

SPACE SYSTEMS COMMAND

S6

Authorization to Operate [\(ATO\)](#) Process Guide



Version 1

May 28, 2025

Prepared and Controlled by:
United States Space Force (USSF) SSC/S6 Communications
483 North Aviation Blvd, Building 270
El Segundo, CA 90245

DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government agencies and their contractors for administrative and operational use. Other requests for this document shall be referred to the USSF SSC S6 Communications.

Document Information

Document Owner	SSC S6
Maintainer	
Approver	
Status	

REVISION AND HISTORY

Revisions and version changes to this document are recorded within the following table. New versions are published when changes to the document equate to 10 percent or greater of the document's content, or if a change requires immediate implementation. This record is maintained throughout the life of the document.

This document will be reviewed at a minimum annually.

Version	Date	Description of Change	Author
1.0		Initial Draft	SSC/S6
2.0	10/28/2024	Edits throughout document	SSC/S6

Table of Contents

1	Introduction.....	6
1.1	Background	6
1.2	Scope / Purpose	7
2	Roles and Responsibilities	7
3	Risk Management Framework.....	9
3.1	Overview	9
3.2	RMF Step Descriptions and Resources.....	10
3.3	RMF Training.....	15
3.4	System Authorization Timeline	16
4	SSC S6 ATO Process.....	17
	<u>Appendix A: Process Step Tables.....</u>	<u>18</u>
	<u>Appendix B: Frequency Asked Questions (FAQs)</u>	<u>37</u>
	<u>Appendix C: Checklist.....</u>	<u>40</u>
	<u>Appendix D: Typical RMF Step Outputs for an ATO</u>	<u>54</u>
	<u>Appendix E: Appointment of Information System Security Manager (ISSM), Information System Officer (ISSO) Template</u>	<u>55</u>
	<u>Appendix F: Enterprise Mission Assurance Support Service (eMASS).....</u>	<u>58</u>
	<u>Appendix G: Information Technology Categorization Selection Checklist (ITCSC) located at AF RMF Knowledge Service (See Resources and Tools).....</u>	<u>61</u>
	<u>Appendix H: Assess Only</u>	<u>62</u>
	<u>Appendix I: Topology Guide.....</u>	<u>63</u>
	<u>Appendix J: Topology / Boundary / Data Flows / Hardware /Software / PPSM.....</u>	<u>66</u>
	<u>Appendix K: Penetration Testing.....</u>	<u>67</u>
	<u>Appendix L: ATO Prerequisites and Supporting Artifacts.....</u>	<u>69</u>
	<u>Appendix M: SSC S6 AO POA&M Policy Memo</u>	<u>71</u>
	<u>Appendix N: Service Level Agreement (SLA) Memorandum of Understanding (MOU)/ Memorandum of Agreement (MOA)</u>	<u>72</u>
	<u>Appendix O: Interconnected Systems.....</u>	<u>73</u>
	<u>Appendix P: CCSD IA Template</u>	<u>75</u>
	<u>Appendix Q: Security Impact Assessment (SIA) Template.....</u>	<u>76</u>
	<u>Appendix R: Authority to Connect (ATC) Process</u>	<u>85</u>

<u>Appendix S: United States Space Force (USSF) Information System Continuous Monitoring (ISCM) and Annual Control Validation (ACV) Policy for SSC Mission Systems</u>	87
<u>Appendix T: AO to AO Transfer Memo</u>	90
<u>Appendix U: Decommission Memo</u>	91
<u>Appendix V: References</u>	92
<u>Appendix W: NIST / RMF Training Resource Links</u>	97
Appendix A: Process Step Tables	17
Appendix B: Frequency Asked Questions (FAQs)	36
Appendix C: Checklist	39
Appendix D: Typical RMF Step Outputs for an ATO	53
Appendix E: Appointment of Information System Security Manager (ISSM), Information System Officer (ISSO) Template	54
Appendix F: Enterprise Mission Assurance Support Service (eMASS)	57
Appendix G: Information Technology Categorization Selection Checklist (ITCSC) located at AF RMF Knowledge Service (See Resources and Tools)	59
Appendix H: Assess Only	60
Appendix I: Topology Guide	61
Appendix J: Topology / Boundary / Data Flows / Hardware /Software / PPSM	64
Appendix K: Penetration Testing	65
Appendix L: ATO Prerequisites and Supporting Artifacts	66
Appendix M: SSC S6 AO POA&M Policy Memo	68
Appendix N: Service Level Agreement (SLA) Memorandum of Understanding (MOU)/ Memorandum of Agreement (MOA)	69
Appendix O: Interconnected Systems	70
Appendix P: CCSD IA Template	72
Appendix Q: Security Impact Assessment (SIA) Template	73
Appendix R: Authority to Connect (ATC) Process	82
Appendix S: United States Space Force (USSF) Information System Continuous Monitoring (ISCM) and Annual Control Validation (ACV) Policy for SSC Mission Systems	84
Appendix T: Decommission Memo	87
Appendix U: References	88
Appendix V: NIST / RMF Training Resource Links	93
Appendix W: Acronyms	94

CUI

1 INTRODUCTION

Space Systems Command (SSC), headquartered in Los Angeles, California, develops, acquires, equips, fields, and sustains critical and resilient space capabilities for warfighters. As part of fielding, SSC is responsible for launch operations, on-orbit checkout, developmental testing, sustainment, and maintenance of military satellite constellations and other Department of Defense (DoD) space systems. As the premier space capability delivery organization for the United States Space Force (USSF) and the DoD, SSC is focused on countering the very real threats in the present and future contested space domain. Through unity of effort across commercial industry, joint forces, government agencies, and academic and allied partnerships, SSC is developing resilient system-of-systems joint force space capabilities to maintain the nation's strategic advantage in space.

To meet the SSC's initiatives, the SSC S6 provides effective, innovative, and cyber-secure information technology (IT) solutions across all programs to meet warfighter and business needs. SSC S6 supports the SSC Authorizing Official (AO), who is responsible [for "USSF Space Systems Command \(SSC\) aerospace research, development, testing, and engineering systems. Boundary does not include systems identified as Space Mission Systems by Commander \(CDR\) United States Space Command \(USSPACECOM\), intelligence, medical, or systems otherwise authorized by another AO".](#)~~for making authorization decisions based on the risk present on the information systems being assessed.~~

SSC S6 ASCA conducts independent assessments on these information systems under SSC's jurisdiction through the lens of Risk Management Framework (RMF) to appraise the level of risk present, ensure that security controls are implemented correctly and are effective in protecting the information system and its networks, and ensuring that security, resilience, and dependability requirements are met at the software application, system, and network environment levels. The product of these efforts will assist the SSC AO in making prudent and well-informed authorization decisions.

1.1 Background

Federal Laws, Executive Orders, DoD, and Agency requirements mandate the adoption of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) security and risk management activities and to integrate those activities into the system development lifecycle. The RMF is a dynamic approach to risk management that effectively manages mission and cybersecurity risks in a diverse environment of complex, evolving, and sophisticated cyber threats and vulnerabilities.²² In addition to meeting these cybersecurity requirements, the implementation of RMF promotes cybersecurity continuity across the SSC S6 and its Mission Partners (MP), plays a key role in national security, and helps to protect our nation's warfighters. Due to the comprehensive and complex physical, information, and human factors present, RMF is often misunderstood or incorrectly applied. This complexity can be overwhelming for organizations, especially those with limited experience or funding. To overcome these challenges, SSC utilizes its subject matter experts (SME) in the field to offer guidance to programs to help advance their RMF goals.

1.2 Scope / Purpose

Cybersecurity requirements, as they apply to the SSC AO area of responsibility (AOR), are identified throughout this document. This Process Guide will aid SSC S6 stakeholders in the application of the DoD and USSF assessment and authorization (A&A) process, specific to the SSC S6 AO office in their pursuit of an Authority to Operate (ATO). It provides a checklist, references, templates, and resources to navigate and help ease the complexity of the ATO request process. An operational system or system connection to mission data must meet these standards to be considered for an authorization. The checklist will act as a guide and will explain each of the RMF steps for the Program, SCAR, and ASCA teams. This will help to ensure that all information is provided within the documentation. To be considered for authorization, any operational system or connection to mission data must comply with the established standards. The included checklist serves as a step-by-step guide through the Risk Management Framework (RMF) process, providing clear direction for Program, SCAR, and ASCA teams. It is designed to ensure that all necessary information is accurately captured and documented throughout the ATO submission process.

2 ROLES AND RESPONSIBILITIES

Table 1 provides a high-level description of responsibilities for RMF roles. They are captured from several sources. (For example: RMF Knowledge Service (KS), NIST guidance, federal, DoD, and/or Agency Instruction). Detailed RMF responsibilities can be found within the ATO Process Step Tables in Appendix A. Or, by referencing the following:

- Department of Defense Instruction (DoDI) 8500.01, March 14, 2014, *Cybersecurity*
- DoDI 8510.01, July 19, 2022, *Risk Management Framework for DoD Systems*
- AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT)
- Risk Management Framework Knowledge Service (RMF KS): <https://rmfks.osd.mil>

Organizations may distribute RMF responsibilities across their workforce and/or their organizational structure to accommodate mission requirements. For example, organizations may not implement or assign an Information System Security Officer (ISSO) to their environment. However, fulfilling the RMF responsibilities throughout the entire system lifecycle (including assessment and authorization) is a federal and DoD requirement.

Table 1. RMF Roles and Responsibilities

RMF Role	RMF Responsibilities	Reference(s)
Authorizing Official (AO)	Responsible for making the authorization decision, based on risk acceptance, by granting or denying an ATO or other authorization. The AO is usually a general officer (GO) or senior executive service (SES) and is appointed by a higher authority responsible for overall hierarchy. The AO is responsible for accepting the risk associated with operating the system under their purview.	DoDI 8510.01
Authorizing Official Designated	Can represent the AO for most issues and makes recommendations to the AO; however, the AODR does not	DoDI 8510.01

Representative (AODR)	grant an ATO or other authorizations. An AODR is appointed by the AO and is usually an O5 or GS14.	
Security Control Assessor or Security Control Assessor Representative (SCA/SCAR)	Appointed by the Chief Information Security Officer (CISO) and is usually an O4 or GS13. The SCA/SCAR is responsible for the assessment determination within their assigned AOR. The SCA's will analyze Cybersecurity Risk Assessment's (CRA's), consider mitigating factors, and implement and oversee the organization wide continuous monitoring strategy.	DoDI 8510 AFI 17-101
Agent of the Security Control Assessor (ASCA)	The ASCA is a licensed 3rd-party agent that assists in assessment activities and provides an independent report for the SCA. This position cannot make decisions on behalf of the government; the ASCA can only provide advice and guidance.	AFI 17-101
Chief Information Officer (CIO)	Responsible for IT investment management and the processes for all annual and multi-year IT planning, programming, and budgeting decisions. Responsible for the processes for managing, evaluating, and assessing how well the agency is managing its IT resources.	
Information Owner (IO)	An IO is an organizational official with statutory, management, or operational authority for specific information. The IO position is occupied by a government employee with capital investment authority.	DoDI 8500.01 NIST 800-37r2
Information System Owner (ISO)	Official responsible for the overall procurement, development, integration, modification, operation, and maintenance of AF IT. Will ensure, with coordination of the Program Manager (PM) staff, the development, maintenance, and tracking of the system security plan for the assigned IT.	CNSSI 4009
Information System Security Engineer (ISSE)	Responsible for information security engineering activities. They should use best practices to implement security controls, such as secure design, architecture, and coding techniques. The ISSE should work with the Information System Security Manager (ISSM), information security architect, ISSO, ISO, and common control provider to coordinate security activities. Additionally, the ISSE will analyze security control status by responding to test results in Enterprise Mission Assurance Support Service (eMASS). The ISSE has a supporting role in developing a system-level continuous monitoring strategy and determining the security impact of proposed or actual changes to the Information System (IS) and its operational environment.	DoDI 8510.01
Information System Security Manager (ISSM)	Responsible for the information assurance (IA) of a program. The organization's cybersecurity program is developed by the ISSM and includes cybersecurity architecture, requirements, objectives, policies, personnel, as well as processes and procedures. ISSMs are also responsible for the continuous monitoring of systems within their purview to ensure compliance with requirements and policies.	DoDI 8510.01
Information System Security Officer (ISSO)	Assist the ISSM's meet cybersecurity requirements and maintenance of the overall security posture of the systems for the program. Per DoDI 8500.01, "When circumstances warrant, a single individual may fulfill both the ISSM and the ISSO roles".	DoDI 8510.01
Program Manager (PM)	Must identify, implement, and ensure full integration of cybersecurity into all phases of the acquisition, upgrade, or	DoDI 5000.02

	modification programs, including initial design, development, testing, fielding, operation, and sustainment in accordance with (IAW) DoDI 8500.01 and DoDI 8510.01.	
--	---	--

3 RISK MANAGEMENT FRAMEWORK

3.1 Overview

This section provides a comprehensive overview of the RMF processes. This section serves as a valuable guide for understanding the conventional approach to A&A. Per NIST, “The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. Managing organizational risk is paramount to effective information security and privacy programs; the RMF approach can be applied to new and legacy systems, any type of system or technology (e.g., Internet of Things (IoT), control systems), and within any type of organization regardless of size or sector”.

