-1.

- Ensuring personnel filling the ISSO or ISSE roles meet the cybersecurity certification requirements.

2.2.9 Information System Security Officer (ISSO)

The ISSO, who is appointed by the ISSM, assists the ISSM in the planning and execution of the cybersecurity requirements of DoD IT and for ensuring adherence to the USMC RMF process. Some ISSMs may appoint ISSOs to ensure the A&A activities are integrated into the project planning and executed as planned while the lead ISSM retains key decision-making authority.

2.2.10 Information System Security Engineer (ISSE)

The ISSE conducts information system security engineering activities on behalf of the ISSM to ensure cybersecurity is integrated into the IT during the acquisition lifecycle, to include post-deployment software support. The ISSE develops and maintains the cybersecurity architecture for the POR. If a project does not have an assigned ISSE, then the systems engineer for the program should function in the ISSE role.

The ISSE has the following cybersecurity responsibilities:

- Overseeing the development and maintenance of a system's cybersecurity solutions
- Ensuring cybersecurity requirements are fully developed and integrated into system acquisition design and configuration
- Supporting identification of the system type (IS, IT product, IT service) and any special considerations including multi-service/agency, joint, cross domain, Personally Identifiable Information (PII), protected health information, tactical, space, etc., to support RMF Step 1 System Categorization
- Applying the security control baseline set and applicable overlays
- Assisting with development and update of the cybersecurity documentation
- Leading the security control implementation and testing efforts
- Assisting with risk assessments for the system
- Assisting with any security testing required as part of A&A or annual reviews
- Assisting in the mitigation and closure of open vulnerabilities

3 AUTHORIZATION TYPES

As explained in DoDI 8510.01 (reference (a)), DoD IT varies greatly in size and complexity, from stand-alone hardware and applications to large computing environments and enclaves. Figure 3-1, taken from DoDI 8510.01, shows the classification breakout of DoD IT:

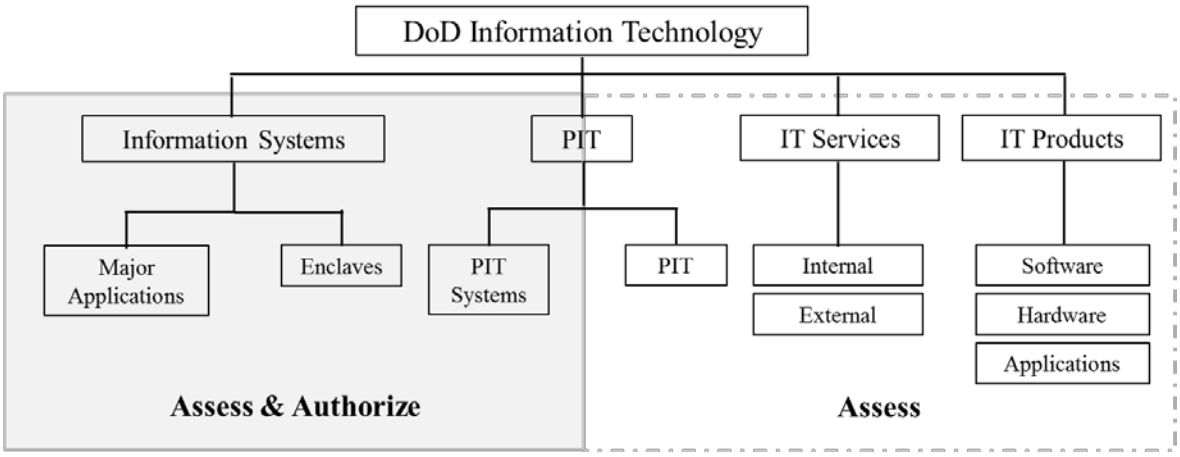

Figure 3-1: DoD IT Classification Breakdown

Of the four categories of IT shown in Figure 3-1, the USMC AO does not classify any IT as PIT.

USMC IT requiring authorization under the RMF methodology will fall under one of five authorization types, which are described in Table 3-1. ECSD 018 (reference (m)) provides more detail about each of the authorization types. It is important to note MCSC SIAT SSE Division processes the following authorization types: Major Application, which results in an authorization decision; Application, which results in a Marine Corps Certified Application (MCCA); and on rare occasions, Site authorizations. USMC programs processing for an MCCA will not implement many of the RMF steps; for example, there will be no need to identify the DFIA defense level or do security categorization.

Table 3-1: Authorization Types

Authorization Type	Description	Organizational Level of Applicability
Commercial Internet Service Provider (C-ISP)	The DoD considers commercial connections/networks as outsourced IT-based services, and these services must undergo assessment and authorization prior to use.	HQMC C4 Cybersecurity
Exercise	Organizations routinely conduct exercises at garrison or deployed locations, and this activity involves ISs that either already reside at the location or are deployed to that location. The exercise authorization type is very similar to a site authorization in that the ISs involved in an exercise are controlled by a single management authority, but for only a specified period of time.	HQMC C4 Cybersecurity
Application	An application is software fielded without hardware, but hosted on an IS. As such, it cannot be tested without having a representative IS in place. The goal of testing an application is to ensure it does not require modifications to its hosting system that could introduce additional risk to the MCEN. An application is assessed under the MCCA process. Refer to Appendix D for more about MCCA.	MCSC
Site	A site equates to an enclave, base, post, or station, whether in garrison or deployed. Site authorization is practical when different ISs are controlled by a single management authority within a well-defined physical location.	HQMC C4 Cybersecurity, MCSC
Major Application	An IS often consists of common hardware, software, and firmware. For MCSC, the AO authorizes a baseline system. The subsequent ATO allows the system to be fielded at one or more locations. For MCSC, tactical enclaves fall under this authorization type.	MCSC

MCSC uses the authorization types, as described above, to authorize ISs and applications developed within the USMC acquisition realm. If another service has authorized a system, the USMC could leverage the lead service's Security Authorization Package to complete a USMC assessment and authorization. The RMF calls this a leveraged authorization, and it follows the

DoD reciprocity agreement to use other services' system authorizations to the maximum extent possible.

Per the reciprocity section of DoDI 8510.01 (reference (a)), the USMC AO will evaluate the other component's security assessment and artifacts to assess potential risk. The AO could decide to either accept the risk as is or have the USMC implement more stringent (or more lenient) mitigations before allowing the system to operate.

Refer to Appendix C for more specific details on the MCSC approach to reciprocity.

Note: This guide uses the terms "system" and "application." The context of these terms follows the definitions from the DITPR-DON Policy Guidelines (reference (v)):

• A *system* is defined as any solution that requires a combination of two or more interacting, interdependent, and/or interoperable hardware, software, and/or firmware to satisfy a requirement or capability.

• An *application* is defined as any software application that uses an existing operating system software program to provide the user with a specific capability or function that is independent of other "applications." If it is dependent on other applications it becomes a system.

4 RMF PROCESS

This section provides an overview of the USMC process for the execution of the RMF assessment and authorization methodology. Figure 4-1 is the MCSC's high-level process flow for the six RMF steps. Table 4-1 identifies the stakeholders who are responsible, accountable, supporting, consulting, or informed for the fundamental activities in each RMF step. The color scheme for each block in the process flow pictured in Figure 4-1 indicates the stakeholder who is responsible for executing the action for the associated process block, per the definition of "Responsible" in Table 4-1. The "Responsible" stakeholder is acting under the authority of the "Authority" stakeholder. Sometimes the "Responsible" and "Accountable" stakeholder are the same.

The sub-sections give a more detailed description of each of the six RMF steps, the actions for the step, artifacts or products associated with the RMF step, entry and exit criteria for the step, and data that must be populated within MCCAST.

The sub-tasks for each RMF step do not have to be completed sequentially as depicted in the RMF Process Flow diagram (Figure 4-1). Some sub-tasks may occur simultaneously. Nor will all activities for a sub-task necessarily be completed before the next sub-task is started. For example, a program may know only some stakeholders at program initiation and may have to wait for some stakeholder assignments, such as the SCV.

The term *SCA* refers to the SCA team and comprises the SCA and the SCA Analysts. Likewise, the term *ISSM* includes ISSO and ISSE, whereby the ISSM could delegate action to the ISSO or ISSE in the execution of the sub-task. If the sub-task is specific to the ISSO or ISSE, then that position will be specifically cited. Finally, the term *PM* refers to the program manager and anyone on his or her staff designated to fulfill program-related duties.

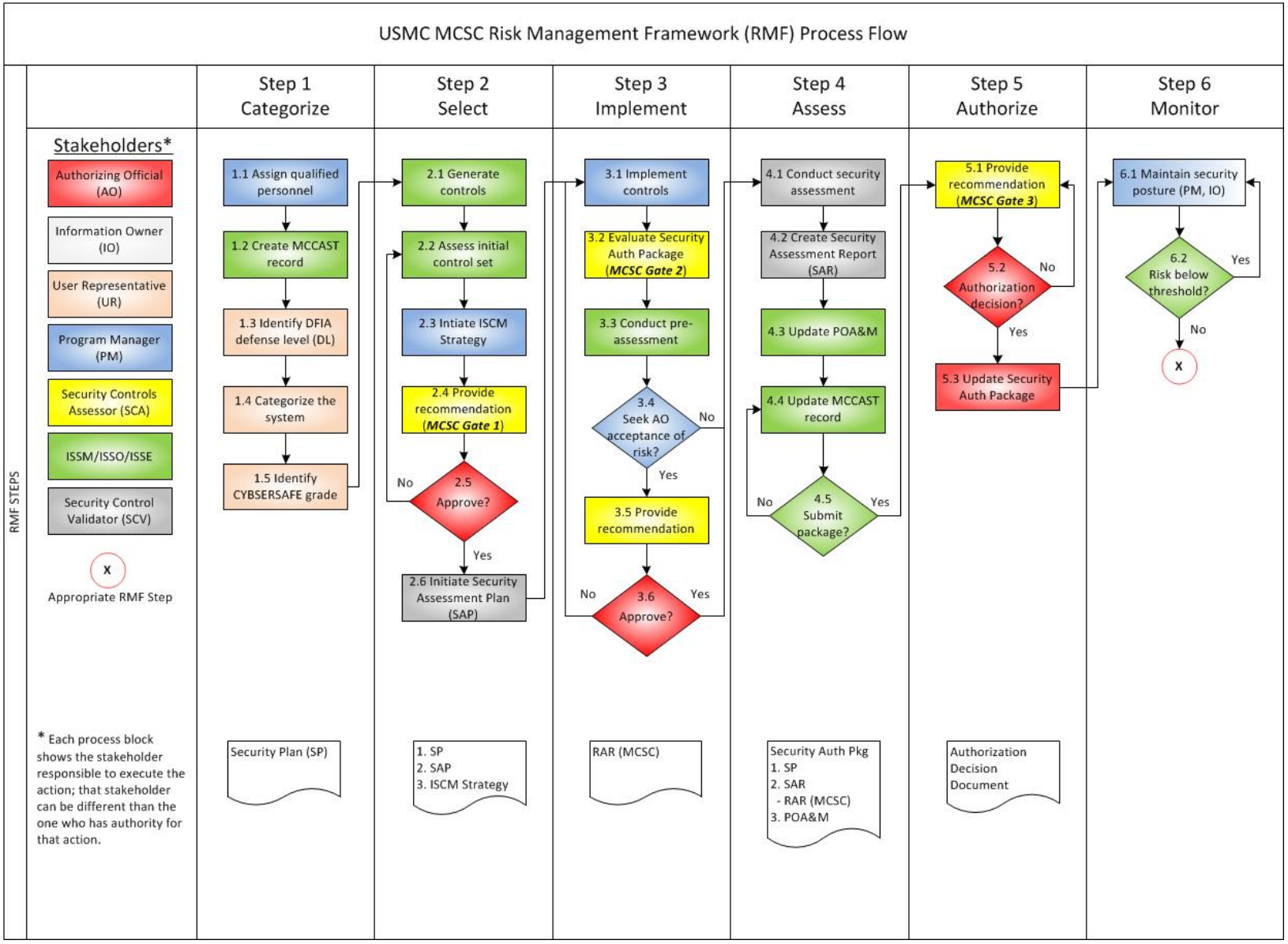

Figure 4-1: RMF Process Flow Diagram

Table 4-1 identifies the RASCI personnel for the fundamental activities of RMF Steps 1-6, and is the legend for understanding the notations in the final column, *RASCI*, in Table 4-2. The last column in Table 4-2 uses the first letter from these RASCI definitions to identify the stakeholders' level of participation in the RMF steps.

Note: The Responsible and Accountable stakeholders have the key roles in the RMF steps; the former for executing the task, the latter for final authority for the task. The stakeholders designated with the other RASCI definitions (i.e., Supportive, Consulted, or Informed) will either assist the Responsible stakeholder, as needed, or affect the sub-task's completion. Readers should focus mainly on the Responsible and Accountable stakeholders for the sub-tasks.