In coordination with DoD Directives (DoDD), Committee on National Security Systems (CNSS) policies, and AFIs, the RMF process employs the NIST RMF in accordance with NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* and DoDI 8510.01. This ensures compliance with the Federal Information Security Modernization Act (FISMA) requirements. The RMF process is the foundation for ATO workflows and approvals within cybersecurity. There are currently seven steps to RMF. Figure 1 depicts the RMF process workflow as a sequential process. However, after the Prepare (Process Initiation) step, the RMF provides for flexibility in its implementation based on organizational and/or mission requirements. The overall objective is to meet federal, DoD, Agency, and local cybersecurity requirements while integrating information system security with the system life cycle and system security engineering processes.

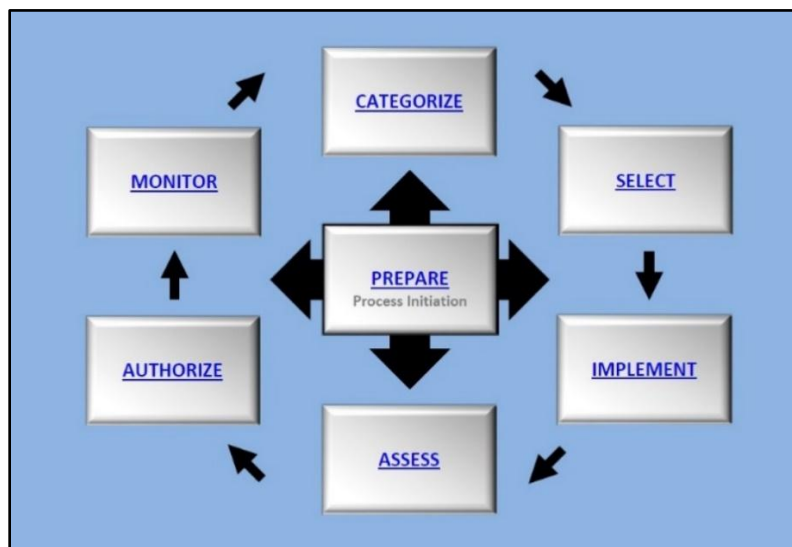


Figure 1. RMF Steps 0-6 (Source NIST)

3.2 RMF Step Descriptions and Resources

The following table provides broad guidance and familiarization on the activities and resources required to achieve milestone decisions during RMF steps. More detailed steps are provided within the ATO Process Flow graphic and its accompanying Process Step Table in Appendix A. Additionally, Appendix D identifies typical outputs (i.e., requirements, activities, documentation, etc.) that are associated with each step of the RMF.

Table 2: RMF Step Overview with Resources

RMF Step	Description and Resources
Step 0: Prepare	Initiate essential activities to prepare at all levels of the organization to manage its security and privacy risks using the RMF. For example: System registration, eMASS training, appointment of RMF roles. References and guidelines include: • CNSSI 4009, Committee on National Security Systems (CNSS) Glossary, March 2022 • DoD Instruction (DoDI) 8500.01, Cybersecurity • DoDI 8510.01, Risk Management Framework for DoD Systems • NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View • NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems • NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments • NIST SP 800-37r2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy • NIST SP 800-160, Vol. 1 Rev. 1, Engineering Trustworthy Secure Systems • NIST Interagency Reports (NISTIR) 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems • RMF KS, https://rmfks.osd.mil
Watch Items	Ensure the following: • Purpose and scope of the assessment is identified • Package is registered in ITIPS / DITPR / SNAP • eMASS training is completed • DD2875 has been submitted for an eMASS account • System is registered in eMASS • Artifacts are uploaded in eMASS
Step 1: Categorize	Determine the level of protection required. Categorization is based on the type of information the system stores, processes, or transmits. This will establish potential impact level (IL) (L-LOW, M-MODERATE, or H-HIGH) for the confidentiality, integrity, and availability (CIA) of the system and information. Accomplishing this step will give you the CIA rating needed for the IT Categorization Selection Checklist (ITCSC). The ITCSC must be validated by the SCA and approved by the SSC S6 AO. The SSC S6 AO will provide the official management decision to authorize the operation, testing, and connection of a system based on the implementation of an agreed-upon set of security controls. Additionally, a baseline set of security controls are established that the information system needs to implement to protect the information system. When approved, the ITCSC must be uploaded as an artifact in eMASS.

	References and guidelines include: • Committee on National Security Instruction (CNSSI) 1253, Security Categorization, and Control Selection for National Security Systems, 27 March 2014 • DoDI 8510.01, Risk Management Framework for DoD Systems • Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems • NIST SP 800-53r4/5, Security and Privacy Controls for Federal Information Systems and Organizations • NIST SP 800-59, Guideline for Identifying an Information System as a National Security System • NIST SP 800-60 Volume 1 and Volume 2 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories • RMF KS, https://rmfks.osd.mil
Watch Items	Ensure the following: • The package is submitted in the correct workflow • ITCSC Instructions are followed • The System name and Acronyms used in the System name are spelled out • The Technical Description/Purpose tells the story of <u>who</u>, <u>what</u>, <u>where</u>, <u>when</u>, <u>why</u>, and <u>how</u> the System supports the warfighter and/or other systems • The Security Description / Environment tells the story of <u>who</u>, <u>what</u>, <u>where</u>, <u>when</u>, <u>why</u>, and <u>how</u> cybersecurity and information assurance hardware and software is, or will be, protecting the System • The Authorization Boundary Topology clearly shows the cybersecurity authorization boundary. Identify any external interfaces to the IT in this section. Indicate all information exchanges (such as removable media, media for system updates, RF, Ethernet, Wi-Fi, etc.). If the system has no external interfaces, clearly state that in this section • The Authorization Boundary Topology matches the infrastructure outlined in both the Technical and Security Descriptions • The Authorizing Official is selected • The approved ITCSC is uploaded as an artifact in eMASS • The Categorization Information section for the Information Types have a justification for any reduction from the default recommended System Categorization • The CUI Information Type is added if the system is Unclassified, and the C-I-A <u>must</u> be at least a M-M-x IAW DODI 5200.48, Controlled Unclassified Information • A signature block is added for the AODR • If the package was returned for rework, ensure that <u>ALL COMMENTS ARE READ</u> before resubmitting the package back to eMASS Step 1 (i.e., packages will be returned with one of the items corrected, but additional items needed to be fixed) • A Privacy Impact Assessment (PIA) (DD2930) is submitted in eMASS as an Artifact
Step 2: Select	Select, tailor, and document the controls necessary to protect the information system and organization commensurate with, risk to organizational operations and assets, individuals, and other organizations involved. This step will determine if the system is a National Security System (NSS). If the system is a NSS, a signed Privacy Impact Analysis (PIA) is required, overlays must be identified, and verification of inheritance opportunities. References and

	-guidelines include: • CNSSI 1253, Security Categorization and Control Selection for National Security Systems • DoD RMF KS, Department of Defense (DoD) Risk Management Framework (RMF) Knowledge Service (KS) • FIPS 200, Minimum Security Requirements for Federal Information and Information Systems • NIST SP 800-30, Guide for Conducting Risk Assessments • NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organization • NIST SP 800-53B, Control Baselines for Information Systems and Organizations • NIST SP 800-59, Guideline for Identifying an Information System as a National Security System
Watch Items	Ensure the following: • The package is submitted in the correct workflow • Explain in specific detail how a control cannot be technically performed, implemented, and/or applied to a system if a control is non-applicable (NA). Controls that are being met due to implementation of other technical or procedural controls are “Compliant” not “NA”. Explain and justify this in the mitigation • Controls marked NA are re-evaluated to ensure that legitimate justification is provided that explains, in detail, how each control cannot be technically performed, implemented, exploited, and/or applied to the system. NA Controls are security controls that are not <u>technically</u> or <u>procedurally</u> relevant to the system • USSF RMF-C inheritance package is added in eMASS • Next ATO submitted 60-90 days from the Authorization Termination Date (ATD) • It is recommended to READ ALL COMMENTS before resubmitting the package back to eMASS Step 2 (i.e., packages are returned with one of the items corrected, but additional items needed to be fixed)
Step 3: Implement	Ensure that controls are implemented in the security and privacy plan and describe how the controls affect the system and the operating environment. Accomplishing this step identifies the standards needed to properly assess controls in eMASS. References and guidelines include: • DoD RMF KS, Department of Defense (DoD) Risk Management Framework (RMF) Knowledge Service (KS) • NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems • NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems • NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide • NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
Watch Items	Ensure the following: • The package is submitted in the correct workflow • The Estimated Completion Date (ECD) is changed when updating the Implementation Plan. If a control is Planned, the date must be in the future. If the control is Implemented, the date must be in the past.

Step 4: Assess	Determines if the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system, data, and organization. The result of this step provides you with the data needed to fill in the eMASS test results needed for an AO decision. References and guidelines include: • NIST SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Federal Information Systems and Organizations • NISTIR 8011, Automation Support for Security Control Assessments: Multiple Volumes
Watch Items	Ensure the following: • The package is submitted in the correct workflow • Enter a Test Result that shows the Policy/Plan, Chapter, and Page Number for the compelling evidence. If this is not completed and we are unable to locate the compelling evidence, ASCA Team will likely make this control NC and a Plan of Action & Milestone (POA&M) item will need to be created • It is recommended that you read the <u>Security Control Description and Recommended Compelling Evidence</u> as indicated in eMASS. You must state the exact location of the compelling evidence in the Test Results. If the Security Control Description indicates a process or procedure, ensure that the process or procedure is stated in the Plan or Policy. If a Plan and Policy are created, ensure that both documents are uploaded as an artifact if it contains the Compelling Evidence • Upload all Policies/Plans for the assessment. If you reference any of the documents (ex. PWS, NIST guidance, OMB, etc.) include these documents as an artifact. If these documents are referenced as Compelling Evidence and not provided, the control will be marked NC • It is recommended to READ ALL COMMENTS before resubmitting the package back to eMASS Step 4 (i.e., packages are returned with one of the items corrected, but additional items needed to be fixed) • When providing evidence, do not write in the future • The mitigation shows how the level of risk will be reduced • The mitigation statement should not be a copy and paste for all Test Results Some reasons for non-compliance: • <u>Processes</u> were not defined in the Policy or Plan. For example, Policy regurgitates the CCI definition without providing a procedure • <u>Techniques, Procedures, Methods</u> were not defined for the <u>what, when, how</u> in the Policy or Plan • <u>Agreements</u> was not provided to include (if applicable) MOA/MOU, ISA, SLA, PIA, CDS, Appointment Letters. This is not an exhaustive list of documentation- • <u>Additional Artifacts</u> was not provided (if applicable) (examples of screenshots (notification banners, etc.) DD2875s, audit trail, configuration settings, After Action Reports (AAR)), NIAP Approved Protection Profiles, <u>System Design Documentation</u>. This is not an exhaustive list of documentation- • <u>Lists</u> were not provided to include (if applicable) <u>Account Management</u>, Authorized Personnel Physical Access, system and facility access authorization, personnel or roles to be notified of formal employee sanctions, system components for vulnerability scanning, NSA approved, FIPS-201 approved products, PKI certification revocation, accounts on multiple systems, processing/storage locations. This is not an exhaustive list

	• <u>Records</u> were not provided to include (if applicable) audit, training (AT, CP, IR, SA), content of audit, system audit, change control, maintenance, sanitization, maintenance tool inspection, Remote Access, key and lock combination changes, Visitor Access, notifications of formal employee sanctions, Physical test (power supply, emergency lighting, fire suppression/detection devices/systems, Records of Rules of Behavior, Inventory of Suppliers, Vulnerability Management, PIV verification, 3rd party credential verification. This is not an exhaustive list • <u>Logs</u> were not provided to include (if applicable) Event, <u>System Backup</u>, <u>System Monitoring</u>, Maintenance, Audit, Physical Access, Visitor Access. This is not an exhaustive list • Evidence of the <u>Implementation</u> was not provided • There was no reference in the Test Results to show the evidence that the CCI is being met • Failed STIGs/Scans • If the CCI definition is to “enforce” and there is no evidence of <u>how</u> it is being enforced • If the CCI definition is to “identify” and there is no evidence of the <u>who</u> or <u>what</u> • If the CCI definition <u>does not</u> clearly define what the description is stating • If the CCI definition requests a list, a list should be provided within the Policy/Plan or an additional artifact uploaded in eMASS. Refer to List noted above. This is not an exhaustive list. • Recording, alerting, retention (auditing) • Use of unauthorized software (EoL)
Step 5: Authorize	The AO will authorize system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations, and the nation resulting from the operation of the system and the decision that this risk is acceptable. This step in the RMF process provides the program with an ATO determination and ATD. References and guidelines include: • DoDI 8510.01, Risk Management Framework for DoD Systems • NIST SP 800-30 Rev. 1, Guide to Conducting Risk Assessments
Watch Items	Ensure the following: • The package is submitted in the correct workflow • Provide a mitigation for <u>all</u> NC controls. This will help ASCA when determining the Risk. <u>Do not</u> copy and paste the Test Result that was provided by our office • It is recommended to <u>READ ALL COMMENTS</u> before resubmitting the package back to eMASS Step 5. Packages will be returned with one of the items corrected, but additional items needed to be fixed
Step 6: Monitor	Maintain ongoing situational awareness about the security and privacy posture of the system and organization to support risk management decisions. Monitor and assess portions of security controls in the system on an ongoing basis, demonstrating and reporting on effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security posture of the system to appropriate organizational officials. This step should adhere to a Continuous Monitoring Plan (CMP) that identifies which security controls should be assessed/tested daily, monthly, quarterly, or annually. Implementing this step gives the program situational awareness on the current security posture and encourages continuous improvement of the system to reduce vulnerabilities. Additionally, the results of this step can update the POA&M and inform the PM on budget needs.

	References and guidelines include: • NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP 800-137A, Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment
Watch Items	Ensure the following: • The package is submitted in the correct workflow • The spreadsheet is uploaded within the workflow • All Red Controls and Yellow controls have been reviewed • An additional 70 White Controls will need to be selected to meet the 50% threshold

Note: Additional information and resources can be found on the RMF Knowledge Service website: <https://rmfks.osd.mil>

3.3 RMF Training

In addition to the standards and publications listed in Table 2, many RMF training resources are available to assist program and system stakeholders to understand the RMF process. A list (not comprehensive) of available RMF training resources can be found in Appendix VW. Several industry / professional certifications are also available that focus on the understanding of the RMF workflow, including but not limited to the Certification in Governance, Risk, and Compliance (CGRC) offered by the International Information System Security Certification Consortium (ISC2). Additional certifications for the roles in Table 2 can be found in DoD 8140.03, *Cyberspace Workforce Qualification and Management Program* produced by the DoD CIO.

3.4 System Authorization Timeline

Figure 2 represents the System Authorization Timeline that shows the steps throughout the RMF process. The steps include Scoping & Onboarding (Step 0); Planning & Preparation for Security Controls Assessment (Steps 1–3); Planning & Preparation for On-Boarding Site Assessment (Steps 3–4), On-Site Assessment, Security Controls Assessment, and eMASS Control Validation (Step 4); Authorization Decision Need Date (Step 5); Security Impact Assessment (SIA) (if needed), and Annual Control Validation (ACV) (Step 6). All Stakeholders in the authorization process should consider schedule flexibility due to unforeseen constraints and/or efficiencies.

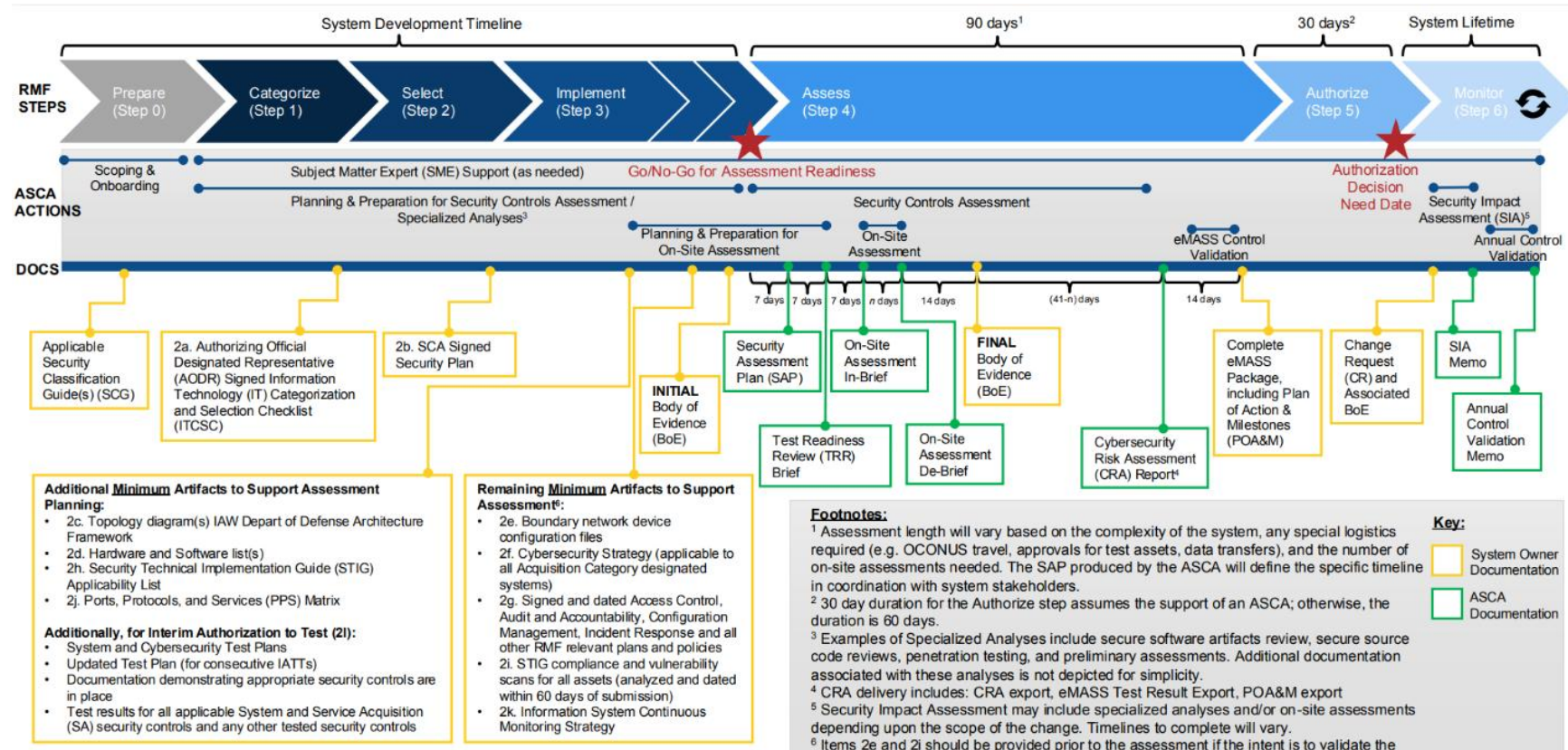


Figure 2. System Authorization Timeline

4 SSC S6 ATO PROCESS

Figure 3 aligns with Appendix A Process Step Tables shown below.

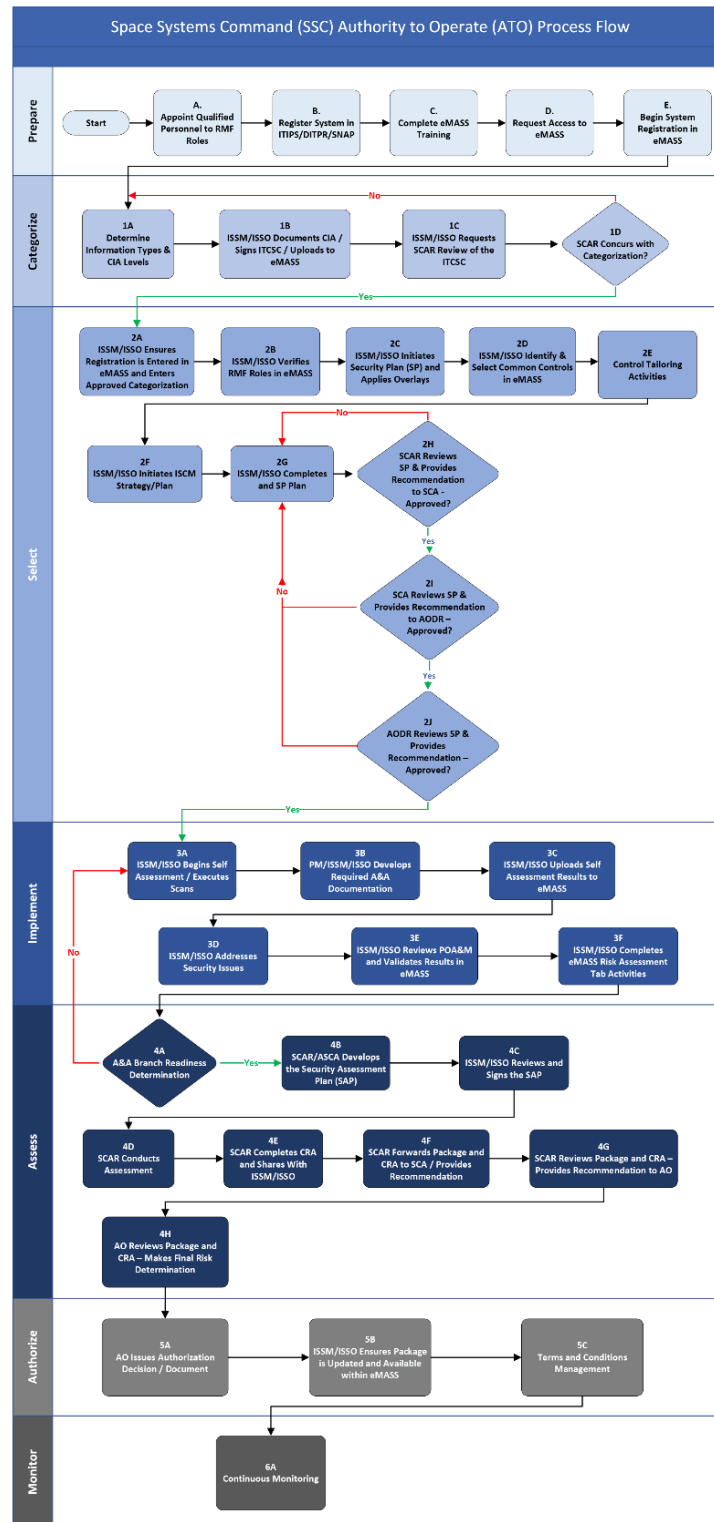


Figure 3. System Authorization Timeline

Appendix A: Process Step Tables

At this initial stage, systems should have already fulfilled system acquisition requirements. Additionally, they must have completed the Concept of Operations (CONOPS) and provided a detailed system description. If applicable, a Security Classification Guide (SCG) should also be included. Once these prerequisites are met, the system can proceed with the RMF Prepare activities.