Table 4-1: RASCI Definitions

Responsible	Those who do the work to achieve the subtask. There is typically one role with a participation type of Responsible, although others can be delegated to assist in the work required (see Support).
Accountable	The Approver or final Approving authority; those who are ultimately accountable for the correct and thorough completion of the deliverable or subtask, and the one to whom Responsible is accountable. In other words, an Accountable must sign off (Approve) on work that Responsible provides. There must be only one Accountable specified for each task or deliverable.
Supportive	Resources allocated to Responsible. Unlike Consulted, who may provide input to the subtask, Support will assist in completing the subtask.
Consulted	Those whose independent opinions and review are sought, and with whom there is two-way communication.
Informed	People who are affected by the activity/decision and, therefore, need to be kept informed, but do not participate in performing the actual subtask. Position that needs to know of the decision or action.

Table 4-2: RMF Steps Responsibility Assignment

Task	Subtask Description	RASCI
RMF Step 1: ***Categorize System***	**1.1 Assign qualified personnel** The PM identifies the RMF personnel for the system.	**R** - PM **A** - AO **S** - SCA **C** - SCA **I** - None identified
	1.2 Create MCCAST record The ISSM creates a new authorization package (record) in MCCAST.	**R** - ISSM **A** - PM **S** – ISSO/ISSE **C** - SCA **I** - SCV
	1.3 Identify DFIA defense level (DL) The UR identifies the defense level of the system using the DFIA model.	**R** - UR **A** - UR **S** - SCA, ISSM **C** - IO **I** - SCV
	1.4 Categorize the system The UR, with support from the SCA and ISSM, categorizes the system in accordance with CNSSI 1253.	**R** - UR **A** - UR **S** - SCA, ISSM **C** - IO **I** - SCV
	1.5 Identify CYBERSAFE grade The UR determines the CYBERSAFE grade for the system. (The USMC implementation of the CYBERSAFE process is to be determined.)	**R** - UR **A** - UR **S** - SCA, ISSM **C** - IO **I** - SCV

Task	Subtask Description	RASCI
RMF Step 2: *Select Security Controls*	**2.1 Generate controls** The ISSM, with support of the ISSE, applies the DFIA defense level, system security categorization, and applicable overlays to generate the system's security controls.	**R** - ISSM **A** - PM **S** - ISSE **C** - SCA, SCV **I** - None identified
	2.2 Assess initial control set The ISSM reviews the initial control set and ensures controls are suitably documented. Only controls that are deemed NC for implementation will require AO review/approval.	**R** - ISSM **A** - PM **S** - ISSE **C** - SCA, SCV **I** - None identified
	2.3 Initiate ISCM Strategy The PM develops the initial ISCM Strategy.	**R** - PM **A** - PM **S** - ISSM **C** - SCA, SCV **I** - None identified
	2.4 Provide recommendation The SCA reviews the initial control set, justification for NC controls, the SP, and the ISCM Strategy and provides a recommendation to the AO. The SCA will coordinate with the PM and ISSM to recommend changes prior to AO review. (***MCSC Gate 1***)	**R** - SCA **A** - SCA **S** - ISSM, PM **C** - SCV **I** - AO
	2.5 Approve? The AO reviews control selection, SP and ISCM. If AO approves, then the security assessment plan can be initiated. If AO does not approve, then ISSM will have to reassess initial control set. *(AO approval of the controls constitutes the initial risk assessment.)*	**R** - AO **A** - AO **S** - None identified **C** - SCA, PM, ISSM **I** - SCV
	2.6 Initiate SAP Working with the ISSE and ISSM, the SCV develops a SAP to assess the resulting applicable security controls per the SP.	**R** - SCV **A** - SCA **S** - ISSE **C** - ISSM **I** - PM

Task	Subtask Description	RASCI
RMF Step 3: ***Implement Security Controls***	**3.1 Implement controls** The PM, with the support of the ISSE, implements the security controls as approved in the SP.	**R** - PM **A** - PM **S** - ISSM, ISSE **C** - SCA **I** - SCV
	3.2 Evaluate Security Authorization Package The SCA evaluates the Security Authorization Package, specifically the SP, SAP, and ISCM Strategy. The SCA can recommend changes to the PM and ISSM prior to self-assessment. (***MCSC Gate 2***)	**R** - SCA **A** - SCA **S** - PM, ISSM **C** - SCV **I** - None identified
	3.3 Conduct pre-assessment The ISSE performs a pre-assessment of the security controls as part of the security engineering process to verify the required security controls are implemented. The ISSE initiates a risk assessment report for any findings that will not be fixed prior to formal assessment in Step 4.	**R** - ISSM **A** - PM **S** - ISSE, SCV **C** - SCA **I** - None identified
	(Steps 3.4-3.6 are optional and only necessary if, during pre-assessment of the controls, the program believes it cannot comply with previously-approved controls and wants to seek early AO acceptance of risk so as to determine course of action.)	
	3.4 Seek AO acceptance of risk? The program may decide to seek AO acceptance of risk for some pre-assessment findings. If so, then the SCA will provide a recommendation to the AO on the pre-assessment risk results. If the program does not seek AO acceptance of risk from the pre-assessment, then the program will request the SCV to conduct the formal security assessment.	**R** - PM **A** - PM **S** - ISSM, SCA **C** - SCV **I** - None identified
	3.5 Provide recommendation If the program is seeking AO acceptance of risk for pre-assessment findings, then the SCA provides a recommendation.	**R** - SCA **A** - SCA **S** - ISSM **C** - SCV **I** - AO
	3.6 Approve? The AO accepts or rejects the pre-assessment risk for any issues that cannot be resolved prior to operations. If the AO accepts, then the program proceeds to Step 4, Assess. If the AO rejects, then the program must address the AO's risk concerns.	**R** - AO **A** - AO **S** - SCA **C** - ISSM **I** - SCV

Task	Subtask Description	RASCI
RMF Step 4: ***Assess Security Controls***	**4.1 Conduct security assessment** The SCV performs the official security assessment using the SAP, which the SCV updates prior to assessment.	**R** - SCV **A** - SCA **S** - PM, ISSM **C** - None identified **I** - None identified
	4.2 Create SAR The SCV initiates the SAR based on the results of the assessment and provides it to the PM and ISSM. The SCV will need support from the ISSM and ISSE to complete the risk assessment for open findings.	**R** - SCV **A** - SCA **S** - ISSM **C** - None identified **I** - None identified
	4.3 Update POA&M The ISSM updates the POA&M with support from the SCV and ISSE based on the assessed open vulnerabilities in the SAR.	**R** - ISSM **A** - PM **S** - SCV, ISSE **C** - None identified **I** - None identified
	4.4 Update MCCAST record The ISSM updates the Security Authorization Package in MCCAST to ensure it is ready for submission.	**R** - ISSM **A** - PM **S** - SCV, ISSE **C** - None identified **I** - None identified
	4.5 Submit package? The ISSM, with concurrence from the PM, submits the Security Authorization Package - including applicable artifacts - to the SCA for review and recommendation.	**R** - ISSM **A** - PM **S** - ISSE **C** - None identified **I** - SCA

Task	Subtask Description	RASCI
RMF Step 5: ***Authorize System***	**5.1 Provide recommendation** The SCA, after reviewing the SP and SAR, completes the risk assessment for the SAR. The SCA may recommend changes to the Security Authorization Package, to include the RAR, prior to completing the risk assessment and submitting the package to the AO. (***MCSC Gate 3***)	**R** - SCA **A** - SCA **S** - SCV, ISSM **C** - None Identified **I** - AO
	5.2 Authorization decision? The AO reviews the Security Authorization Package in order to make the final risk determination for an authorization decision. If the AO determines the risk is acceptable, the AO makes an authorization decision. Otherwise, the AO could request the SCA to resolve issues with the Security Authorization Package or issue a DATO and the program must address the risk concerns before seeking authorization.	**R** - AO **A** - AO **S** - SCA **C** - None Identified **I** - None Identified
	5.3 Update Security Authorization Package The AO generates an Authorization Decision Document. This document contains the authorization decision, terms and conditions for the authorization, and the authorization termination date (for an ATO).	**R** - AO **A** - AO **S** - SCA **C** - None Identified **I** - PM, ISSM

Task	Subtask Description	RASCI
RMF Step 6: ***Monitor Security Controls***	**6.1 Maintain security posture** The PM and the IO are jointly responsible for implementing the ISCM Strategy and maintaining the system's security posture as agreed to in the authorization decision. Together, the two stakeholders must track compliance/non-compliance of the associated security controls over the lifecycle of the system. Maintenance of the security posture will be maintained through various activities as identified in the ISCM Strategy: a. Annual security reviews b. Command Cyber Readiness Inspections c. IA Vulnerability Management (IAVM) notice and Operational Directive compliance d. Vulnerability scanning e. Security Technical Implementation Guide (STIG) compliance f. POA&M adjudication	**R** - PM, IO **A** - PM, IO **S** - ISSM, ISSE **C** - SCA, SCV **I** - AO
	6.2 Risk below threshold? The ISSM continuously assesses risk based on actions for maintaining the system's security posture. The ISSM will work with the PM to take the necessary corrective actions so the risk level remains acceptable. If the risk level cannot be kept at an acceptable level, the PM will request a new assessment, and if necessary, authorization.	**R** - ISSM **A** - PM, IO **S** - ISSE **C** - SCA, SCV **I** - AO

4.1 RMF Step 1 - Categorize System

Step 1 in the RMF process begins with the PM, with help from the SCA, identifying and assigning qualified cybersecurity personnel to a program. Next, the ISSM will create a new authorization package record in MCCAST and populate any fields where data is known. The UR plays an early pivotal role during Step 1 by identifying the DFIA defense level for the system. The DFIA defense level identifies the organization responsible for implementing each of the security controls. Specifically, the controls the PM must implement versus those the PM can inherit from another agency. Finally, the UR will also categorize the system, which will determine the baseline security controls and applicable overlays.

When the system security categorization is complete, the PM coordinates with the Functional Area Manager (FAM) to register the system in the DoD Information Technology Portfolio Repository DON (DITPR-DON).[7]

To facilitate Security Authorization Package development, the ISSM and UR should work closely with the SCA during this RMF step. Also, the PM should assign a qualified SCV early in the process.

Input

- System concept of operations
- Types of information processed by the system (see NIST Special Publication 800-60 references (h) and (i))
- Planned system architecture
- System security requirements from UR

Output

MCCAST

- New authorization package
- Initial SP

Other

- DITPR-DON record (or DADMS record, if MCCA)

4.1.1 Assign Qualified Personnel to Stakeholder Roles

The PM will assign qualified personnel to the stakeholder roles. The stakeholders must meet suitability requirements per DoDI 5200.02 (reference (d)) and the DoD and USMC training requirements. The cybersecurity workforce (ISSM, ISSO, ISSE, SCV) must meet the cybersecurity certification requirements, as required by DoD Directive (DoDD) 8140.01 (reference (e)) and detailed in ECSD 024 (reference (u)).

[7] https://www.dadms.navy.mil/

The PM will ensure assigned personnel have no conflicts of interest. For example, the SCA cannot be, or report to[8], the PM or Program Executive Office (PEO); the UR cannot be nor report to the PM; and the SCV cannot report to the PM. These examples are representative and not an exhaustive list of possible conflicts.

Programs must assign a fully-qualified SCV for their system from the AO-approved list of SCVs. HQMC C4 CY maintains the list of approved SCVs on their website.[9]

4.1.2 Create MCCAST Record

The ISSM will create a new record in MCCAST (i.e., authorization package for the system). If an ISSM needs guidance to create a new record, he or she should review the training material in MCCAST or work with the lead ISSM. The ISSM can also contact the MCCAST Help Desk.

4.1.3 Identify DFIA Defense Level

The UR should use the DFIA model to determine the defense level. The DFIA model identifies a subset of the NIST Special Publication 800-53 RMF security controls (reference (j)) based on the CNSSI 1253 criteria (reference (c)) and identifies the defense level associated with each control. It establishes an inheritance model to identify a standardized set of inherited and implemented controls across the USMC. In the model, an RMF control is only associated with one defense level. Programs will use the DFIA model early in the engineering lifecycle as a streamlined and repeatable approach for selecting controls.

Table 4-3 lists definitions to help in the understanding of the DFIA model.

Table 4-3: DFIA-Related Definitions

Common Control (Inheritable Control)	A security control that is inherited by one or more organizational information systems. (CNSSI 4009 (reference (s))
Common Control Provider	An individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls.
Defense Level	A set of layers extending across multiple technical entities (systems, hosts, applications, etc.) that provides security functions, features, or services.
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. (CNSSI 4009)
System-Specific Security Control	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system. (CNSSI 4009)

[8] "Report to" indicates one person is not subordinate to the other in a supervisory chain of command.
[9] https://eis.usmc.mil/sites/c4/cy1/Pages/CA.aspx

Table 4-4 lists the DFIA defense levels and provides examples. A system in its intended operational environment will fall within one of the defense levels. These defense levels identify implemented controls (i.e., ones the program must implement) and inherited controls (i.e., ones the system can inherit from another agency).