Prepare Step A – Appoint Qualified Personnel to RMF Roles	
Roles	• AO / SCA / SCAR • ISSM / ISSO / ISSE • ISO / PM • SSC S6
Entrance Criteria	Prior to initiating the Assessment and Authorization process, Program's / IT Systems should have already addressed the following, and not limited to: • Full system description (This description should tell the story of who, what, when, where, why, and how the system supports the warfighter and/or other systems) • Identifying business functions and mission/business processes that the system is intended to support • All system acquisition requirements • CONOPS • System SCG (if applicable) • Identifying and understanding all stages of the information life cycle for each information type processed, stored, or transmitted by the system • Determined placement of system within the enterprise architecture • Determined an authorization boundary (comprehensive boundary drawing) reference the SSC S6 AO Topology Guidance (see Appendix I) • Identified privacy requirements and responsible point of contacts (POC)
Description	The Program Office / System Owner / RMF Team is responsible for implementing the RMF for a specific IS or Platform IT (PIT), System, and Assess Only products. Personnel filling the RMF roles must be assigned and qualified for those positions and are listed in the System Security Plan (SSP). The assigned personnel should receive an appointment letter outlining their duties and responsibilities. The RMF Roles include: • ISO • PM • ISSM / ISSO / ISSE
Templates	• ISSM/ISSO appointment letters (Appendix E) • PM appointment letter
Notes	The SSC S6 templates are not required for use. Program offices may use their own artifacts but must contain the required information. See NIST SP 800-53r4, RMF security related controls: AC-5, AT-3, PE-2, PS-2, PS-6, SA-5.
References	• CNSSI 4009, Committee on National Security Systems (CNSS) Glossary, March 2022 • DoDI 8500.01, Cybersecurity • DoDI 8510.01, Risk Management Framework for DoD Systems • NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

	• NIST SP 800-37r2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy • NIST SP 800-39, Managing Information Security Risk • AF RMF Knowledge Service
Exit Criteria	Finalized (signed) RMF role appointment letters have been accomplished and are available to support the A&A effort.

Prepare Step B – Register System in ITIPS / DITPR / SNAP	
Roles	• ISO • ISSM / ISSO • PM
Entrance Criteria	Exit criteria from Step A is complete.
Description	All IT investments will be approved through the AF corporate structure process. Once approved, the investment will be registered by the PM in the Information Technology Investment Portfolio Suite (ITIPS) per AFI 17-101 and AFI-17-110. The system will then be registered in the USSF Enterprise Portfolio Management Repository; Department of Defense Information Technology Portfolio Repository (DITPR), Systems/Network Approval Process (SNAP).
Templates	• IT Investment Portfolio Suite (dps.mil) (Common Access Card (CAC) required) • https://ditpr.dod.mil (CAC required) • https://snap.dod.mil (CAC required)
Notes	The ISO and PM is responsible for ensuring their systems are registered in ITIPS / DITPR / SNAP and works with the acquisition organization to identify the required portfolio and capital planning and investment information.
References	• AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) • AFI 17-110, Information Technology Portfolio Management Capital Planning Investment Control • CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities • DoDI 8530.1, Department of Defense Instruction Computer Network Defense (CND)
Exit Criteria	ITIPS / DITPR / SNAP system registration.

Prepare Step C – Complete eMASS Training	
Roles	• ISSE • ISSM • ISSO
Entrance Criteria	Completion of Prepare Step B.
Description	A user must take eMASS training to request an account. Reference Appendix VW .
Templates	• N/A
Notes	A course that serves as an introduction to eMASS with an overview of registering a system, managing a system, importing assets, initiating a package, and generating system and enterprise level reports.
References	• https://rmfks.osd.mil/rmfresources/eMASS/CBT/index.html • www.disa.mil (requires CAC)
Exit Criteria	Completion of eMASS training and eMASS training certificate acquired.

Prepare Step D – Request Access to eMASS	
Roles	• ISSE • ISSM • ISSO • PM
Entrance Criteria	Completion of Prepare Step C.
Description	When training is complete, request an eMASS account utilizing a DD Form 2875 (System Access Request). Reference Appendix VV . Submit eMASS account request (DD Form 2875) to: ssc.cio.cyber@spaceforce.mil
Templates	• DD Form 2875 for eMASS
Notes	Detailed eMASS information, including frequently asked questions, can be found here: https://rmfks.osd.mil/rmf/HelpandResources .
References	• AF RMF KS • DoDI 8510.01, Risk Management Framework for DoD Systems • NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
Exit Criteria	eMASS account request sent to SSC S6: ssc.cio.cyber@spaceforce.mil Activated eMASS account.

Prepare Step E – Begin System Registration in eMASS	
Roles	• ISO • ISSM • ISSO • PM
Entrance Criteria	Exit criteria in Step D are complete.
Description	Programs and/or systems seeking an ATO must register in eMASS. Program cybersecurity teams must enter new DoD systems into eMASS at the beginning of the system development life cycle; failure will result in increased cost and time delays later in the RMF process. Perform eMASS new system registration per the eMASS Process Guide for the Risk Management Framework Practitioners.
Templates	• N/A
Notes	eMASS offers two ways to register a new system record within the application: Primary: New system registration page; a user creates a new record directly within the application. Secondary: System details template import; a user completes information in an Excel-based template and imports into the application to create the system record.
References	• DoDI 8500.01, <i>Cybersecurity</i> • eMASS Functionality Guide (available on eMASS) • eMASS Process Guide
Exit Criteria	Completed System Registration in eMASS.

Categorize Step 1A – Determine Information Types & CIA Levels	
Roles	• AO • AODR • ASCA • ISO • ISSE • ISSM • ISSO • PM

CUI

	• SCA / SCAR
Entrance Criteria	Prepare Steps A-E completed.
Description	ISO/IO/ISSM determines information type(s): • Categorization is based on the type of information the system stores, processes, or transmits. The result is an IL for the CIA of the system and information. Accomplishing this step will give the CIA rating needed for the ITCSC. Assigning a system the appropriate CIA value – categorizing a system – is at the heart of properly applying RMF • ISO/IO/ISSM assigns CIA ILs (LOW, MODERATE, HIGH) • If the system is Unclassified (U), the Controlled Unclassified Information (CUI) Information Type must be at least a M-M-x per the DoD CIO Memorandum, <i>Requirements for Applying Baseline Controls for CUI Systems, 04 October 2021</i> • The ISO/ISSM/ISSO then determines if any modifications to the recommended CIA values are needed • Initiate the ITCSC Note: If the impact levels are reduced from the NIST SP 800-60 Vol 1 and Vol 2, you must provide Amplification Data in the Amplifying Data column of the ITCSC to justify why the impact level was reduced.
Templates	• Department of the Air Force (DAF) ITCSC Template. See Appendix G.
Notes	Per AFI 17-101, the ISO is responsible for identifying the information types stored in, processed by, or generated by the IS Information Assurance impact is categorized into low, moderate, or high designations to address the impact of a potential data loss. For guidance on how to assess the impact of CIA, see FIPS 199 and AFI 17-101. During the ITCSC review, the SCA/SCAR may request clarification and/or more information. Stakeholder collaboration is expected during this step.
References	• AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) • CNSSI 1253, Security Categorization and Control Selection for National Security Systems • DoD CIO CUI Baseline Requirements Memo.pdf • DoD Cloud Computing Security Requirements Guide, Version 1, Release 4 • DoDI 8500.01, Cybersecurity • DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) • eMASS Process Guide • FIPS 199, Standards for Security Categorization of Federal Information and Information Systems • https://rmfks.osd.mil • NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems • NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments • NIST SP 800-39, Managing Information Security Risk, Organization, Mission, and Information System View • NIST SP 800-59, Guide for Identifying an Information System • NIST SP 800-60 Vol. 1, Guide for Mapping Types of Information, and Information Systems to Security Categories • NIST SP 800-60 Vol. 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
Exit Criteria	Information types are identified. CIA levels are determined. ITCSC initiated.

Categorize Step 1B – ISSM/ISSO Documents CIA Results and Digitally Signs the ITCSC / Upload to eMASS	
Roles	• ISSM • ISSO
Entrance Criteria	Exit criteria in Step 1A is complete.
Description	ISSM/Program Manager documents CIA results and digitally signs the ITCSC (Categorization Memo). ISSM/ISSO uploads the digitally signed ITCSC to eMASS.
Templates	• DAF ITCSC Template (see Appendix G)
Notes	N/A
References	• NIST SP 800-60 Vol. 1, Guide for Mapping Types of Information, and Information Systems to Security Categories • NIST SP 800-60 Vol. 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
Exit Criteria	ITCSC completed and uploaded to eMASS. The ISSM/ISSO notifies SSC S6 A&A Branch that the ITCSC has been uploaded to eMASS: ssc.cio.cyber@spaceforce.mil

Categorize Step 1C – ISSM/ISSO Requests SCAR Review of the Completed ITCSC	
Roles	• ISSM • ISSO • SCA • SCAR
Entrance Criteria	Exit criteria from Step 1B is complete.
Description	ISSM/ISSO will request SCA/SCAR review of completed categorization documents via SSC S6 A&A Branch e-mail: • ssc.cio.cyber@spaceforce.mil
Templates	• N/A
Notes	This review will include a detailed review of any categorization supporting documents. The System Categorization levels are identified in the Security Plan (SP) and therefore will be approved with the SP via the eMASS Package Approval Chain (PAC).
References	• N/A
Exit Criteria	Request for SCAR review of the system ITCSC sent to: ssc.cio.cyber@spaceforce.mil

Categorize Step 1D – SCAR Concurs with Categorization	
Roles	• SCA • SCAR
Entrance Criteria	Exit criteria from Step 1C is complete.
Description	After reviewing the submitted ITCSC, the SCA/SCAR will either approve or disapprove the systems categorization. If approved, the SCA/SCAR will update eMASS accordingly.
Templates	• N/A
Notes	The SCA/SCAR may reach out to the Program / ISSM for more information. There may be some back and forth at this step to ensure system information types and CIA IL are accurately identified prior to proceeding through the A&A effort. Stakeholder collaboration is expected during this step.
References	• N/A
Exit Criteria	System categorization concurrence by the SCA/SCAR.