Table 4-4: DFIA Defense Levels

Defense Levels (DL) and Definition		
DL	**Definition**	**Example**
0	Physical site or host that hosts network, system, or application *Primarily provides physical and environmental security controls common to all systems at all sites.*[10]	Base, post, or station
1	MCEN enclave *MCEN Computer Network Defense (CND) Service Provider and transport services.*	Marine Corps Network Operations and Security Center (MCNOSC)
2	Data center and other network environments *Sub-enclave within the MCEN that provides primary network infrastructure, basic network services, and IA stack for cyber security boundary protection.*	• Regional Network Operations and Security Center (RNOSC) • Marine Air-Ground Task Force (MAGTF) Information Technology Support Center, Marine Corps Enterprise Information Technology Services (MCEITS) • Tactical Data Network (TDN) Data Distribution System-Modular (DDS-M) • TDN DDS Information Assurance Module (IAM)
3	(A) Connected mission/business system *Network-based system that implements security functions and services within the system solution. May communicate via DL 2 to another enclave/site or may communicate all the way through DL 1.*	MCSC system or application
	(B) Disconnected mission/business system *Stand-alone system, which could include a physically separated network, and implements security functions and services within the system solution.*	MCSC system or application

Most MCSC programs manage systems that reside at DL 3; these systems will reside within an enclave, whether in-garrison or deployed to a tactical environment. DL 3 systems must implement the system-specific security controls as shown by the DFIA model. The enclave is considered a common control provider and is responsible for compliance with common controls as well as system-specific security controls for a DL 3 system. The use of a program's DoD Architectural Framework (DoDAF) diagrams (Operational Viewpoint [OV]-1, Systems

[10] Enterprise policy controls should be assigned as DL0 and are applied to systems at all DFIA levels.

Viewpoint [SV]-2, and SV-3) will help to determine where a system resides within the DFIA model.

4.1.4 Categorize the System

The key result for RMF Step 1 is system security categorization performed by the UR. MCSC's approach to system security categorization follows the guidelines in CNSSI 1253 (reference (c)) in that programs will assign impact values (high, moderate, and low) for the three security objectives: Confidentiality, Integrity, and Availability (C-I-A).

System categorization takes into account the information types processed, stored, or transmitted by the system. NIST Special Publication 800-60 Vol 1 (reference (h)), lists the information types and their impact values, and NIST Special Publication 800-60 Vol 2 (reference (i)), describes the method for setting impact values of the information types. The UR, with support of the PM, will need to identify the relevant information types and assign impact values. Per the DoD PM's Cybersecurity Guide (reference (t)), the distinct impact values to C-I-A for each information type are included in the Initial Capabilities Document (ICD) or problem statement. For legacy systems, the UR should endorse the system's security requirements in a format that best meets the needs of the program.

Once the *information type categorization* is done, the PM can determine *system security categorization* by using the high-water mark values for C-I-A for each information type. For example, if a system processes five information types, and the highest impact value for Confidentiality is Moderate, then the system security categorization will have Confidentiality equal to Moderate. The same concept would apply for Integrity and Availability. The system security categorization is a high-water mark of the information types within each security objective (see Table F-2 for an example).

The categorization process must be conducted as an organization-wide activity that accounts for the enterprise architecture and how a specific system fits into it. Categorizing an individual IS must be based on the organization's mission objectives. Accordingly, the IS's categorization indicates the potential impact to the organizational operations, organizational assets, and individuals if a security breach occurs.

Associated with system security categorization is the process for identifying and selecting the CNSSI 1253 (reference (c)) overlays that could apply to the IS. MCSC has identified the following overlays that could apply to programs managed by MCSC: Classified Information Overlay and the Privacy Overlays. (The Privacy Overlays consist of four possible overlays: PII Low, PII Moderate, PII High, and Protected Health Information.) The UR must answer the overlay applicability questions to complete the system security categorization process.

After the UR completes the system security categorization and MCSC accepts what the UR provides, the ISSM will enter the system security categorization information into MCCAST so the control selection can be completed.

After the ISSM creates the MCCAST record for the authorization package, information entered into MCCAST is automatically mapped into the SP. The ISSM can export this initial draft of the SP as a report and send it to other stakeholders for review if they do not have MCCAST accounts. In subsequent RMF steps, more information will be mapped into the SP as needed.

4.1.5 Identify CYBERSAFE Grade

Note: The USMC process for CYBERSAFE is being developed and will be addressed as soon as possible. This guide will be updated as the USMC develops more details of the CYBERSAFE process for MCCAST implementation. The following paragraph addresses CYBERSAFE at a high-level.

The Department of Navy established the CYBERSAFE program to provide reasonable assurance of survivability and resiliency of critical warfighting information systems. Per DoDD 3020.40 (reference (p)), this effort for "mission assurance" is a process to ensure the continued function of capabilities and assets "critical to the execution of DoD mission-essential functions in any operating environment or condition." To meet this intent, programs must complete the CYBERSAFE analysis, per references (q) and (r), to determine a system's criticality and its impact to organizational mission. CYBERSAFE will help programs determine the effort required for additional assurances to systems and components of those systems identified as mission critical and mission essential. Those additional assurances are characterized by the CYBERSAFE Grades A, B, or C, with a grade determining the application of additional overlays of RMF controls beyond those resulting from system security categorization.

Table 4-5 is a brief description of each CYBERSAFE grade that results from CYBERSAFE analysis and the resulting impact.

Table 4-5: CYBERSAFE Grades and Characterization

Grade	System Characterization	Impact
A (Mission Critical)	System and components that provide or support mission critical functions (e.g., enclave boundary and platform boundary protection devices). Compromise of such systems or components would have a severe or catastrophic adverse effect to organizational operations, possibly resulting in mission failure. CYBERSAFE Grade A overlays implement the most comprehensive controls to provide mission assurance for the system's most critical systems and components.	Apply requirements for Grade B as well as the Grade A overlays where the security objective (C-I-A) has a critical operational impact.
B (Mission Essential)	Systems and components that provide or support mission essential functions. Compromise of such systems and components would have serious adverse effect to organizational operations and result in degraded mission state.	Apply selected assurance controls and enhanced assurance controls identified in the Grade B overlay.

Grade	System Characterization	Impact
C (Non-Mission Essential)	Systems and components that provide or support non-mission essential functions (e.g., routine administrative and business applications) and are not critical to the direct fulfillment of military or intelligence missions. Compromise of such systems or components would have limited adverse effect on organizational operations.	No additional RMF controls beyond those already identified by system security categorization and applicable overlays.

4.2 RMF Step 2 - Select Controls

Step 2 of the RMF process begins with generating the RMF security controls based on the output of RMF Step 1. The ISSM will assess this initial control set and identify any controls the program will not be able to comply with during the RMF implementation step. The DFIA model will identify the common controls inherited from the enclave(s) above the system. Accordingly, the PM will need an SLA with the agency responsible for implementing the common control. The PM will identify the continuous monitoring strategy for the system, and will need to get AO acceptance of the NC controls before proceeding to the next RMF step. The AO approval of the controls equates to the initial risk assessment of the system and the resulting controls will form the final control set for implementation. Once the AO has approved the final control set, the SCV can initiate the SAP.

During the early stages of Step 2, the program should identify the SCV (if it did not already do so in Step 1.) The SCV will be an important stakeholder in the successful completion of the tasks for Step 2.

Input

- System's DFIA defense level
- System categorization
- Applicable overlays
- CYBERSAFE grade
- MCCAST record (See Appendix J for MCCAST data associated with this step)
- Planned system architecture

Output

MCCAST

- Updated MCCAST authorization package
- Updated SP
- Initial SAP
- Initial ISCM Strategy
- AO-approved control set

Other

- Initial Cybersecurity strategy
- Draft SLA for organizations providing common controls

4.2.1 Generate Controls

Knowing the DFIA defense level, system security categorization, and applicable overlays, the ISSM will use MCCAST to generate the RMF controls for the system solution. The UR's decisions made in Step 1 will determine the RMF controls within MCCAST. The result of this task is the initial control set for the program.

4.2.2 Assess Initial Control Set

The ISSM will review the initial control set and determine if any of the controls will be NC. The ISSM must justify the reason for the NC controls because the AO must approve any controls that will have an implementation status other than compliant.

4.2.3 Initiate ISCM Strategy

The PM, with help from the ISSM and ISSE, will initiate the ISCM Strategy. The ISCM Strategy will address how the program plans to monitor the status of the initial control set, which will be automatically mapped into the SP report template within MCCAST. The development of the ISCM Strategy requires automated and manual processes for monitoring control status. The use of automated scanning and monitoring tools is ideal for the more timely status of controls that lend themselves to automated monitoring (i.e., most of the technical controls). However, some controls (typically non-technical controls) can only be monitored via manual review processes. The ISCM Strategy must address the monitoring of all controls. RMF Step 6 addresses more detail about the types of activities for executing the ISCM Strategy as part of the task for maintaining the system's security posture after system authorization.

4.2.4 Provide Recommendation (*MCSC Gate 1*)

The SCA will provide a recommendation to the AO to approve or disapprove the control selection based on an assessment of the following MCCAST products: the initial control set and justifications for NC controls, the SP, and the ISCM Strategy.[11] As necessary, the SCA will work with the PM and ISSM to update the Security Authorization Package prior to the SCA providing a recommendation to the AO.

This step marks MCSC's Gate 1.

4.2.5 Approve

The AO will review the MCCAST products (initial control set, SP, ISCM Strategy) and either approve or disapprove the control selection. For the initial control set, the AO will focus on the

[11] As of the date of this document, this notification to the AO will be done via the SIAT C&A Manager ticketing system.

controls with an implementation status of NC; typically, the AO will not review the controls given an implementation status of compliant.

If the AO approves the initial control set, then the SCV will begin work on the SAP.

If the AO does not approve the initial control set, then the ISSM will reassess the initial control set to resolve the AO's concerns.

4.2.6 Initiate Security Assessment Plan (SAP)

The SCV, working closely with the ISSE and ISSM, will initiate the SAP. The SAP addresses how to test and validate the applicable RMF controls, as documented in the SP. The SCV will use program architecture documentation and the MCCAST authorization package record to create the SAP. NIST Special Publication 800-53A Rev 4 (reference (k)) provides guidance on the RMF assessment processes and how to build effective assessment plans and how to analyze and manage assessment results.

4.3 RMF Step 3 - Implement Security Controls

In Step 3 of the USMC RMF, the PM is responsible for implementing the security controls as part of the systems engineering and technical review process. Once the controls are implemented, the ISSM, ISSO or ISSE will conduct a pre-assessment to evaluate how successfully the controls were implemented prior to the independent assessment performed by the SCV in Step 4. If the ISSM identifies a major risk during the pre-assessment, the PM may decide to seek AO acceptance of that specific risk.

If the PM decides to seek AO acceptance, the ISSM generates a RAR, which identifies the specific risk(s) to be addressed, then discusses the risk(s) with the SCA. After reviewing the RAR, the SCA makes a recommendation to the AO. Finally, the AO evaluates the information provided in the RAR along with the SCA's recommendation and makes a risk determination.

The RAR, generated in Step 3, feeds the SAR generated in Step 4. The SAR is submitted as part of the authorization package at the end of Step 4.

The PM also must ensure the creation of a Ports, Protocols, and Services Management (PPSM) registration for the system in the Defense Information Systems Agency (DISA) PPSM registry, as explained in ECSD 021 (reference (o)). The HQMC C4 Cybersecurity PPSM Technical Advisory Group representative has the registration forms. When entering the Ports, Protocols, and Services (PPS) into the registry, the ISSM should rely on the systems engineer or the ISSE to provide the details. The DoDAF diagrams will be useful, especially the SV-2, SV-3, and SV-6.

Input

- Applicable controls
- SP

Output

MCCAST

- Updated SP

- Pre-assessment results
- Initial POA&M
- RAR

Other
- Initial PPSM registration

4.3.1 Implement Controls

The PM is ultimately responsible for implementing security controls within the system. Specifically, the PM ensures cybersecurity efforts are funded, staffed, and supported. The ISSM supports the PM by identifying cybersecurity requirements and working with the systems engineer and ISSE to develop and secure the system. The engineers are responsible for physically implementing the controls on the system. During this step, the PM-designated individual registers the system in the PPSM registry; however, the engineering staff needs to identify the PPS used in the system. Also, the PM ensures the software for the system is registered in DADMS.