Select Step 2A – ISSM/ISSO Ensures Registration is in eMASS and Enters ISSM Approved Categorization	
Roles	• ISSM • ISSO
Entrance Criteria	Exit criteria from Step 1D is complete.
Description	For detailed instructions on how to register a new system in eMASS please reference the eMASS Functionality Guide. The ISSM enters the approved System Categorization in eMASS and your primary security control set (NIST SP 800-53 Revision 5), which establishes a baseline control set and begins the creation of the SP.
Templates	• N/A
Notes	N/A
References	• eMASS Functionality Guide
Exit Criteria	Verified completed system registration in eMASS. Categorization entered the eMASS system record.

Select Step 2B – ISSM/ISSO Verifies RMF Roles are Assigned in eMASS	
Roles	• ISSM • ISSO • PM
Entrance Criteria	Exit criteria from Step 2A is complete.
Description	The ISSM/ISSO and other senior officials as needed, ensures and verifies the correct personnel are assigned to the PAC and Control Approval Chain (CAC) roles in eMASS.
Templates	• N/A
Notes	Roles in eMASS are NOT broken out by ISSM, ISSO, etc. but rather grouped into the Program Office Role. The ISSM/ISSO should be listed in both the PAC and the CAC. However, all Program Office Supporting Team members should ONLY be listed in the CAC and <u>NOT</u> the PAC.
References	• N/A
Exit Criteria	Verified RMF Role assignments are entered into eMASS.

Select Step 2C – ISSM/ISSO Initiates eMASS Security Plan and Applies Control Overlays	
Roles	• ISSM • ISSO
Entrance Criteria	Exit criteria from Step 2B is complete.
Description	After the ISSM-Approved Categorization is input by the ISSM during eMASS System Registration and your primary security control set (NIST SP 800-53 Revision 5) is selected, a baseline control set is established. This initiates the development of the SP in eMASS. The SP represented by an eMASS record and contains the baseline control set provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Templates	• N/A
Notes	The ISSM could apply overlays, within eMASS, to a system's baseline control set to address unique security requirements associated with specific needs and scenarios (See the RMF KS's Overlay Application and Selection resource). If the information system contains Protected Health Information (PHI) / Personally Identifiable Information (PII), the Privacy Overlay must be applied. All CNSSI 1253 security controls apply to DoD systems. Reference the 3-by-3 matrix in the CNSSI 1253 that shows the security controls that are applicable to a NSS. Therefore, NSS-specific controls are automatically included in the System's [as it

	appears in eMASS] initial security control baseline. If approved by the AO, non-applicable NSS controls can be tailored by the Program Offices. Removal of specific NSS controls from the baseline must include justification as supporting documentation.
References	• CNSSI 1253, Security Categorization and Control Selection for National Security Systems • https://rmfks.osd.mil/rmf/RMFImplementation/Select/Pages/OverlaySelection.aspx
Exit Criteria	Completed the system SP in eMASS. Applicable security control overlays applied to baseline.

Select Step 2D – ISSM/ISSO Identify & Select Common Controls in eMASS	
Roles	• ISSM • ISSO
Entrance Criteria	Exit criteria from Step 2C complete.
Description	The ISSM selects security controls in eMASS that are available for inheritance (e.g. common security controls) from IS and updates common controls in the eMASS Implementation Tab. Evidence must be included or referenced in the eMASS SP to show how the IS receives protection from the inherited security controls. The ISSM establishes inheritance in eMASS by selecting common controls and marking them “Inherited.” In the case that only a portion of a control is deemed to be common, that control becomes a hybrid control.
Templates	• N/A
Notes	The RMF KS provides guidance for the identification of Common Control Provider’s (CCP) and the application of common controls here: https://rmfks.osd.mil/rmf/ControlsandAuthorization/securitycontrols/Pages/Common
References	• DoDI 8510.01, July 19, 2022, Risk Management Framework for DoD Systems • CNSSI 1253, Security Categorization and Control Selection for National Security Systems • eMASS Functionality Guide • NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments • NIST SP 800-53r4/5, Security and Privacy Controls for Federal Information Systems and Organizations • RMF KS, https://rmfks.osd.mil • Security Plan Implementation Plan Guidance
Exit Criteria	CCP’s identified (if applicable). Common Controls added to control baseline (if applicable).

Select Step 2E – Control Tailoring Activities	
Roles	• ISSM • ISSO
Entrance Criteria	Exit criteria from Step 2D complete.
Description	Once baseline security controls have been selected (with overlays applied and common controls identified), the ISSM initiates the tailoring process in eMASS to modify the initial control set to more closely account for conditions affecting the specific system (i.e. conditions related to organizational missions/business functions, information systems, or environments of operation). Concurrently, the ISSM adds relevant supplemental security controls and marks extraneous or impertinent controls as “Not Applicable.” Include Not Applicable (N/A) justification when marking a control as N/A within eMASS.
Templates	• N/A
Notes	Re-evaluate each control marked Not Applicable (NA) to ensure that each contain legitimate justification that explains, in detail, how each control cannot be

	technically performed, implemented, exploited, and/or applied to the system. NA Controls are defined as security controls that are not <u>technically</u> or <u>procedurally</u> relevant to the system. DODI 8510.01.
References	- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) - NIST SP 800-53 Rev. 4/5, Assessing Security and Privacy Controls in Federal Information Systems and Organizations
Exit Criteria	Completed security control baseline tailoring.

Select Step 2F – ISSM/ISSO Initiates ISCM Strategy/Plan	
Roles	- ISSM - ISSO
Entrance Criteria	Exit criteria from Step 2E complete.
Description	The ISSM initiates a system level strategy for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system. It should include plans for monitoring proposed or actual changes to the system within its environment of operation. The system level ISCM Plan must include the plan for annual assessments of all implemented security controls.
Templates	N/A
Notes	The ISCM Plan must conform to all applicable published DoD enterprise-level or DoD system level continuous monitoring strategies (e.g., DoD's ISCM Strategy) to ensure the complete set of planned, required, and deployed security controls within an information system (or inherited by the system) continue to be effective over time in light of the inevitable changes that occur. A finalized ISCM Plan/Strategy will be required to be submitted along with all other supporting artifacts as identified in Step 3B.
References	- ISCM strategy (In accordance with the SSC S6 A&A Branch ISCM and Annual Control Validation Policy for SSC mission and business systems) - NIST SP 800-137, Final, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations - NIST SP 800-137A, Developing an ISCM Assessment
Exit Criteria	ISCM plan/strategy drafted.

Select Step 2G – ISSM/ISSO Completes and Submits eMASS Security Plan	
Roles	- ISSM - ISSO
Entrance Criteria	Exit criteria from Step 2F is complete.
Description	The ISSM submits the eMASS SP through the eMASS PAC.
Templates	RMF Templates are not required for use. Program Offices may use their own artifacts but must contain the required information (if applicable)
Notes	If at any time the eMASS Security Plan (SP) is rejected in the PAC, the SP will be returned to the ISSM / Program.
References	- eMASS Process Guide - NIST SP 800-12, An Introduction to Information Security - NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems - NIST SP 800-100, Information Security Handbook: A Guide for Managers
Exit Criteria	eMASS Security Plan completed and submitted to the systems eMASS record.

Select Step 2H – SCAR Reviews SP and Recommends Approval or Disapproval	
Roles	• SCAR
Entrance Criteria	Exit criteria from Step 2G is complete.
Description	The SCAR will review all the fields for completeness within the SP Emphasis of the SCAR review: • All fields must have responses ◦ Fields that are not applicable should reflect “N/A”. The exception is the Authorization Termination Date field • A to be determined (“TBD”) response is not acceptable • Verify access rights and privileges are entered within the System User Categories field • Verify that the Internet Protocols, data services, and associated ports (internal/external) of the system comply with the Ports Protocols and Services (PPS) requirements. • Review referenced documents (i.e., System Authorization Boundary, Hardware (HW) / Software (SW), Firmware, System Enterprise and Information Security Architecture, Information Flows/Paths, Network Connection Rules). Ensure the field identifies the document file and that it is hyperlinked in eMASS. ◦ Verify that End-of-Life (EoL) SW is not being used (e.g., Windows 7 Operating System (OS), this could result as a High Risk). If the Program has an Extended SW Agreement, this should be uploaded as an artifact in eMASS. See RMF security related controls SA-22, SA-22(1). Reference https://endoflife.date for End-of-Life software versions and types all in one place • Verify all interconnections identified (eMASS # / DITPR#) within the Interconnected Information Systems and Identifiers field are included in the security design document. Reference Appendix O, Interconnected Systems • Confirm the encryption techniques in the Encryption Techniques field is documented in the security design document (if applicable) • Ensure that “Type Authorization” lists all locations within the System Location field (if applicable) • Ensure that the Cryptographic Key Management Information field is completed • Ensure that the Privacy Impact Assessment Required, Privacy Act Systems of Records Notice (SORN) Required, and E-Authentication Risk Assessment Required fields are completed with either a “Yes” or “No” • Link the “PIA” (if applicable) • Ensure that all external security services (if applicable) are listed within the External Security Services field and the following fields are complete: Security Requirements Description, Service Description, and the Risk Determination • Ensure ISSO/ISSM has listed all executed/signed Service Level Agreement (SLAs)/Memorandum of Agreements (MOAs)/Memorandum of Understandings (MOUs) • Verify realistic future dates have been entered for all planned controls • Ensure that past dates are entered for all implemented controls • Verify Implemented and Planned controls do not have “N/A” entered in the Comments field • Confirm Not-Applicable controls do not have a date entered • All justifications entered in the N/A Justification field must be applicable to the

	specific control - For all N/A controls the Comments field has N/A justification - The SCAR will complete the SP review for completeness and send forward with recommendation to the SCA
Templates	N/A
Notes	If at any time the SP is rejected by the PAC, the SP will be returned to the ISSM. At the discretion of the PAC, the ASCA may be asked to provide a review of the SP. This will generate an Air Force Research Lab (AFRL) Integration Testing and Evaluation Center (ITEC) ITCSC Review/Validation report. A PIA (DD Form 2930) is required for all Information Systems (see the ITCSC under References (e).
References	- AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) - DoDI 8551.01, Ports, Protocols, and Services Management (PPSM) - eMASS Functionality Guide - eMASS Process Guide - DAF Information Technology Categorization and Selection Checklist (ITCSC) v8.3.pdf
Exit Criteria	Completed SP review and forwarded to the SCA for review.

Select Step 2I – SCA Reviews SP and Recommends Approval or Disapproval	
Roles	SCA
Entrance Criteria	Exit criteria from Step 2H is complete.
Description	The SCA reviews SP, Boundary documentation, Security Assessment Plan (SAP), and the SCAR's SP comments, and forwards a recommendation to the AODR for review/approval.
Templates	N/A
Notes	If at any time the SP is rejected by the PAC, the SP will be returned to the ISSM.
References	- eMASS Process Guide - eMASS Functionality Guide
Exit Criteria	SCA completed SP review and forwarded to AODR for review.

Select Step 2J – AODR Reviews SP and Recommends Approval or Disapproval	
Roles	AODR
Entrance Criteria	Exit criteria from Step 2I is complete.
Description	The AODR reviews the Security Plan to ensure that all required and necessary information is included. The AODR reviews the SCA SP comments and approves/disapproves the SP via the PAC.
Templates	N/A
Notes	If at any time the SP is rejected by the PAC, the SP will be returned to the ISSM.
References	- eMASS Functionality Guide - eMASS Process Guide
Exit Criteria	Approved system SP.