4.3.2 Evaluate Security Authorization Package (*MCSC Gate 2*)

After the program implements the security controls and updates the system authorization package, the ISSM will notify the SCA.[12] The SCA will evaluate the Security Authorization Package. This evaluation serves as a risk mitigation to ensure the program is sufficiently prepared for the self-assessment. Specifically, the SCA will review the following products: SP, SAP, and ISCM Strategy. The SCA can recommend changes to the PM and ISSM to help ensure success in the pre-assessment.

This step marks MCSC's Gate 2.

4.3.3 Conduct Pre-Assessment

The ISSM is responsible for managing the pre-assessment with the help of the ISSO and ISSE. The ISSM may need other members of the project team to support the self-assessment as well. During the pre-assessment, the ISSM evaluates all items that will be assessed by the SCV in Step 4. The pre-assessment enables the ISSM to identify and address vulnerabilities prior to the SCV's formal assessment.

In step 2, the ISSM worked with the SCV to generate a SAP. The ISSM conducts the pre-assessment using the SAP. Once the pre-assessment identifies vulnerabilities, the ISSM generates an initial POA&M to document those vulnerabilities.[13] At that point, the ISSM will work with the project team to analyze the vulnerabilities and determine which ones should be remediated and how the remaining vulnerabilities should be mitigated. Once initiated, the

[12] As of the date of this document, this notification will be via the C&A Manager ticketing system.
[13] For programs executing new starts or re-authorizations under RMF, this initial POA&M will consist of RMF controls. For existing programs accredited under DIACAP that must execute an ASR under RMF, POA&Ms could have a mix of DIACAP and RMF controls.

POA&M remains active throughout the system lifecycle. The POA&M is updated every time a new vulnerability is discovered or closed.

Note: Programs must follow the classification instructions per the program's security classification guide (SCG). Stakeholders must pay special attention to the data handling and dissemination of test results, in particular vulnerability results.

4.3.4 Seek AO Acceptance of Risk

After the ISSM and PM determine how to address each vulnerability, the ISSM reviews the POA&M to determine if any vulnerability poses unacceptable risk. If the ISSM is concerned about a specific risk, the ISSM must identify the risk to the PM, and the PM must determine whether or not to seek AO acceptance of the risk.

If the PM decides to seek AO acceptance of the risk, the ISSM generates a RAR. The RAR identifies the vulnerability, how it will be mitigated, and why the PM and ISSM believe the vulnerability to be high risk. The PM and ISSM then submit the RAR to the SCA.

4.3.5 Provide Recommendation

When the SCA receives the RAR, the SCA will evaluate the RAR and communicate with the PM and ISSM to fully understand the risk. The SCA may recommend actions to the PM to improve the security posture of the system or to update the Security Authorization Package for submission. Once the risk is understood and the PM is ready to submit to the AO, the SCA will develop a recommendation based on the information provided and submit the RAR and recommendation to the AO.

4.3.6 Approve

The AO will review the RAR from the pre-assessment and the SCA's recommendation. If the AO has questions, the AO will contact the SCA to discuss the system. Once the AO has a full understanding of the risk, the AO will either accept or reject the risk.

If the AO accepts the risk, the system moves to Step 4.

If the AO rejects the risk, the AO will notify the SCA who will work with the PM and ISSM to resolve the issue. The resolution may involve the PM reevaluating the implementation of the controls and engineering a solution to improve the security posture of the system. Once the risk is addressed the ISSM conducts another pre-assessment and updates the SP.

4.4 RMF Step 4 – Assess Security Controls

In Step 4 of the USMC RMF, the SCV conducts the official security assessment and generates the SAR. After the SCV gives the SAR and POA&M to the ISSM, the ISSM adds PM-specific details to the POA&M, such as points of contact, resources required, scheduled completion date, and comments. The ISSM then reviews the MCCAST record and updates it prior to submitting the package. Once the MCCAST Security Authorization Package is ready for submission, the PM makes the decision to submit it.

Note: Programs must follow the classification instructions per the program's SCG. Stakeholders must pay special attention to the data handling and dissemination of test results, in particular vulnerabilities.

Input

- SP
- POA&M

Output

MCCAST

- Final (baseline) SP
- SAR
- Updated POA&M

Other

- N/A

4.4.1 Conduct Security Assessment

The SCV executes the security assessment using the SAP initiated in Step 2. As the SCV assesses the system, he or she will annotate the results for each test. HQMC C4 CY provides specific validator training that SCVs must follow to assess a system.

4.4.2 Create Security Assessment Report

The SCV documents the results of the security assessment in a SAR. In addition to the SAR, the SCV creates an initial POA&M that includes all vulnerabilities found during the security assessment. The SCV will identify in the POA&M applicable mitigations found during the assessment and provide mitigated risk levels. The SCV will also identify false positives and misleading results in the POA&M.

The SCV's assessment must be supported by test results generated by the SCV. If the SCV plans to use any results from the pre-assessment, then the SCV must obtain permission from the SCA beforehand and disclose this information in the SAR. The following items must be included in SCV's assessment within MCCAST:

- Assured Compliance Assessment Solution (ACAS) detailed vulnerability report
- ACAS summary report
- .nessus files (from ACAS)
- .ckl files (from Security Technical Implementation Guide [STIG] viewer)
- eXtensible Configuration Checklist Description Format (XCCDF) results….xml files (from Security Content Automation Protocol [SCAP])
- Vulnerator output

- SAR
- POA&M
- Code analysis assessment reports, if applicable

The SCV must follow the MCSC guide for creating and maintaining the POA&M per Appendix E.

HQMC C4 CY is responsible for providing the specific requirements for conducting RMF security control assessments.

4.4.3 Update POA&M

The ISSM reviews the SCV's SAR and determines if the PM needs to remediate or mitigate newly discovered vulnerabilities. Once those decisions are made, the systems engineer and ISSE must remediate or mitigate those findings. When all vulnerabilities have been addressed, the ISSM updates the POA&M. Finally, the ISSM conducts a review to ensure all vulnerabilities are included on the POA&M, all vulnerabilities are described adequately, and all vulnerabilities have an acceptable mitigation. The ISSM must follow the MCSC guide for creating and maintaining the POA&M per Appendix E.

4.4.4 Update MCCAST Record

The ISSM updates the Security Authorization Package in the MCCAST system record. The ISSM must ensure all information required for submission is included in the MCCAST system record.

4.4.5 Submit Package

After the ISSM performs a risk assessment, the ISSM makes a recommendation to the PM. The PM then decides if the package is ready for submission.

If the PM decides to submit, then the ISSM ensures the package is completed in MCCAST and ready for the SCA to review.

If the PM decides the package is not ready for submission, then the package goes back to the ISSM for updates.

4.5 RMF Step 5 – Authorize System

In Step 5, the SCA analyzes the package and makes a risk assessment. The SCA's risk assessment is entered into the SAR and is submitted to the AO via MCCAST. The AO reviews the package and risk assessment provided by the SCA and either makes an authorization decision or sends the package back to the SCA with comments that require resolution prior to an authorization decision.

Input

- SP
- SAR
- POA&M

Output

MCCAST

- SCA risk assessment
- Authorization decision
- Updated MCCAST record

Other

- N/A

4.5.1 Provide Recommendation (*MCSC Gate 3*)

Once the ISSM notifies the SCA that the package is ready for review,[14] the SCA's team performs a thorough review of the package prior to the SCA forming a risk assessment.

After the SCA thoroughly understands the system, the SCA makes a risk determination. If the package is complete and addresses all vulnerabilities, the SCA will sign the SAR in MCCAST and submit the record to the AO for review.[15]

If the package is not complete or has not addressed all vulnerabilities, the SCA sends the package back to the PM, specifically the ISSM, to address the issues.

Once the ISSM has addressed all issues from the SCA's review, the SCA signs the SAR and submits the Security Authorization Package to the AO.

This step marks MCSC's Gate 3.

4.5.2 Authorization Decision

The AO reviews the Security Authorization Package to determine if the system's residual risk falls within an acceptable level. The AO considers the current security state of the system, as reflected in the SAR, and balances mission need against risk to the mission, the information being processed, the broader information environment, and other missions reliant on the shared information environment. The AO must also consider any applicable risk-related guidance from DoD Information Security Risk Management Committee (ISRMC), Defense Information Assurance Security Accreditation Working Group (DSAWG), mission owner(s), and other SMEs. Weighing these factors, the AO renders a final risk determination related to the operation of the system.

If the AO determines the risk level is acceptable, then the AO will approve the system package in MCCAST; thereby making an authorization decision and granting an ATO. The AO's authorization decision may be an ATO, ATO/ATC, IATT, or MCCA. A system is considered unauthorized if an authorization decision has not been made.

[14] As of the date of this document, this notification will be via the C&A Manager ticketing system.
[15] As of the date of this document, this notification will be via the C&A Manager ticketing system.

If the AO determines the risk level is unacceptable, either the AO will send the package back to the SCA with items to resolve or the AO will issue a DATO. The SCA is responsible for working with the PM and ISSM to address the AO's concerns.

4.5.3 Update Security Authorization Package

The AO's office updates the Security Authorization Package to include the authorization decision, terms and conditions for the authorization, and the authorization termination date.

4.6 RMF Step 6 – Monitor Security Controls

This step represents the final step of RMF – continuous monitoring of the authorized system. It is the execution phase of the ISCM Strategy developed during Step 2 and approved by the authorization decision. The PM and IO will ensure continuous monitoring of the operational system drives ongoing updates to the security posture of the system.

Inputs

- ISCM Strategy
- Results from continuous monitoring activities

Output

MCCAST

- Updated SP (based on results from ISCM activities)
- SAR
- Updated POA&M
- Updated MCCAST record
- Continuous monitoring artifacts provided at frequency defined in the ISCM Strategy
- Annual Security Review artifacts

Other

- Naval notification message for decommissioning (if applicable)
- Updated DITPR-DON record

4.6.1 Maintain Security Posture

The PM and IO are jointly responsible for maintaining the system's security posture for the life of the system. The acquisition program management office manages the system development while the operational community (end user) does most of the security sustainment, unless the acquisition PM has been assigned full lifecycle management responsibility. The roles and responsibilities of the PM and the IO in maintaining the system's security posture must be formally documented in a written agreement, such as an SLA or Memorandum of Agreement (MOA).

RMF Step 6 has two parts. The first is calendar-based and consists of an Annual Security Review (ASR), periodic patching and scanning, and reauthorization every three years. Reauthorization may occur sooner than three years if changes to the system architecture significantly alter the security posture of the system or if the threat environment poses a greater risk to the system. The second part is conditional and is composed of incident response handling, compliance with IAVM notices and CTOs, Cybersecurity Inspection (CSI) and Command Cyber Readiness Inspection (CCRI) findings, POA&M adjudication, and decommissioning. Programs must follow their IAVM plan (e.g., track vulnerabilities, remediate findings, mitigate risk) per ECSD 020 (reference (n)). Specific guidance on handling CCRIs for tactical systems is contained in Appendix K.

The FISMA requires an annual security assessment of the approved RMF controls. As part of the ASR, the PM and ISSM will test one-third of the security controls every year. As stated in Step 2, this testing will include control assessment via automated scanning and manual review. Not all controls can be assessed by automated means (i.e., SCAP Compliance Checker and ACAS scans). PMs must include ASRs in their integrated master schedule. Also, the ISSM must update the DITPR-DON record with ASR information.

Regardless of the source of the event affecting the system's security posture, the PM or IO must ensure remediation actions are taken based on the ongoing monitoring activities. The ISSM will ensure the SP, SAR, and POA&M are updated based on the results of the continuous monitoring process.

A system approaching end of life will go through the decommissioning process, which will trigger a series of actions (e.g., a DATO and Naval message notifications to the fleet). ECSD 018 (reference (m)) provides a detailed list of all the associated actions for decommissioning. The ISSM will need to update the MCCAST record to comply with the decommissioning actions.

4.6.2 Risk below Threshold

The ISSM assesses the risk posed to the system in its operational environment. When events require corrective actions or the system's level of risk exceeds an acceptable level[16], the ISSM will work with the PM or IO to take the necessary corrective actions. If the PM or IO cannot keep the risk level to an acceptable level, the PM or IO will notify the SCA and AO, submit an updated POA&M, and request a new assessment (and authorization if applicable). The program will re-enter the RMF process at an AO-agreed point.

[16] The term "acceptable level" is subjective because risk is affected by the evolving threat, identification of new vulnerabilities, and changes to system design. The ISSM must weigh these factors to determine if risk level becomes higher than as defined by the current authorization decision.

Appendix A **REFERENCES**

(a) Department of Defense (DoD) Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” 12 March 2014

(b) DoD Instruction 8500.01, “Cybersecurity,” 14 March 2014

(c) Committee on National Security Systems Instruction 1253, “Security Categorization and Control Selection for National Security Systems,” 27 March 2014, as amended

(d) DoD Instruction 5200.02, Change 1, “DoD Personnel Security Program,” 9 September 2014, as amended

(e) DoD Directive 8140.01, “Cyberspace Workforce Management,” 11 August 2015

(f) Federal Information Processing Standard Publication (FIPS Pub) 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004

(g) NIST Special Publication 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems,” February 2010

(h) NIST Special Publication 800-60 Volume 1 Revision 1, “Volume I: Guide to Mapping Types of Information and Information Systems to Security Categories,” August 2008

(i) NIST Special Publication 800-60 Volume 2 Revision 1, “Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories,” August 2008

(j) NIST Special Publication 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” 30 April 2013

(k) NIST Special Publication 800-53A Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations,” December 2014

(l) NIST Special Publication 800-30 Revision 1, “Guide for Conducting Risk Assessments,” September 2012

(m) United States Marine Corps Enterprise Cybersecurity Directive 018, Marine Corps Certification and Accreditation Process v3.0, 7 September 2012

(n) United States Marine Corps Enterprise Cybersecurity Directive 020, Marine Corps Information Assurance Vulnerability Management Program v1.0, 31 December 2013

(o) United States Marine Corps Enterprise Cybersecurity Directive 021, “Ports, Protocols and Services Management v1.0,” 5 May 2012

(p) Defense Directive 3020.40, “DoD Policy and Responsibilities for Critical Infrastructure,” Change 2, 21 September 2012

(q) United States Navy Space and Naval Warfare Systems Command, “Navy Cybersecurity Safety (CYBERSAFE) Grading Criteria Standard,” v0.03, 31 July 2015

(r) United States Navy Space and Naval Warfare Systems Command, “Grade Requirements Standard,” v0.03, 31 July 2015

(s) Committee on National Security Systems Instruction 4009, Committee on National Security Systems (CNSS) Glossary, 6 April 2015

(t) DoD Program Manager’s Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, v1.0

(u) United States Marine Corps Enterprise Cybersecurity Directive 024, “Cybersecurity Workforce Improvement Program (CWIP),” Version 1.0 15 June 2014

(v) Department of Defense Information Technology Portfolio Repository – Department of the Navy (DITPR–DON) Process Guidance, Version 1.0, 28 November 2011

(w) Department of Defense (DoD) Cybersecurity Risk Assessment Guide, updated 5 November 2015

Appendix B **ACRONYMS**

Acronym	Definition
A&A	Assessment and Authorization
ACAS	Assured Compliance Assessment Solution
AO	Authorizing Official
AO CSA	Authorizing Official Cybersecurity Analyst
ASR	Annual Security Review
ATC	Authorization to Connect
ATO	Authorization to Operate
BMA	Business Mission Area
C&A	Certification and Accreditation
C4	Command, Control, Communications, and Computers
CAL	Category Assurance List
CAT	Category
CCRI	Command Cyber Readiness Inspection
C-I-A	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
C-ISP	Commercial Internet Service Provider
CND	Computer Network Defense
CNSSI	Committee on National Security Systems Instruction
COTS	Commercial Off-the-Shelf
CSA	Cybersecurity Analyst
CSI	Cybersecurity Inspection
CTO	Communications Tasking Order
CYBERSAFE	Cybersecurity Safety
CVE	Common Vulnerabilities and Exposures
DADMS	Department of Navy Application Database Management System
DATO	Denial of Authorization to Operate
DC	Deputy Commander
DDS	Data Distribution System
DDS-M	Data Distribution System-Modular
DFIA	Defense-in-Depth Functional Implementation Architecture
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIMA	DoD portion of the Intelligence Mission Area
DISA	Defense Information Systems Agency
DITPR-DON	DoD Information Technology Portfolio Repository DON
DL	Defense Level
DoDAF	DoD Architectural Framework
DoDD	DoD Directive
DoDI	DoD Instruction
DON	Department of the Navy

Acronym	Definition
DSAWG	Defense Information Assurance Security Accreditation Working Group
ECSD	Enterprise Cybersecurity Directive
EIEMA	Enterprise Information Environment Mission Area
FAM	Functional Area Manager
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GOTS	Government Off-The-Shelf
HQMC	Headquarters Marine Corps
IAM	Information Assurance Module
IASE	Information Assurance Support Environment
IATB	Interim Authority to Build
IATT	Interim Authorization to Test
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
ICD	Initial Capabilities Document
IO	Information Owner
IS	Information System
ISCM	Information System Continuous Monitoring
ISO	Information System Owner
ISRMC	Information Security Risk Management Committee
ISSE	Information System Security Engineer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
KS	Knowledge Service
MA	Mission Area
MAGTF	Marine Air-Ground Task Force
MC	Mission Critical
MCCA	Marine Corps Certified Application
MCCAST	Marine Corps Certification and Accreditation Support Tool
MCCDC	Marine Corps Combat Development Command
MCEITS	Marine Corps Enterprise Information Technology Services
MCEN	Marine Corps Enterprise Network
MCNOSC	Marine Corps Network Operations and Security Center
MCSC	Marine Corps Systems Command
ME	Mission Essential
MITSC	MAGTF Information Technology Support Center
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MS	Mission Support

Acronym	Definition
NC	Non-Compliant
NIST	National Institute of Standards and Technology
NSS	National Security System
OV	Operational Viewpoint (DoDAF view)
PEO	Program Executive Office
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIT	Platform Information Technology
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
POR	Program of Record
PPS	Ports, Protocols, and Services
PPSM	Ports, Protocols, and Services Management
RAR	Risk Assessment Report
RASCI	Responsible, Accountable, Supportive, Consulted, and Informed
RMF	Risk Management Framework
RNOSC	Regional Network Operations and Security Center
SAP	Security Assessment Plan
SAR	Security Assessment Report
SCA	Security Control Assessor
SCAP	Security Content Automation Protocol
SCG	Security Classification Guide
SCV	Security Control Validator
SIAT	Systems Engineering, Interoperability, Architectures and Technologies
SIPRNet	Secret Internet Protocol Router Network
SISO	Senior Information Security Officer
SLA	Service Level Agreement
SP	Security Plan
SRG	Security Requirements Guide
SSE	Systems Security Engineering
STIG	Security Technical Implementation Guide
SV	Systems Viewpoint (DoDAF view)
TDN	Tactical Data Network
UR	User Representative
USMC	United States Marine Corps
WMA	Warfighting Mission Area
XCCDF	eXtensible Configuration Checklist Description Format

Appendix C **RECIPROCITY**

Reciprocity under RMF is defined in CNSSI 4009 (reference (s)) as the "mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information." Applied appropriately, reciprocity enhances cybersecurity through consistent application of controls across multiple enclaves while reducing redundant testing, assessment and documentation, and the associated costs in time and resources.

At MCSC, the PM coordinates with the lead service or organization to identify cybersecurity requirements. Ideally, MCSC has an MOA, MOU, SLA in place with the lead service or is a voting member on the configuration control board. The lead service or organization then implements cybersecurity controls, develops the RMF package, and obtains an ATO from the lead service or organization's AO.

Once the lead service or organization obtains the ATO, they provide the RMF security authorization package to the MCSC PM[17]. The security authorization package includes the following:

a. Security Plan, to include
   - documented security controls
   - hardware List
   - software List
   - interfaces and interconnections
   - authorization boundary diagram
   - data flow diagram
   - continuous monitoring plan
   - PPSM registration number
   - DITPR-DON or DITPR registration number

b. POA&M

c. ATO

d. Security Assessment Report, to include scan results[18]

The ISSM is responsible for reviewing the entire RMF package to ensure the package is complete and the package provides an accurate assessment of the security posture of the system.

[17] DoDI 8510.01 states the deploying service "must provide the complete security authorization package to receiving organizations."

[18] The ISSM needs to ensure the lead service's scan results are current (within 60 days) for the USMC's authorization determination. Otherwise, the ISSM will ensure current security scans are conducted.

Some lead services or organizations are grouping open vulnerabilities on their POA&M and identifying incorrect CATs in the process. Because this practice provides an unrealistic perspective of the security posture of the system, the MCSC ISSM must ensure the content of the lead service's POA&M conforms to the USMC's POA&M requirements. The only updating that must occur is ensuring each vulnerability has a separate line and ensuring each line item has a RAW CAT and mitigated CAT. This will help the SCA make an appropriate risk assessment.

Additionally, the ISSM is responsible for assessing the system they receive from the lead service to verify the information the lead service provided. If discrepancies are found, the PM must work with the lead service or organization to resolve the discrepancies.

Once the ISSM is confident that the information in the RMF package is accurate, the PM submits to SIAT/SSE/CE via MCCAST.

The rest of the process is handled as already documented in this guide for systems that are not reciprocity.

Even after the ATO is obtained, the MCSC ISSM must upload an updated POA&M to the system record in MCCAST every time the lead service distributes an update. At all times, the MCCAST record should contain a POA&M that reflects the system currently fielded.

If the ATO is nearing the expiration date, and the PM determines the lead service or organization is not going to have a new ATO in place in time to allow MCSC to obtain an ATO, the PM can request a USMC ATO for a specified period of time, usually 90 days. To obtain an ATO, the PM needs to provide updated scans and a USMC POA&M, assuming the rest of the information listed above is already in the MCCAST record.

Appendix D **MARINE CORPS CERTIFIED APPLICATION**

HQMC C4 CY is working on guidance for certified applications. The information below is provided as a way forward until the higher-level guidance is available.

After obtaining the requirement for an application, the PM should generate an MCCA record in MCCAST. Security controls are not generated for MCCAs. However, the PM should ensure applicable STIGs have been applied to the application, the application must be developed in secure manner, and automated code reviews must be performed if the application is developed by the government or in any way modified by the government.

At some point in the development cycle, a Privacy Impact Assessment must be completed. If the application uses PII, this must be annotated in the system record. Additionally, the application must be registered in DADMS or DITPR-DON. If the application does not meet the definition of a system, it must be registered in DADMS[19]. If the application meets the definition of a system, the application must be registered in DITPR-DON. (NOTE: DADMS or DITPR-DON registration is NOT an authorization to use software/applications. DADMS and DITPR-DoN are IT investment tracking and management tools for FISMA compliance.)

Once the application is developed and all applicable STIGS are applied, the ISSM should conduct a self-assessment. This process involves (1) conducting a pre scan on the designated platform that the application will go on, (2) loading the application onto the designated platform after the pre scan is completed, and (3) conducting a post scan of the designated platform with the application loaded. The vulnerabilities on the post scan that were not on the pre scan are the vulnerabilities related to the application. These vulnerabilities must go on the application's POA&M.

Once the MCCAST record has been populated, the ISSM notifies the SCA the package is ready for review.[20] The SCA will analyze the information provided and submit a recommendation to the AO for an MCCA decision.

[19] To ensure consistency in registration and reporting, this guide follows the definitions of “system” and “application” from the DITPR-DON Policy Guidance (reference (v)). Those definitions are shown in the NOTE at the end of Section 3.
should be entered into DITPR-DON and subsequently in the Echelon II/FAM modules in DADMS:

[20] As of the date of this document, this notification to the SCA will be done via the SIAT C&A Manager ticketing system.

Appendix E **PLAN OF ACTION AND MILESTONES**

The system security POA&M, as shown in Figure E-1, identifies the vulnerabilities affecting the security posture of a system and identifies the tasks and milestones to remediate or mitigate those issues. The PM and ISSM use the system security POA&M to plan and monitor corrective actions. The system security POA&M also is used by the SCA, AO, and general inspectors during security evaluations. MCCAST is the central repository for USMC system POA&Ms.

POA&Ms are permanent records. All system vulnerabilities, both technical and non-technical, are identified in the system security POA&M. Once an entry is made onto a POA&M, the vulnerability can be closed but not removed. All initial findings on the POA&M have a status of "ongoing," but as vulnerabilities are addressed, the status may change to "completed" or "AO accepted risk."

The SCV populates the POA&M with the open findings from the security control assessment of the system (e.g., RMF Step 4). Entries on the POA&M may also be made as a result of a program's self-assessment or activities from the execution of continuous monitoring.

Note: Lead ISSMs must review and approve all POA&Ms before submission to the SCA.

Weakness (1)	Raw CAT (2)	IA Control (3)	Mitigated CAT (4)	Mitigation (5)	POC (6)	Resources Required (7)	Scheduled Completion Date (8)	Milestone Changes (9)	Source Identifying Weakness (10)	Status (11)	Comments (12)

Figure E-1: POA&M Layout

The explanation for each POA&M column is as follows:

Weakness (1)

This details on the vulnerability: vulnerability name, identification, description, and vulnerability reference (such as Common Vulnerabilities and Exposures (CVE), IAVA, STIG, Marine Administrative Message, or Operational Directive).

Raw CAT (2)

This is the risk level for the finding as assigned by the vulnerability reference. The raw category (CAT) should be formatted in one of two formats: either I, II, III; or Very High, High, Moderate, Low, Very Low.