Implement Step 3A – ISSM/ISSO Begins Self-Assessment, Executes Scans	
Roles	- ISSM - ISSO
Entrance Criteria	Exit criteria from Step 2J is complete.
Description	ISSM (assisted by the ISSO) leads the execution of Self-Assessment on the IS/Application by executing scans and completing applicable checklists per the

	SAP, to identify system security vulnerabilities, and then document results. All scan results must be uploaded to the eMASS Asset Module. Once "Test Results" have been entered for all Assessment Procedures (AP)/Control Correlation Identifier (CCIs) for security controls, the ISSM submits the "Program Office" comments to advance the control within the CAC in eMASS.
Templates	SAP
Notes	The executed Checklists and Scans cannot be more than 60 days old when submitting to eMASS for review.
References	- NIST SP 800-53, Assessing Security and Privacy Controls in Federal Information Systems and Organizations - NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
Exit Criteria	AODR approved SP.

Implement Step 3B – PM/ISSM/ISSO Develops A&A Supporting Artifacts	
Roles	- ISSM - ISSO - PM
Entrance Criteria	Exit criteria from Step 3A is complete.
Description	Per FIPS 200, "Organizations must develop and promulgate formal, documented policies and procedures governing the minimum-security requirements set forth in this standard and must ensure their effective implementation". Policies and procedures governing the minimum-security requirements must ensure the effective implementation that: - Address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance - Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls These are best captured in a standardized format (such as the SSC S6 provided i-Assure templates) or Program provided Control Family policy and procedural Documentation in an SSC S6 approved format. See NIST SP 800-53 control family "dash-one" security control requirements. In other words, completed RMF Control Family Implementation documents.
Templates	SSC S6 provided i-Assure RMF Control Family Templates
Notes	The Development of all supporting A&A artifacts is the most time consuming of all Program A&A responsibilities. Development may occur in all steps prior to the Readiness Determination (Step 4A). Additionally, each document should provide a control responsibility matrix resource that identifies the page, section, and/or paragraph of the document that describes how the program/system satisfies the individual security control requirement. If the I-Assure Template is used for an artifact, note that the template may contain language such as "Automatically compliant with this CCI because they are covered at the DoD level." The Program must perform their due diligence in determining if this is, or is not, true.
References	- AFI 17-100, Air Force Technology (IT) Service Management - DoDI 8500.01, Cybersecurity - DoDI 8510.01, Risk Management Framework for DoD Systems - FIPS 199, Standards for Security Categorization of Federal Information and Information Systems - FIPS 200, Minimum Security Requirements for Federal Information and

	Information Systems • https://rmfks.osd.mil/rmf/Pages/default.aspx • NIST SP 800-53, Assessing Security and Privacy Controls in Information Systems and Organizations • SSC S6 ATO Prerequisites and Supporting Artifacts (Appendix I) • Security Technical Implementation Guides (STIGs) (DISA) - https://public.cyber.mil/stigs/
Exit Criteria	All required A&A supporting artifacts.

Implement Step 3C – ISSM/ISSO Uploads Self-Assessment Results to eMASS	
Roles	• ISSE • ISSM • ISSO
Entrance Criteria	Exit criteria from Step 3B is complete.
Description	The ISSM continues Self-Assessment(s) by responding to the AP/CCIs for security controls by entering “Test Results” in eMASS. There is no limit to the number of self-assessments that can be executed; the amount is at the ISSM’s discretion. At a minimum, one self-assessment must be executed. Other self-assessments may be required to confirm system updates. Self-Assessments are an important tool in identifying cybersecurity weaknesses, prioritizing mitigation, and remediation actions, and increasing the efficiency of the independent assessor teams (if applicable) deployed to sites to test and review systems later in the process.
Templates	• N/A
Notes	eMASS has a Compelling Evidence section that outlines evidence required. If the evidence calls for a sample Audit Log, then the Program should provide a sampling of an Audit Log. Failure to provide the indicated evidence will result in the control being assessed as non-compliant (NC). If there is a control that is compliant (C), state the artifact name along with the specific page and section number. If there is no evidence required to prove (C), then the reasoning and justification for the Compliant status should be technical and detailed. The AP/CCI has a “Recommended Implementation Guidance” which identifies required actions for Compliance.
References	• eMASS Process Guide • NIST SP 800-53, Assessing Security and Privacy Controls in Federal Information Systems and Organizations • NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems • NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
Exit Criteria	Self-assessment results loaded to the systems eMASS record.

Implement Step 3D – ISSM/ISSO Addresses All Known Security Issues	
Roles	• ISSE • ISSM • ISSO
Entrance Criteria	Exit criteria from Step 3C is complete.
Description	The ISSM/ISSO/ISSE leads remediation and mitigation activities to strengthen the system’s security posture and degree of control compliance prior to the deployment of the Assessment Team. Remediation and mitigation activities should result in the elimination or reduction of the severity of highly compromising vulnerabilities and decrease the total number of non-compliant controls remaining

	on the system. During the Self-Assessment and remediation/mitigation activities, the ISSM/ISSO/ISSE adds, closes, and updates identified vulnerabilities to the POA&M. Mitigation Strategies are developed, milestones identified, and scheduled completion dates entered. The ISSO reviews the updated POA&M and forwards to the ISSM for additional review. All False Positives must be documented in the POA&M in accordance with the eMASS Functionality Guide.
Templates	N/A
Notes	A POA&M item must be completed for all NC controls.
References	- eMASS Functionality Guide - NIST SP 800-30, Guide to Conducting Risk Assessments - POA&M Management Guide
Exit Criteria	Any issues found during the self-assessment have been addressed.

Implement Step 3E – ISSM/ISSO Reviews POA&M and Validates Results Within eMASS	
Roles	- ISSM - ISSO
Entrance Criteria	Exit criteria for Step 3D is complete.
Description	The ISSM reviews the POA&M and validates mitigation strategies, milestones, and scheduled completion dates. The ISSM must concur with the POA&M prior to forwarding to the SSC S6 A&A Branch for review.
Templates	N/A
Notes	Ensure that you are in the correct CAC Step. When updating the Implementation Plan, the program must change the ECD. If a control is Planned, the date must be in the future. If the control is Implemented, the date must be in the past.
References	eMASS Functionality Guide
Exit Criteria	Completed/updated POA&M review. Validated that the POA&M has been uploaded to eMASS.

Implement Step 3F – ISSM/ISSO Completes eMASS Risk Assessment Tab Activities	
Roles	- ISSM - ISSO
Entrance Criteria	Exit criteria in Step 3E is complete.
Description	ISSM/ISSO completes the self-assessment and updates eMASS Risk Assessment Tab accordingly. This will generate an automated eMASS notification that the system is ready to be reviewed.
Templates	N/A
Notes	ISSM/ISSO must notify SCAR that they are ready for a Readiness Determination – Step 4A.
References	eMASS Functionality Guide
Exit Criteria	SCAR has been notified that the system has completed the risk assessment tab activities and is ready for the system readiness determination.

Assess Step 4A – A&A Branch Readiness Determination	
Roles	- ASCA - ISSM - ISSO - PM - SCA - SCAR
Entrance Criteria	Exit criteria for Step 3F is complete.
Description	The SCAR will review the A&A associated documents, technical data pertaining

	to Self-Assessment, and any other information provided that is considered relevant to a system's security posture. Once all documentation has been reviewed, the SCAR will make an assessment readiness recommendation to the SCA. If the System is deemed not ready for an assessment, the SCAR will recommend that the Program Office continue to work on preparing the System for an assessment. Common reasons for delay in assessment include but not limited to: • Unacceptable high-risk vulnerabilities • Unmitigated vulnerabilities not reflected on system POA&M • Incomplete or inconsistent status of security controls documented in eMASS • Out of date scans (older than 60 days) • Incomplete A&A documentation as identified in the SSC S6 ATO (or other) Prerequisites and Supporting Artifacts Checklist
Templates	• Use of the I-Assure Templates (recommended) includes a built-in Security Controls Traceability Matrix (SCTM) section as an appendix in each control family document • If the security control description requests a process, the checkbox should be checked and a description of (example: who, what, when, where, why, and how the process is taking place)
Notes	Program Offices may use their own artifacts. But they must contain the required information. A mapping identifying the page, section, and paragraph must also be provided per document. This is commonly known as a SCTM.
References	• DoDI 8510.01, July 19, 2022, Risk Management Framework for DoD System • NIST SP 800-30, Guide for Conducting Risk Assessments • NIST SP 800-53Ar4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans • RMF KS, https://rmfks.osd.mil • SSC S6 ATO Prerequisites and Supporting Artifacts Checklist • STIGs/Security Requirement Guides (SRGs)
Exit Criteria	SSC S6 A&A Branch determination that the system is ready to be assessed.

Assess Step 4B – SCAR/ASCA Develops the Security Assessment Plan (SAP)	
Roles	• ASCA • SCAR
Entrance Criteria	Exit criteria for Step 4A is complete.
Description	The SAP provides a framework for validating a system security baseline in support of a Cyber Risk Assessment. Data from SAP activities will support a CRA that will determine the overall risk level, identify key risks, and provide risk reductions for the SSC SCA to consider improving or maintaining acceptable security for the Department of Defense Information Network (DoDIN). Objectives of the CRA include, but are not limited to: • Confirming the effectiveness of RMF controls • Validating the security baseline • Identifying and documenting computer, facility, environmental, policy, and procedural security implementation gaps or vulnerabilities that may be present The SAP lays out the plan of how the assessment will be completed, and on what timeline.
Templates	• Ensure that the most current SAP template is used
Notes	The SAP will identify: • System descriptions • Authorization status • Validation / testing methodologies

	○ Tools used ○ STIG applicability ○ Potential on-site interviews needed and physical location security verification to be done ● Post assessment activities ● Stakeholder and validator contact information The SAP may be developed at any time during the A&A effort. However, this is the formal inject point.
References	● IASE STIG Library, https://public.cyber.mil/stigs/
Exit Criteria	Completed and approved AFRL ITEC SAP.

Assess Step 4C – ISSM/ISSO Reviews and Signs the SAP	
Roles	● ISSM ● ISSO
Entrance Criteria	Exit criteria for Step 4B is complete.
Description	The ISSM/ISSO reviews and signs the SAP. The purpose of reviewing the SAP is to understand and accept the assessment plan. The ASCA will use the SAP as a guide to ensure the security controls are implemented correctly.
Templates	● SAP
Notes	A briefing of the SAP may occur before the SAP is finalized to aid in the Program's self-assessment. This will give the Program an opportunity to correct any weaknesses in the security or privacy controls.
References	● eMASS Process Guide ● NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations ● NIST SP 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations ● NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, September 2008
Exit Criteria	The ISSM/ISSO reviewed and signed the SAP.

Assess Step 4D – SCAR (or ASCA) Conducts Assessment	
Roles	● ASCA ● SCA ● SCAR
Entrance Criteria	Exit criteria in Step 4A is complete.
Description	The SCAR or ASCA conducts the assessment (in accordance with the SAP) to determine if controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system, data, and organization. Every device within the System's/Application's A&A Boundary will be assessed (per the SAP). Each test procedure (automated and manual) is executed, and the results documented in eMASS within the Controls Details Page. At the conclusion of the assessment, the ISSM is briefed on the findings. Corrective action(s) (fixes/remediation to the vulnerabilities) proposed by the ISSM must be accomplished within the time specified on the approved SCAR or ASCA timeline. Vulnerabilities that cannot be remediated within the specified timeframe will be added to the system POA&M.
Templates	● N/A
Notes	The SSC S6 SCA / SCAR may reach out to the ISSM/ISSO for clarifying system data. If the Program Office hires an ASCA, the ATO package review timelines are adjusted as defined in Figure 2.
References	● eMASS Process Guide

	• NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations • NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information System • NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, September 2008
Exit Criteria	SCAR or ASCA completed the assessment to ensure controls are implemented correctly.