IA Control (3)

This is the security control that maps to the vulnerability. The security controls can be found in NIST Special Publication 800-53. Often the tool gives the security control.

Mitigated CAT (4)

This is the risk level after the vulnerability has been mitigated, as determined by the SCV, when the POA&M entry is a result of a security control assessment. (For internal assessments conducted by the ISSM, the ISSM can provide the mitigated risk level.) It equates to the residual risk. The mitigated CAT should be formatted in one of two formats: either I, II, III; or Very High, High, Moderate, Low, Very Low.

Mitigation (5)

This details how the vulnerability is being mitigated.

The following guidelines should be used when developing the mitigation strategy:

- Be short and concise (2-3 sentences)
- Identify how to significantly reduce the attack surface, attack vector and/or impact of a given vulnerability
- Address the local and/or remote aspects of the vulnerability
- Address the number of individuals who have physical and/or logical access to the vulnerable asset
- Should not discriminate between privileged and non-privileged users
- When possible, cite an authoritative source for justification/explanation of mitigations: “In accordance with the Enclave STIG V-XXXX, this finding can be mitigated to a CAT II if…” or “In accordance with Microsoft KB123456, the following configuration setting was implemented…”

The following mitigation concepts are bad examples of mitigation strategies:

- Use ‘future action’ or ‘future configuration’ as mitigation
- Rationalize why a vulnerability is not remediated (i.e., lack of funding, etc.)
- Describe a hacker’s exploitation steps (i.e., “A hacker would first have to ____, then ____, before they could ____.)
- Contain generic “Defense in Depth” statements without addressing how each layer directly reduces the attack surface or reduces the impact
- Describe the clearance/trust level of the users
- Describe the level of training that a user has obtained
- Address only one of several attack vectors
- Provide information not directly related to the discrete vulnerability

- Use the fact that the vulnerability is located on Secret Internet Protocol Router Network (SIPRNet) alone as a mitigation factor

POC (6)

This is the Point of Contact (POC) responsible for addressing the vulnerability. POC can be someone on the PM staff or the support staff.

Resources Required (7)

This is the cost (in dollars) required to address the vulnerability.

Scheduled Completion Date (8)

This is the date when the vulnerability will be fixed.

The following guidelines should be used to determine the scheduled completion date:

- When fixes are performed by the program:
  - Enter the date when the last asset will be updated
- When fixes are not performed by the program:
  - Enter the date when the program will release the update
- If there is no plan to address the vulnerability (AO Accepted Risk), NA will go in this column
- This column should:
  - Never change once data is entered
  - Never be left blank

Milestone Changes (9)

This is the revised scheduled completion date if the original scheduled completion date cannot be met.

The following guidelines should be applied to any information that is added to the Milestone Changes column:

- This column remains blank until the schedule slips
- Fiscal year and quarter is an acceptable entry while the release date is being solidified
- Further schedule slips will by captured by replacing the prior slip date

Source Identifying Weakness (10)

This is the event, tool, and date related to discovery of the vulnerability.

Status (11)

This is the status of the vulnerability:

- ***Ongoing*** – vulnerability has not been resolved yet.
- ***Completed*** – vulnerability has been resolved.
- ***AO Accepted Risk*** – vulnerability will not be resolved.

Comments (12)

This is any supporting information that does not fit within the context of the other POA&M fields. If there is no plan to fix the vulnerability, "Requesting AO accept risk" and the justification will be identified here.

SCENARIOS

Below are some specific scenarios related to POA&M maintenance and the related guidance on how to complete the POA&M.

Zero Day Vulnerabilities

- Complete columns 1-3, 5, 6,and 10 as normal
- Column 4: "CAT IV"
- Columns 7/8/9: Leave blank.
- Column 11: "Ongoing"
- Column 12: Have the reference(s) identified in the comments column.
- Once a fix has been identified, the CAT will revert to the original CAT.

"AO Accepted Risk" Vulnerabilities

- Complete columns 1-7, 10 as normal
- Column 8: "NA"
- Column 9: Leave blank
- Column 11: "AO Accepted Risk."
- Column 12: State "Requesting AO accept risk" and then justify why the AO should accept the risk.[21]

[21] If the AO authorizes a system (i.e., grants an ATO), then the AO has accepted the risk as stated in the POA&M. Columns 11 and 12 would not change because the AO must accept the risk each time the AO reviews the POA&M; therefore, the POA&M should indicate the program is asking the AO to accept risk each time.

OTHER GUIDELINES

Below are some final guidelines for completing the POA&M.

- Each distinct vulnerability must go on a separate line in the POA&M. Vulnerabilities should not be bundled or grouped.
- Each row in the POA&M identifies one vulnerability on one managed image/device. If a vulnerability affects multiple devices, the POA&M will have multiple rows – one row for each vulnerability-device combination.
- The SCA and the AO use the program's POA&M to assess the risk of the baseline AND the fielded assets. All POA&Ms must address the security posture of the program's baseline AND the security posture of Operating Forces.
- Vulnerabilities should not be closed until the patch has been released to Operating Forces.
- The scheduled completion date should represent the date the patch is released to Operating Forces.
- Mitigations and comments should cover the security posture of Operating Forces.
- Completed vulnerabilities will stay on the POA&M.
- New POA&Ms will be created for first-integer changes to the system version (i.e., from v2.0 to v3.0) or for significant deviation from the previously authorized baseline.
- If there is a conflict between the STIG and scan tool, generally the STIG should be followed. However, the SCV (or ISSM) needs to determine which configuration setting would be more secure to the system’s security posture and go with that result. The SCV (or ISSM) should document this conflict in the POA&M’s comment column.

Appendix F SYSTEM CATEGORIZATION

Under the RMF, system security categorization sets the foundation for the system's security requirements as defined by the security controls. Categorization must take place early in the system acquisition lifecycle in order for a program to establish a secure system architecture at a time when it is easiest and least expensive to implement. In the past under DIACAP, the determination of impact levels for confidentiality, integrity, and availability (hereafter referred to as C-I-A) was often made subjectively. Incorrectly determining the impact values could lead to under-protecting or over-protecting an information system. Neither scenario is desirable; the former case leads to poorly secured information systems, and he latter case leads to higher cost for marginal benefit. The RMF system security categorization process gives an objective approach to help determine the security requirements based on risk and impact on mission due to loss of C-I-A.

Defining System Categorization

System categorization assigns impact values of low, moderate, or high to the three security objectives: C-I-A. The DoD uses CNSSI 1253 (reference (c)) as the guide for determining categorization, and the USMC follows the same process. The descriptions in Table F-1 are a summary of system security categorization.

The impact values of low, moderate, or high are assigned based upon the anticipated magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or the loss of information or information system availability. Table F-1, taken from FIPS Pub 199 (reference (f)), lists the potential impact definitions for each security objective.

Table F-1: Impact Values from FIPS Pub 199

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

When system security categorization is complete, an information system will have a categorization in the following format:

$$\text{Security Category}_{IS} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\}$$

An example of a system security categorization would be as follows:

$$\text{Security Category}_{IS} = \{(\text{C, Moderate}), (\text{I, High}), (\text{A, Low})\}$$

How to Categorize a System

To categorize a system properly, stakeholders must first categorize each of the information types the information system will process, store, or transmit. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management, etc.) defined by an organization or, in some instances, by a public law, executive order, directive, policy, or regulation.

NIST Special Publication 800-60 Volume II (reference (i)) provides an extensive list of information types for *Mission-based* systems and *Management and Support* systems. This NIST publication identifies approximately 170 information types for the *Mission-based* systems and *Management and Support* systems.

It is important to determine which mission or function the system serves prior to selecting information types. Per the NIST Special Publication 800-60 Volume 1 (reference (h)), *Management and Support* systems "are primarily intended to provide administrative or business services that support mission accomplishment." *Mission-based* systems are primarily "to support provision of basic services to U.S. citizens and residents. This addresses information types associated with both services provided by the Federal government to citizens and mechanisms used to achieve the purposes of government or deliver services for citizens."

The following list of questions may help to identify the information types processed, stored, or transmitted by the system:

1. Does the information directly support the warfighting mission? If so, it should be considered a *Defense* or *National Security* information type.
2. Does the information provide administrative support to the warfighter, such as policy development or workforce planning? If so, it should be considered a *Management and Support* information type.
3. Does the information provide services to the warfighter, such as energy or housing? Then it should be considered a *Mission-based* information type.

Once the stakeholders identify the information types for a system, the next step is for the stakeholders to assign impact values (see Table F-1) to each of the applicable information types. The stakeholder should develop a table of applicable information types and impact values, which will make it easier to come up with the system security categorization.

The final step for system security categorization is for the stakeholders to use the high-water mark for each information type within each security objective. The highest impact value of the information types within each security objective will represent the system security categorization.

Table F-2 provides a notional example of information types for an information system, the provisional impact values, and the resulting system security categorization.

Table F-2: Example of Information Types and Security Categorization

Information Type	**Provisional Impact Values**		
	C	**I**	**A**
Intelligence	H	H	M
Weather	L	M	L
Logistics	L	M	M
Air Tasking Orders	M	H	M
Cost Accounting	L	M	L
System Categorization	**H**	**H**	**M**

Appendix G **RISK ASSESSMENT REPORT**

This appendix describes the MCSC Risk Assessment Report (RAR). It aligns with the content of the DoD Cybersecurity Risk Assessment Guide (reference (w)), which provides a risk assessment methodology consistent with NIST SP 800-30 r1 (reference (l)). Adopting the methodology of the DoD Cybersecurity Risk Assessment Guide ensures the development of the RAR follows the DoD guidelines. Also, it ensures the DoD's risk factors and their descriptions within this appendix map directly back to NIST SP 800-30. In addition to relying on the DoD Cybersecurity Risk Assessment Guide, this appendix uses the content of the RMF KS website[22], which offers the cybersecurity workforce useful insight for conducting security control assessments and completing a RAR. While DoDI 8510.01 (reference (a)) does not explicitly require a RAR, the RMF KS points out that the RAR "is essential supporting material to the security assessment report (SAR)." The RMF KS also states the RAR "contains information not available elsewhere that an organization can use to communicate the results of risk assessments for those security controls identified as non-compliant within the SAR."

The DoD Cybersecurity Risk Assessment Guide describes how the analytical approach affects the risk assessment process. The DoD guide cites three analytical approaches: (1) threat-oriented, (2) asset/impact-oriented, and (3) vulnerability-oriented. The most appropriate analytical approach for conducting security control assessments is the vulnerability-oriented approach. That approach begins with a set of predisposing conditions or weaknesses (e.g., non-compliant security controls) and then provides a method to estimate the likelihood threat sources will initiate or cause threat events that could exploit those vulnerabilities and cause an adverse impact. This RAR appendix follows this vulnerability-oriented approach. As such, this appendix offers a RAR template that includes risk factors beginning with identifying the vulnerabilities or predisposing conditions. The RAR template then addresses the severity or pervasiveness of vulnerabilities, followed by determining the likelihood of threat events resulting in adverse impact, and ends with assigning a risk value.

The MCSC RAR provides the risk assessment of non-compliant security controls and vulnerabilities. The RAR reflects the findings, whether the assessment was conducted (1) as part of the program's self-assessment or (2) as the security control assessment performed by the security control validator. The non-compliant controls must go through a risk assessment process to identify the residual risk for each non-compliant control. In turn, the security control assessor uses the RAR to develop a recommendation to the authorizing official of the system's overall risk level within its intended operational environment.

This appendix explains the information elements, hereafter called "fields," for the MCSC RAR template. Most of the fields and their descriptions trace to either the RMF KS or the DoD RAR template available for download on that website. If more detail and explanation is needed for RAR content then refer to the DoD Risk Assessment Guide and NIST SP 800-30. For example, the RMF KS has one table for assigning threat relevance, which is a combination of multiple factors. NIST SP 800-30 describes each of those factors in more depth. The MCSC RAR template also includes two fields not identified in the RMF KS -- Vulnerability ID and Asset Affected.

[22] https://rmfks.osd.mil/rmf/RMFImplementation/AssessControls/Pages/ResidualRisk.aspx

One other note on how the approach of the DoD Cybersecurity Risk Assessment Guide is consistent with NIST SP 800-30, yet implements a specific aspect for DoD use. The DoD guide identifies the five qualitative values (e.g., Very High, High, Moderate, Low, Very Low) for the risk factors, whereas NIST SP 800-30 uses the qualitative values along with the associated quantitative values. This appendix sticks with the DoD approach of using only the qualitative terms.

Table G-1 lists the fields for the MCSC RAR template and describes the content of the fields. The succeeding tables provide descriptions for some of the risk factors as well as 5x5 matrices for assigning values to some of the risk factors.

Table G-1 RAR Fields

Field Name	Value	Field Description/Instructions
Non-Compliant Security Control		The applicable security control/enhancement associated with the vulnerability. If more than one security control is associated with the vulnerability, then list all security controls on separate lines and repeat the vulnerability description.
Vulnerability ID		The vulnerability identifier. The STIG or vulnerability scanner most often provides the vulnerability ID.
Vulnerability Description		Describe the vulnerability associated with each non-compliant security control. The STIG or vulnerability scanner most often provides the vulnerability details.
Security Objectives	C, I, or A	Identify the security objective (Confidentiality, Integrity, and/or Availability) supported by the security control/enhancement by using C, I, or A. See CNSSI No. 1253, Table D-2, Additional Security Control Information, for security objectives related to the controls. In some cases security controls may support multiple security objectives and should be separated by a hyphen "-" (e.g., C-I or C-I-A or C-A or I-A).
Severity or Pervasiveness	VH, H, M, L, VL[23]	The *severity* value is assigned to the vulnerability, but a *pervasiveness* value is assigned to predisposing conditions. The PM estimates this value based on a comparison of the raw findings during the security control assessment and the effectiveness of mitigation actions. If mitigations are completely effective, this value is non-existent and the remainder of the cells in the row would contain no values, as there can be no likelihood of exploitation, impact, or risk. This value is determined by assessment at the control correlation identifier (CCI) level. If a control has a STIG or SRG associated through CCIs, the vulnerabilities identified by STIG or SRG assessments will be used for the value in this column, but there is not a one-to-one correlation between raw STIG CAT values (i.e., CAT I, CAT II, CAT III) and this value. (See Table G-2 below for descriptions of the values for severity or pervasiveness.)
Threat Relevance	VH, H, M, L, VL	The threat relevance combines potential threat events, relevance of the events, and threat sources that could initiate the events. If threat relevance does not meet the organization's criteria for further consideration, do not complete the remaining columns, as there is no risk. This factor is based on the risk assessor's estimate after considering a combination of an adversarial threat source's *capability*, *intent*, and *targeting* or a non-adversarial threat source's range of effects based on available evidence, experience, and expert judgment. This

[23] VH = Very High, H = High, M = Moderate, L = Low, VL = Very Low

		factor considers multiple NIST SP 800-30 risk factors; that is, which threat sources may initiate which threat events against the vulnerability or predisposing condition. There is a many-to-many relationship between these risk factors. While this model simplifies this relationship and assignment of a value, risk assessors may want to review NIST SP 800-30 to understand the factors, examine the exemplar lists of these factors, and separately document how these relationships were examined and measured. (See Table G-3 below for descriptions of values for threat relevance.)
Likelihood	VH, H, M, L, VL	The likelihood a threat event will be initiated or occur and result in adverse impacts. (See Table G-4 below for descriptions of the values for likelihood.) Likelihood is a combination of likelihood of attack initiation/occurrence and likelihood the initiated attack succeeds or the threat even results in adverse impact. If resource constraints allow, risk assessors may reference NIST SP 800-30 for guidance on determining this value (i.e., could use another 5x5 matrix to plot the two factors and determine the overall likelihood.) However, as the likelihood is summarized herein, risk assessors assign a likelihood value by comparing the results of "Severity or Pervasiveness" with "Threat Relevance." The factors from these two columns are plotted on a 5x5 matrix, and the intersection on the matrix indicates the value for likelihood. (See Table G- 5 below for the 5x5 matrix to assign the likelihood value based on severity (or pervasiveness) and threat relevance.)
Impact	VH, H, M, L, VL	The adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. Risk assessors may consider the concept of operations, system description, user representative input, etc. (See Table G-6 below for descriptions of the values for impact.)
Impact Description		The operational impact due to the non-compliant security control.
Risk		This risk as a combination of likelihood and impact. (See Table G-7 below for descriptions of values assigned to risk.) Risk assessors assign a value by comparing the results "Likelihood" with "Impact." The factors from these columns are plotted on a 5x5 matrix, and the intersection on the matrix indicates the value for risk.

		(See Table G-8 below for the 5x5 matrix to assign the risk value based on likelihood and impact.)
Proposed Mitigation		The proposed mitigations that, if implemented, will reduce the risk.
Residual Risk		The risk level expected ***after the initial mitigations*** are implemented. These mitigations are included in the POA&M.
Asset Affected		The asset or device affected by the vulnerability.
Recommendations		The program manager lists the recommendations to address actions that will, at a minimum, reduce the High and Very High Risk non-compliant security controls to a Moderate residual risk level.

Vulnerability Severity and Pervasiveness of Predisposing Conditions

Table G-2 describes the assessment scale of vulnerability severity and pervasiveness of predisposing conditions. The DoD Cybersecurity Risk Assessment Guide identifies two separate tables – one for vulnerability severity and the other for pervasiveness of predisposing conditions. Since the RMF KS approach merges the two tables, the RMF KS table is used in this appendix.

Table G-2 Vulnerability Severity or Pervasiveness[24]

Value	Severity or Pervasiveness Description
Very High (VH)	Vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability. ***--OR--*** Predisposing condition applies to all organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
High (H)	Vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective. ***--OR--*** Predisposing condition applies to most organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Moderate (M)	Vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective. ***--OR--*** Predisposing condition applies to many organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Low (L)	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective. ***--OR--*** Predisposing condition applies to some organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Very Low (VL)	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective. ***--OR--*** Predisposing condition applies to few organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

[24] Source: RMF KS, *Model for Assessing Residual Risk Level for Non-Compliant Security Controls*, Table 3

Relevance of Threat

Table G-3 is a compilation of the threat-related risk factors of five different tables from the DoD Cybersecurity Risk Assessment Guide, equating to the *threat event* attributes and the *threat source* attributes of capability, intent, and targeting. This appendix adopted the RMF KS approach of one merged table for threat relevance.

Table G-3 Threat Relevance[25]

Value	Relevance of Threat Description
Very High (VH)	Threat event or TTP has been seen by the organization. **Confirmed**, and… Adversarial: The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks. The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals. The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations. ***--OR--*** Non-adversarial: The effects of the error, accident, or act of nature are **sweeping**, involving almost all of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure].
High (H)	Threat event or TTP has been seen by the organization's peers or partners. **Expected**, and… Adversarial: The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks. The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks. The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions. ***--OR--*** Non-adversarial: The effects of the error, accident, or act of nature are **extensive**, involving most of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including many critical resources.
Moderate (M)	Threat event or TTP has been reported by a trusted source. **Anticipated**, and...

[25] Source: RMF KS, *Model for Assessing Residual Risk Level for Non-Compliant Security Controls*, Table 4

	Adversarial: The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks. The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's missions/business functions to achieve these ends. The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information. ***--OR--*** Non-adversarial: The effects of the error, accident, or act of nature are **wide-ranging**, involving a significant portion of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including some critical resources.
Low (L)	Threat event or TTP has been predicted by a trusted source. **Predicted**, and… Adversarial: The adversary has limited resources, expertise, and opportunities to support a successful attack. The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft. The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class. ***--OR--*** Non-adversarial: The effects of the error, accident, or act of nature are **limited**, involving some of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], but involving no critical resources.
Very Low (VL)	Threat event or TTP has been described by a somewhat credible source. **Possible**, and... Adversarial: The adversary has very limited resources, expertise, and opportunities to support a successful attack. The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft. The adversary may or may not target any specific organizations or classes of organizations. ***--OR--*** Non-adversarial: The effects of the error, accident, or act of nature are **minimal**, involving few if any of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], and involving no critical resources.

Likelihood

Table G-4 describes the likelihood values. Likelihood, as explained by the DoD Risk Assessment Guide and used herein, is the likelihood a threat event will occur or be initiated by an adversary and the likelihood the initiation or occurrence of that threat event will results in adverse impact.

Table G-5 is the 5x5 matrix for determining the likelihood values.

Table G-4 Likelihood Descriptions[26]

Value	Likelihood Description
Very High (VH)	Adversarial: Adversary is **almost certain** to initiate the threat event (i.e., adversary capability, intent, and/or targeting are very high). ***--OR--*** Non-adversarial: Error, accident, or act of nature is **almost certain** to occur; or **occurs more than 100 times a yea**r. And, if the threat event is initiated or occurs, it is **almost certai**n to have adverse impacts.
High (H)	Adversarial: Adversary is **highly likely** to initiate the threat even (i.e., adversary capability, intent, and/or targeting are high). ***--OR--*** Non-adversarial: Error, accident, or act of nature is **highly likel**y to occur; or **occurs between 10-100 times a year**. And, if the threat event is initiated or occurs, it is **highly likel**y to have adverse impacts.
Moderate (M)	Adversarial: Adversary is **somewhat likely** to initiate the threat event (i.e., adversary capability, intent, and targeting are moderate). ***--OR--*** Non-adversarial: Error, accident, or act of nature is **somewhat likely** to occur; or **occurs between 1-10 times a year**. And, if the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low (L)	Adversarial: Adversary is **unlikely** to initiate the threat event (i.e., adversary capability, intent, and/or targeting are low). ***--OR--*** Non-adversarial: Error, accident, or act of nature is **unlikely** to occur; or **occurs less than once a year, but more than once every 10 years**. And, if the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low (VL)	Adversarial: Adversary is **highly unlikely** to initiate the threat event (i.e., adversary capability, intent, and/or targeting are very low). ***--OR--*** Non-adversarial: Error, accident, or act of nature is **highly unlikely** to occur; or **occurs less than once every 10 years**. And, if the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

[26] Source: RMF KS, *Model for Assessing Residual Risk Level for Non-Compliant Security Controls*, Table 5

Table G-5 Overall Likelihood Rating[27]

Relevance of Threat	Vulnerability Severity/Predisposing Condition Pervasiveness				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

[27] Source: RMF KS, *Model for Assessing Residual Risk Level for Non-Compliant Security Controls*, Table 8

Impact

Table G-6 provides the descriptions for the impact values. The DoD Cybersecurity Risk Assessment Guide describes this risk factor as the adverse impacts from threat events given: (1) the threat sources that could initiate the events; (2) the vulnerabilities and predisposing conditions; and (3) the susceptibility reflecting the safeguards (i.e., compliant and effective security controls) planned or implemented to impede those threat events. (A planned safeguard cannot provide mitigation, but the AO may consider if a future safeguard will be effective in mitigating a risk accepted in the interim.)

Table G-6 Impact Descriptions[28]

Value	Impact Description
Very High (VH)	The threat event could be expected to have **multiple severe or catastrophic** adverse effects.
High (H)	The threat event could be expected to have a **severe or catastrophic** adverse effect. For example, the threat event might: (i) cause severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate (M)	The threat event could be expected to have a **serious** adverse effect. For example, the threat event might: (i) cause significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low (L)	The threat event could be expected to have a **limited** adverse effect. For example, the threat event might: (i) cause degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low (VL)	The threat event could be expected to have a **negligible** adverse effect.

[28] Source: RMF KS, *Model for Assessing Residual Risk Level for Non-Compliant Security Controls*, Table 6

Table G-7 provides descriptions of the risk values. The DoD Cybersecurity Risk Assessment Guide describes risk as the risk to the organizational operations, organizational assets, individuals, other organizations, or the Nation from the identified threat events given: (1) the impact that would result from the events; and (2) the likelihood of the events occurring. The level of risk associated with identified threat events represents a determination of the degree to which organizational operations, organizational assets, individuals, other organizations, or the Nation are threatened by those the events. When assessing risk from a vulnerability-oriented approach, each risk corresponds to a specific vulnerability (e.g., non-compliant security control). In general, the risk level is typically not higher than the level of impact, and likelihood can serve to reduce risk below that level.

Table G-8 is the 5x5 matrix for assigning the risk value based on impact and likelihood.

Table G-7 Risk Descriptions[29]

Value	Risk Description
Very High (VH)	A threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High (H)	A threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate (M)	A threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low (L)	A threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low (VL)	A threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table G-8 Risk[30]

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	*Very Low*	*Low*	*Moderate*	*High*	*Very High*
High	*Very Low*	*Low*	*Moderate*	*High*	*Very High*
Moderate	*Very Low*	*Low*	*Moderate*	*Moderate*	*High*
Low	*Very Low*	*Low*	*Low*	*Low*	*Moderate*
Very Low	*Very Low*	*Very Low*	*Low*	*Low*	*Low*

[29] Source: RMF KS, *Model for Assessing Residual Risk Level for Non-Compliant Security Controls*, Table 7
[30] Source: RMF KS, *Model for Assessing Residual Risk Level for Non-Compliant Security Controls*, Table 9

Appendix H **SECURITY ASSESSMENT PLAN**

The SAP captures all of the procedures and tools used to assess all components identified in the system's authorization boundary. The SAP also should include a list of devices in the authorization boundary, tools to be used, and applicable Security Requirements Guides (SRGs), STIGs, and SCAP benchmarks to be assessed. A complete list of artifacts, SRGs, STIGs, and SCAP benchmarks can be found on the DISA Information Assurance Support Environment (IASE) website.[31]

A SAP is generated by the PM or ISSM for the self-assessment; another SAP is generated by the SCV for the validation.