Assess Step 4E – SCAR/ASCA Completes CRA and Shares With ISSM/ISSO	
Roles	• ASCA • SCAR
Entrance Criteria	Exit criteria in Step 4D is complete.
Description	If the CRA is completed by the ASCA, the CRA will be signed by the ASCA and will be sent to the Program stakeholders for awareness. The ASCA will provide a recommendation for the package to move forward and present to SCA for review. If the CRA is completed by the SCAR, the package will be sent to the SCA for review.
Templates	• Ensure that the most current CRA template is used
Notes	No further development (based on the results of the risk assessment) may occur until the authorization determination is made by the AO.
References	• N/A
Exit Criteria	Completed / Finalized Cyber Risk Assessment shared with the Program's stakeholders.

Assess Step 4F – SCAR or ASCA Forwards Package and CRA to SCA / Provides Recommendation	
Roles	• ASCA • SCA • SCAR
Entrance Criteria	Exit criteria in Step 4E is complete.
Description	The SCAR or ASCA forwards / advances the eMASS package and completed CRA to the SCA for their review.
Templates	• N/A
Notes	N/A
References	• N/A
Exit Criteria	SCA completed review of the security authorization package.

Assess Step 4G – SCA Reviews Package and CRA / Provides Recommendation to AO	
Roles	• AO • SCA
Entrance Criteria	Exit criteria in Step 4F is complete.
Description	The SCA determines the level of residual risk based on the CRA, ASCA and System Owner input, and previously addressed vulnerability mitigations. The SCA clearly communicates their recommendation to the AO. Only SAF/CN has the authority to grant an AO the approval to issue an ATO with a "Very High" or "High" risk.
Templates	• N/A

Notes	At any point during the assessment activities, the package may be returned to the system owner for re-work. Reasons may include (but not limited to): • Unacceptable high-risk vulnerabilities • Unmitigated vulnerabilities not reflected in system POA&M • Incomplete or inconsistent status of security controls documented in eMASS • Out of date scans (older than 60 days) • Incomplete A&A documentation as identified in the SSC S6 ATO (or other) Prerequisites and Supporting Artifacts Checklist
References	• NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations • NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems • NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, September 2008
Exit Criteria	Completed formal system authorization recommendation to the AO.

Assess Step 4H – AO Reviews Package / Final Risk Determination	
Roles	• AO
Entrance Criteria	Exit criteria in Step 4G is complete.
Description	The AO assesses the risk to organizational operations by considering the current security state of the system, as well as any recommendations provided in the CRA. The AO then weighs this against the operational need for the system. The AO makes a final determination of the risk to DoD operations and assets, individuals, other organizations, and the Nation from the operation and use of the system.
Templates	• N/A
Notes	At the AO's discretion, terms and conditions of the ATO may be applied to the system / program. A separate discussion between the AO, SCA, Program Manager, and ISSM/ISSO may be required for needed clarification. The AO may issue a Denial of Authorization to Operate (DATO) based on the risk determination. In which case, the eMASS package will be updated to reflect the DATO and returned to the Program for further action.
References	• DoDI 8500.01, Cybersecurity • DoDI 8510.01, Risk Management Framework (RMF) for DoD Systems • NIST SP 800-30, Guide to Conducting Risk Assessments • NIST SP 800-37, NIST Risk Management Framework
Exit Criteria	AO reviewed the systems authorization package.

Authorization Step 5A – AO Issues Authorization Decision / Document	
Roles	• AO
Entrance Criteria	Exit criteria in Step 4H is complete.
Description	AO issues a risk-based authorization decision and provides the program / system authorization documentation, which is uploaded to the system's eMASS record.
Templates	• N/A
Notes	The Authorization Decision Document (ADD) contains: • Authorization Decision: ○ ATO ○ ATO with Conditions ○ DATO • Terms and Conditions: ○ Provides a description of any specific limitations or restrictions placed on

	the operation of the information system or inherited controls that must be followed by the system owner or common control provider. • Authorization Termination Date (ATD): ◦ Established by the AO, the ATD indicates when the security authorization expires. The AO may choose to eliminate the ATD if the continuous monitoring program is sufficiently robust to provide the AO with the necessary information to conduct ongoing risk determination and risk acceptance activities. The risk determination and acceptance activities regard both the security state of the information system and the continued effectiveness of security controls implemented within or inherited by the system.
References	• NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations • NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems • NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, September 2008
Exit Criteria	The AO formally assumed responsibility for operating a system at an acceptable level of risk. ATD is identified. ADD uploaded to eMASS.

Authorization Step 5B – ISSM/ISSO Ensures Package is Updated and Available in eMASS	
Roles	• ISSM • ISSO
Entrance Criteria	Exit criteria in Step 5A is complete.
Description	Once the system has been authorized and approved for operation, the ADD is automatically placed in the eMASS Artifacts tab. Upon receipt of the ADD, the ISSM must review the terms/conditions of the authorization. Specific actions with completion date(s) must be added to the POA&M for tracking purposes. The ISSM ensures that authorization documents for both information systems and for common controls are made available to appropriate organizational officials (e.g., ISOs inheriting common controls, risk executive (function), CIOs, Senior Information Security Officer ((SISO), ISSO, ISSM). Authorization documents, especially information dealing with information system vulnerabilities, are: • Marked and appropriately protected in accordance with federal and organizational policies • Retained in accordance with the Program Office's record retention policy The Authorizing Official verifies, on an ongoing basis, that the terms and conditions established as part of the authorization are being followed.
Templates	• N/A
Notes	N/A
References	• NIST SP 800-30, Guide to Conducting Risk Assessments • NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations • NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems • NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, September 2008
Exit Criteria	Once the ADD is signed, the Authorization Package with supporting documentation is available to System Stakeholders in eMASS. ISSM acknowledges receipt and implements the terms and conditions of the decision. The ADD is marked and appropriately protected in accordance with federal, DoD, and Agency policy.

Authorization Step 5C – Terms and Conditions Management	
Roles	• ISSM • ISSO • PM
Entrance Criteria	Exit criteria in Step 5B is complete.
Description	If an ATO is granted, the program can commence system operation within the conditions attached to the ATO, if any. If a DATO determination is made, the program is not authorized to operate and must mitigate the findings that drove the DATO decision and resubmit ATO package for redetermination.
Templates	• N/A
Notes	N/A
References	• DoDI 8500.01, Cybersecurity • DoDI 8510.01, Risk Management Framework for DoD Systems
Exit Criteria	Terms and Conditions of the ATO met / applied to the system and / or operation environment. Program Stakeholders should document (and make available within eMASS) activities that address the terms and conditions of the ATO.

Step 6A –Continuous Monitoring	
Roles	• AO • AODR • ISSM • ISSO • PM • SCA • SCAR
Entrance Criteria	Exit criteria from Step 5C is complete.
Description	This step will adhere to a Continuous Monitoring Plan that identifies which security controls must be assessed/tested daily, monthly, quarterly, or annually. Implementing this step provides the program situational awareness on the system's current security posture and encourages continuous improvement to reduce vulnerabilities. Continuous monitoring activities are updated in the POA&M: • The ISSM/ISSO maintains security control status IAW SSC S6 system-level continuous monitoring strategy • The ISSM/ISSO assesses security controls (technical, managerial, operational, and inherited) and performs an SIA IAW the SSC S6 system-level continuous monitoring strategy • The ISSM/ISSO responds to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in the POA&M • The ISSM/ISSO maintains system and environment changes and complies with terms and conditions that accompany the ATO • The ISSM/ISSO must notify SSC S6 SCA/SCAR when significant changes in the Chief Security Officer (CSO) risk posture occurs • The ISSM/ISSO performs POA&M management by addressing, mitigating and eliminating discovered vulnerabilities • The ISSM/ISSO performs key security updates and documents updates accordingly
Templates	• SSC S6 ISCM and ACV Policy (See Appendix P)
Notes	• N/A

References	• DoDI 8500.01, Cybersecurity • DoDI 8510.01, Risk Management Framework for DoD Systems • NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP 800-137A, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • Space AO ISCM and Annual Control Validation (ACV) Policy 24JAN2023
Exit Criteria	Typical outputs for continuous monitoring include: 1) Continuous monitoring and risk evaluation 2) Required evidence of security posture maintenance 3) Updated / current POA&M and eMASS test results 4) SIA.

Appendix B: Frequency Asked Questions (FAQs)

Step 0 – Prepare

- **Q: What is the purpose of the Prepare step?**
 - **A:** To carry out essential risk management tasks at the organization, mission and business process, and system levels to help prepare the organization to manage its security and privacy risks using the Risk Management Framework. Ultimately, the intention of the Prepare step is to provide the information and resources necessary to successfully manage information security and privacy risk to the organization and its missions from the operation and use of systems.
- **Q: What am I trying to accomplish in Step 0?**
 - **A:** Facilitating communication between senior leaders and executives at the organization mission and business process levels and system owners, organization-wide identification of common controls and the development of organizationally tailored control baselines, reducing the workload on individual system owners and the cost of system development and asset protection, reducing the complexity of the information technology and operations technology infrastructure using enterprise architecture concepts and models to consolidate, optimize, and standardize organizational systems, applications, and services, and identifying, prioritizing, and focusing resources on the organization's high-value assets and high impact systems that require increased levels of protection and taking steps to commensurate with the risk to such assets.

Resources:

- [NIST RMF Prepare Step-FAQs.pdf](#)

Step 1 – Categorization

- **Q: What is the purpose of the System Categorization of the Prepare Step 1?**
 - **A:** To determine the potential impact (low, moderate, high) to organizational operations and assets, individuals, other organizations and the Nation with respect to loss of confidentiality, integrity, and availability of organizational systems and information processed, stored, and transmitted by those systems. It establishes a baseline of security controls that the information system needs to implement to protect the information on the system.

Resources:

- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations

- **Q: What is required for the Technical Description/Purpose?**
 - **A:** The Technical Description/Purpose should tell the story of **who**, **what**, **where**, **when**, **why**, and **how** the system supports the mission and/or other systems. This will give the ASCA team a better understanding of the system.

Step 2 – Select Controls

- **Q: What is the purpose of the Security Plan Step 2?**
 - **A:** The Security Plan provides an overview of the security requirements for the system and describes the security controls in place and planned for meeting those requirements.
- **Q: Where do I select controls? What is control selection?**
 - **A:** Air Force eMASS. This is when you enter the system into eMASS and choose the relevant STIG/SRGs.

Resources:

- NIST SP 800-18 Rev 1, Guide for Developing Security Plans for Federal Information Systems

Step 3 – Implementation

- **Q: What is the purpose for Implementation Plan Step 3?**
 - **A:** The Implementation Plan is implemented by the Program. Security controls are implemented, and scans will be conducted that will identify weaknesses and deficiencies. A POA&M will be developed IAW RMF KS to the required AP/CCI. The AP/CCIs will define how to implement the control.

Resources:

- Security Technical Implementation Guides (STIGs) (DISA)
- Department of Defense (DoD) Risk Management Framework (RMF) Knowledge Service
- Security Requirements Guides (SRGs) (DISA)

Step 4 – Assess

- **Q: What happens during the Assess process Step 4?**
 - **A:** A site visit is conducted by the ASCA team to validate the baseline and the system architecture to include the network infrastructure, HW/SW baseline, and STIGs/Scans. The SAP will be created to establish the expectations for the security control assessment and the level of effort for the security control assessment.