The plan is broken down into the five sections as follows:

a. **Introduction**. This contains the basic who and what of the test plan. Who is performing the testing, what the purpose and objectives are, and the timeframe of the test is to be conducted. This section also discussions test limitations or deviations from the standard test methods.

b. **Test Architecture**. This is a discussion of the test environment. It includes where the testing is to be conducted, what the equipment configuration is, and what type of test equipment and personnel will be required. Additionally, this section must include any deviations from the normal operating mode of the system or deviations from normal test methods along with justification.

c. **Test Process Overview**. This is the first section on the execution of the test plan. It establishes the grading, entrance, and exit criteria, any certification requirements, and any governing instructions. In short, this section contains the ground rules for the test.

d. **Test Procedures**. This section contains the detailed procedures for each test. It is likely that most test plans will have the procedures section in a separate document due to size and maintenance requirements.

e. **Security Test Report**. This section captures specific elements related to testing not contained elsewhere. This report provides additional information useful for documenting test events and any conditions or exceptions realized during the event that may require further review.

Note: Programs must follow the classification instructions per the program's SCG. Stakeholders must pay special attention to the data handling and dissemination of test results, in particular the vulnerability results.

[31] http://iase.disa.mil/stigs/Pages/index.aspx

Appendix I SECURITY ASSESSMENT REPORT

The SAR contains the results of the security control assessment, including recommendations to fix deficiencies in the controls. It includes information from the SCV necessary to determine effectiveness of the security controls employed within or inherited by the information system based upon the SCV's findings. The AO relies on the SAR as the primary document to determine risk to organizational operations and assets, individuals, other organizations, and the nation

The SAR documents the SCV's assessment of a program's compliance with approved security controls. It addresses security controls in a non-compliant status, including existing and planned mitigations. A SAR is always required before an authorization decision. If a compelling mission or business need requires the rapid introduction of a new IS (e.g., urgent need statement), assessment activity and a SAR are still required.

The RMF KS has a template for a SAR[32]; it is contained within the RMF Core Security Authorization Package spreadsheet as a separate tab along with accompanying instructions.

The following is a summary of some of the information contained within the SAR:

- Information system details, to include system security categorization
- Stakeholder names
- List of applicable security controls
- Each control in the SAR has these fields:
    - Common Control Provider, if applicable
    - Overlay, if the control is part of the final control due to overlay applicability
    - Compliance status (compliant, non-compliant, N/A)
    - N/A justification
    - Vulnerability summary for the security control that includes vulnerabilities identified during the assessment
    - Security control risk level (i.e., remaining risk after mitigation). Per RMF KS, the risk levels are
        - Very High
        - High
        - Moderate
        - Low
        - Very low
    - Recommendations from SCV for correcting control deficiency, which must include a recommendation to fix, mitigate, or accept risk.

[32] https://rmfks.osd.mil/rmf/General/SecAuthPackage/Pages/SAR.aspx

Appendix J **SECURITY PLAN**

The SP, a critical part of the Security Authorization Package, provides the essential programmatic, mission, architectural, and security details about the information system. The information for an SP will be entirely contained within MCCAST, and the SP can be exported from MCCAST for external review and coordination. When exported, the SP will contain the system's name, acronym, DITPR-DON identification, version information, points of contact for those responsible for the system during the assessment process, and the implementation plan for the security controls.

Note: The system name in MCCAST should match the DITPR-DON record. If they do not match, the PM or ISSM must provide a justification for the discrepancy.

The SP is initiated during Step 1 of the RMF process. Much of the information required in the SP exists in system design and mission description documentation.

An initial SP is a requirement at the RMF Step 2; the completed SP is a requirement for the final authorization decision. The ISSM is responsible for preparing the SP and ensuring all system information is captured thoroughly and correctly as the system proceeds through the RMF process.

Transition Note: The DIACAP System Security Plan and C&A Plan contain much of the same content, if not formatting, as the RMF SP and can be used to build an almost complete SP for systems with existing packages. During transition of the information to the RMF SP template, all data should be re-verified to ensure it is still accurate.

Security Plan Content

All MCSC systems must use MCCAST to capture the required SP information. The following information should be entered into the MCCAST record.

Items required for the RMF Step 2 are identified as **underlined** items below. All other items are required for the final authorization decision.

- **System name, acronym, and version number**: Includes the full descriptive system name, the acronym (if applicable), and the specific system version that is being assessed.
- **System Description**: Provides a narrative description of the system, its major components and interfaces and their function, a description of the function of each asset within the assessment boundary, and the system uses. Information identified here should include whether the system is stand-alone or connected and should identify the lead service if it is a reciprocity package.
- **System Type**: Identifies the DoD IT type of the system. The four options are Platform IT, IS Major Application, IS Enclave, or Platform IT System.
- **National Security System (NSS)**: Identifies whether the system is a NSS.

- **System Lifecycle/Acquisition Phase**: Identifies where the system is in the development lifecycle. The selection options are: Pre-Milestone A (Material Solution Analysis); Post-Milestone A (Technology Maturation and Risk Reduction); Post-Milestone B (Engineering and Manufacturing Development); Post-Milestone C (Production and Deployment); Post-Full Rate Production/Deployment Decision (Operations and Support).
- **Authorization Status:** Identifies the current authorization status of the system. Selection options are: Not Yet Authorized, ATO, ATO with Conditions, IATT, and DATO.
- **Ports, Protocols, and Services Management (PPSM) Registry Number**: Identifies the PPSM registry number is the identification assigned by DISA when a system's PPS list has been submitted.
- **System Identification (DITPR-DON ID)**: Identifies the numerical system identifier used to uniquely identify the system within DITPR-DON. This number is received when the system is registered in DITPR-DON. For reciprocity systems, the DITPR number may be used.
- **Governing Mission Area**: Identifies the business area that governs the system's mission requirements. Selection options are: Enterprise Information Environment MA (EIEMA); Business MA (BMA); Warfighting MA (WMA); DoD portion of the Intelligence MA (DIMA).
- **Mission Criticality**: Identifies the mission criticality of the system from the following options: Mission Critical (MC), Mission Essential (ME), or Mission Support (MS).
- **Type or Site Authorization**: Identifies whether the system needs a Type (multiple locations) or Site (one location) authorization.
- **DoD Security Control Set**: Under RMF, NIST Special Publication 800-53 (reference (j)) this identifies the library of controls for the control set baseline for the system.
- **RMF Points of Contact**: Identifies the system personnel assigned to RMF roles. As indicated in MCCAST, mandatory roles are AO, SCA, ISSM, UR and PM. Other roles that should be identified include SCA Analyst, SCV, ISSO, and ISSE.
- **System Authorization Boundary Diagram**: Provides a diagram of the system with all system components in the authorization boundary identified. The authorization boundary must be indicated by a dotted red line around the system components. If a component is not to be assessed as part of the Security Authorization Package, it should be outside of the authorization boundary on the diagram, regardless of where it sits physically in location to the system. The following items must be included:
    - System components – should map to the hardware list
    - Location within the architecture
    - Interfaces
    - Data flows
    - Ports and protocols – should map to the PPS table

- **Hardware/Firmware**: Provides a list of all hardware included within the previously identified system authorization boundary and that hardware's associated firmware. The hardware/firmware list must include the following information for each component:
    - Device name
    - Manufacturer
    - Model number
    - Firmware version
    - IA or IA-enabled (Yes/No)
        - If IA-enabled, identify the Common Criteria Evaluation Assurance Level)
- **Software**: Provides a list of all software existing on the system. The software list must include the following information for each piece of software:
    - Name
    - Acronym
    - Version
    - Function
    - Software Category (Commercial Off-the-Shelf [COTS], Government Off-The-Shelf [GOTS], Modified COTS)
    - IA or IA-enabled (Yes/No) (per CNSSI 4009 definition (reference (s))
    - Functional Area Manager (FAM) Approval Status
    - DADMS Identification
    - DADMS Approval Status (list any restrictions, if applicable)
    - DADMS Last Date Allowed
    - Externally Assessed or Authorized (Yes/No - Mark yes for any software loaded but not part of the assessment boundary)

  The software list should be developed from the system design documentation.
- **Network Connection Rules**: Provides a link to or list of the network connection rules for communicating with external systems. Information from the Interconnection Agreements can be used for the description. This list can be developed based on already developed Interconnection Agreements, Memorandums of Understanding (MOUs), MOAs, and any functional requirements identified in the system design documentation. The Category Assurance List (CAL) boundaries should also be identified.
- **System Ownership/Controlled**: Identifies the ownership/operation of the system. The options are: DoD Owned and DoD Operated IS; DoD Owned and Non-DoD Operated IS; DoD Controlled/Non-DoD Owned and Operated IS; DoD-Partnered System.
- **System Categorization**: Identifies the system security category developed as described in Appendix F of this guide.

- **Applied Overlays**: Identifies overlays applied to the security control set for the system. This is determined per the process described in Section 4 of this guide.
- **Implementation Status/Security Controls Status table**: Represents the implementation plan of the security controls for the system. All of the security controls, their statuses, and their implementation details must be addressed. The following fields must be addressed for every planned or implemented security control:
    - Security Control Number – the reference number for the security control per the NIST Special Publication 800-53 (reference (j)).
    - Implementation Status – Status options are Compliant and Not Compliant.
    - Implementation Notes – ISSMs will explain either how the control is being implemented (compliant) or why the control cannot be implemented (Not Compliant).
    - Responsible Entities – Identifies the parties responsible for implementing the security control. For inherited controls where another system is responsible, the ISSM should provide MCCAST identification and DITPR-DON identification, as well.
    - Estimated Completion Date – The estimated date identifying when the control will be implemented.
    - Comments – A space to provide further clarifying information.
- **Privacy Impact Assessment (PIA)**: All systems must have a PIA completed. The PIA identifies whether or not the system has PII.
- **Physical Location**: The physical locations where the systems will be located.
- **Interconnected Information Systems and Identifiers**: Provides a list of the interconnected systems with their unique identifiers. At a minimum their MCCAST number and PPS registration number must be identified.
- **Cryptographic Key Management Information**: If the system has a Public Key Infrastructure (PKI) waiver, the AO signed waiver should be referenced in the SP and uploaded to MCCAST as an artifact.
- **System User Categories**: Provides a description of the users and their access rights and privileges for the system. The types of users include: DoD Personnel; Contractors; Federal/State/Local; Organization; Foreign Nationals; Coalition Partners; General Public. The user types should be part of the system's mission or functional requirements. The access rights and privileges should be accounted for in the system design documents.
- **Other Information**: Provides a place to include any other relevant information about the system, including security-related information discovered or used in the assessment of the system that's not reflected anywhere else.
- **Authorization Date**: If a system is currently or has previously been authorized, even if the authorization is now expired, enter the date the authorization was issued. If the system has never been authorized, this can be left blank. This can be found in the authorization letter. This is required only if applicable.

- **Authorization Termination Date**: Includes the end date of the current or previous authorization, even if it has expired. This can be found in the authorization letter. This is required only if applicable.
- **Security Review Date**: Provides the date of the last annual security review for systems with an existing authorization, or the last date the system was tested for systems with no prior authorization.

Appendix K COMMAND CYBER READINESS INSPECTIONS

CCRIs are activities that fall under the sustainment phase of the acquisition life-cycle. Therefore, CCRIs tie to RMF Step 6. Under RMF, MCSC's handling of the CCRI process will remain the same.

For tactical systems, MCSC PMs are responsible for providing a MCSC baseline POA&M to Using units each time a new system baseline is fielded. When a unit has a CCRI, the unit should use the MCSC baseline POA&M to identify what vulnerabilities are related to the current baseline.

If a vulnerability came out after the baseline was fielded, the unit should assume the vulnerability applies to the system and the vulnerability will be addressed on the next MCSC baseline POA&M.

If a unit has additional questions, the unit should contact the PM by submitting a formal request through MCSC Operations.

Appendix L **COMMENT RESOLUTION MATRIX**

Use this comment matrix when submitting comments to SIAT SSE about this guide.

Reviewer/Org./ Number/Email	Page #	Section #/ Header Name	Para #	Type C/S/A	Comments	Recommended Change	Rationale

Type (C/S/A) indicates the following:

Critical (C) - comments will cause non-concurrence with a document if comments are not satisfactorily resolved.

Substantive (S) - comments are provided because sections in the document appear to be or are potentially unnecessary, incorrect, incomplete, misleading, confusing, or inconsistent with other sections.

Administrative (A) - comments correct what appear to be typographical or grammatical errors.