Resources:

- NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organization

Step 5 – Authorize

- **Q: What is the purpose of Authorize Step 5?**
 - **A:** The purpose of the risk assessment is to determine the overall cybersecurity risk level of the system or the risk it poses to other connected systems.

Resources:

- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments

Step 6 – Monitor

- **Q: What is the purpose of Continuous Monitoring Step 6?**
 - **A:** Continuous Monitoring maintains the awareness of information system vulnerabilities and threats. Continuous monitoring is an important activity in assessing the security impacts on an IS resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation. Reference Appendix S.

Resources:

- NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations
- **Q: Do I need to redo all the RMF steps and take super long to renew an ATO?**
 - **A:** If you are doing your SIAs and maintaining your baseline, updates to ATO should be easier.

Resources:

- NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations

Appendix C: Checklist

The purpose of the checklist is to aid the Programs, ASCA teams and SCARs in ensuring all RMF steps and actions are complete before submitting their package to the Space SCA and AO. References, notes and templates have been added for further information.

STEP 0. PREPARE		
Program/ASCA/SCARs	Yes	No
1. Did the Program appoint qualified personnel to RMF roles? Reference NIST SP 800-37r2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy and DoDI 8510.01, Risk Management Framework for DoD Systems (Section 2.7, (l, m).		
2. Did the Program upload the signed PM and ISSM appointment letters in eMASS? See Appendix E for Appointment Letter Template.		
3. Did the Program register the system in ITIPS / DITPR / SNAP? IT Investment Portfolio Suite (dps.mil) (Common Access Card (CAC) required) https://ditpr.dod.mil (CAC required) https://snap.dod.mil (CAC required)		
4. Did the Program complete eMASS training? Computer Based Training (CBT) on eMASS functionality is available here: https://rmfks.osd.mil/rmfresources/eMASS/CBT/index.html		
5. Did the Program request access to eMASS? Submit eMASS account request (DD Form 2875) to: ssc.cio.cyber@spaceforce.mil		
6. Did the Program enter the new system in eMASS?		

Primary: New system registration page; a user creates a new record directly within the application. Secondary: System details template import; a user completes information in an Excel-based template and imports into the application to create the system record.		
7. Was a full system description (the description should tell the story of who, what, when, where, why, and how the system supports the warfighter and/or other systems) addressed? DoDI 8510.01, Risk Management Framework for DoD Systems (Table 2 and Section 4 (i)).		
8. Were business functions and mission/business processes that the system is intended to support identified? DoDI 8510.01, Risk Management Framework for DoD Systems (Table 1 and Table 2).		
9. Were all system acquisition requirements addressed? DoDI 8510.01, Risk Management Framework for DoD Systems (Section 4.4, b(d)).		
10. Is a System SCG (if applicable) addressed?		
11. Were privacy requirements and responsible point of contacts (POC) identified? DoDI 8510.01, Risk Management Framework for DoD Systems (Table 2).		

STEP 1. ITCSC		
Section 1. System Identification Information		
SCAR/Program	Yes	No
1. Did the Program upload their ITCSC in eMASS? Refer to Appendix G for the ITCSC template.		
2. Did the SCAR review of the completed ITCSC?		
3. Did the SCAR approve the System Categorization?		
4. Is the System Name and Acronyms used in the System Name spelled out? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 1. System Identification Information		
5. Is the Version number of the system added? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 1. System Identification Information		
6. Is the IT Investment Portfolio System (ITIPS) Identification (ID) added? If no ITIPS exists, enter 0000000. Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 1. System Identification Information		
7. Did the Program select the Authorizing Official (Check One) & Authorization Boundary? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 2. System Identification Information and https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx		
8. Was a RMF Action selected (Assess Only (Assess and Incorporate), Assess & Authorize, Assess Only (Assess and Approve for Use))? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 1. System Identification Information and DAF Assess Only Guidance Folder on the		

DAF RMF Knowledge Service at https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx		
9. Does the Technical Description/Purpose tell the story of who , what , where , when , why , and how the system supports the mission and/or other systems? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 3. System Identification Information		
10. Does the Program process PII/PHI? If so, was a signed Privacy Impact Assessment (PIA) DD Form 2930 provided? Reference: DODI 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, (Incorporating Change 1, August 11, 2017) and AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) for Department of the Air Force Information Technology (IT) (Section 4.3.1)		
Section 2. Authorizing Official (AO) & Authorization Boundary		
1. Is the Package in the correct workflow?		
2. Did the Program select an Authorizing Official in eMASS? Was the appropriate AO selected based on the system or mission owner's organization. A list of the AOs and Boundary descriptions is located at DAF RMF KS. https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx and Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 2. Authorizing Official (AO) & Authorization Boundary		
Section 3. Technical Description/Purpose		
1. Does the Technical Description explain the function and purpose of the system? Does the description tell the story of who , what , when , where , why , and how the system supports the mission and/or other systems? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 3. Technical Description/Purpose		
2. Did the Program describe the MAJOR hardware/software components of the system? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 3. Technical Description/Purpose		
3. Did the Program describe the services provided by the system and whether any of the services are publicly accessible (Publicly accessible means does not require authentication to access the information)? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 3. Technical Description/Purpose		
4. Did the Program describe how each of the Information Types are, or will be, stored, processed, and/or transmitted by the system? CNSSI 1253, Security Categorization and Control Selection for National Security Systems and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems		
Section 4. Security Description/Environment		
1. Does the Security Description/Environment tell the story of who , what , where , when , why , and how cybersecurity and information assurance hardware and software is, or will be, protecting the system? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 4. Security Description/Environment		

2. Did the Program describe the network security infrastructure to include the internal security components such as (encryption devices, firewalls, wireless, VPN, IDS, IPS, DMZ, HBSS, and antivirus?) Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 4. Security Description/Environment		
3. Did the Program upload a SLA, MOA/MOU as an artifact if services are being provided? Reference Appendix N for template. Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 4. Security Description/Environment		
4. Did the Program describe the system's interconnections (if any)? Reference Appendix O. Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 4. Security Description/Environment		
5. Did the Program describe the Defense in Depth and the processes that are in place to protect the system? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 4. Security Description/Environment		
Section 5. System Operational Status		
1. Did the Program provide an Operational Status (Operational, Under Development, Major Modification)? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 5. System Operational Status		
Section 6. System Architecture		
1. If a Cloud System, did the Program select the System Architecture (On-Prem Deployed, Hybrid Deployed, Cloud Deployed)? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 6. System Architecture		
Section 6a. **FOR CLOUD SYSTEMS ONLY**		
1. Did the Program select one Type of Service utilized (IaaS, PaaS, SaaS)? Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 6. Cloud		
2. Did the Program select the Information Impact Level (IL2 – (L-M-x and below), IL4 – (M-M-x and below), IL5 – (M-M-x and below), IL6 – (M-M-x and below)? Refer to Cloud Security Requirements Guide and Cloud Connection Process Guide for additional guidance. Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 6. Cloud ref (f) 7A – 7I)		
Section 7. Cloud Ref (f)		
1. Did the Program complete <u>all</u> of Section 7 (A-I)? DoD Cloud Computing Security Requirements Guide, Version 1, Release 4 and Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 6. Cloud ref (f) 7A – 7I)		
Section 8. Proposed System		
1. Did the Program select a System Type (Enclave, Major Application, PIT System)? Note: A IS/PIT Systems are Assess and Authorize. Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 8. Proposed System		
Section 9. Authorization Boundary Topology and System Location		

1. Did the Program provide a detailed boundary drawing? Required DoDAF artifact (DoDAF OV-1 and SV-1).		
Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 9. Authorization Boundary Topology and System Location and DAF Risk Management Framework (RMF) Knowledge Service at https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx		
2. Does the Authorization Boundary Topology clearly show the cybersecurity authorization boundary?		
This should match the infrastructure outlined in the System and Security Descriptions. External interfaces to the IT should be identified in this section. <u>An external interface is any interface that crosses the authorization boundary.</u> Indicate all information exchanges (such as removable media, media for system updates, Radio Frequency (RF), Ethernet, Wi-Fi, etc). If the system has no external interfaces, clearly state that in this section.		
Section 10. Overlays		
1. Did the Program identify Overlays (Intelligence, Cross Domain Solution, NC3, Space Platform, Classified Information, DoD Functional Mission/Capability Specific)?		
CNSSI 1253F, Security Categorization, and Control Selection for National Security Systems, 27 March 2014 – Appendixes 1 – 6. and Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 10 (A-F). Overlays		

Section 11. National Security System (NSS) Status Determination		
1. Did the Program answer <u>all</u> the questions in Section 11 (A-I)? If the answer was “yes” to any of the questions, then the System is an NSS.		
Refer to NIST SP 800-59, Guideline for Identifying an Information System as a National Security System and Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 11 (A-I). National Security System (NSS) Determination		
Section 12. Privacy		
1. Did the Program answer <u>all</u> the questions in Section 12 (A-I)?		
As per the DAF ITCSC, contact the base Privacy Manager for assistance. <i>Refer to</i> CNSSI 1253F, attachment 6 and Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 12 (A-I). Privacy		
Section 13. Classification		
1. Did the Program provide the Highest data classification level (Top Secret, Secret, Confidential, Controlled Unclassified Information, Unclassified)?		
Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 13 (A-B). Classification		
2. Did the Program answer <u>all</u> the questions in Section 13 (B-E)?		
Section 14. Categorization		
1. Did the Program identify <u>all</u> Information Types?		
NIST SP 800-60 Volume 1 and Volume 2 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories Committee on National Security Instruction (CNSSI) 1253, Security Categorization, and Control Selection for National Security Systems, 27 March 2014		

2. Did the Program fill in the Confidentiality, Integrity, Availability (C-I-A) (Low, Moderate, High) for each of the Information Types?		
If the system processes CUI, did add the CUI reference and make the C-I-A (M-M-x)? NIST SP 800-60 Volume 1 and Volume 2 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories		
3. Did the Program reduce from the defaulted System Categorization for an Information Type?		
If so, the Program must add additional justification for the change <u>must be added</u> in the Amplifying Data column? Reference NIST SP 800-60 Volume 1 and Volume 2 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories		
4. Was a request made for the SCAR to review the ITCSC?		
5. Did the SCAR concur with the ITCSC?		
6. Was the ITCSC uploaded to eMASS?		
Section 15. RMF Roles		
1. Was the ITCSC signed by <u>all</u> the Key Roles *AO, AODR, *PM, *ISO, *SCA, *ISSM, ISSE, User Representative and Requirements Lead?		
* Denotes Mandatory (Minimum Staffing Requirement). Reference DAF Information Technology Categorization and Selection Checklist (ITCSC) Instructions, 15. RMF Roles and Summary.		
STEP 2. SECURITY PLAN		
Program/SCAR	Yes	No
1. Is the Package in the correct Workflow in eMASS?		
2. Did the Program ensure the registration is in eMASS and approved categorization is uploaded?		
3. Does the Approved ITCSC match what is shown in the eMASS record (i.e., MMM)?		
4. Was a baseline control set established?		
NIST SP 800-18r1, Guide for Developing Security Plans for Federal Information Systems and DoDI 8510.01, Risk Management Framework for DoD Systems, Section 3.2, Table 3		
5. Did the Program ensure and verify the correct personnel are assigned to the Package Approval Chain (PAC) and Control Approval Chain (CAC) roles in eMASS?		
The ISSM/ISSO <u>should</u> be listed in both the PAC and the CAC. However, all Program Office Supporting Team members should ONLY be listed in the CAC and <u>NOT</u> the PAC.		
6. Did the Program initiate the Security Plan?		
NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems		
7. Did the Program provide the minimum supporting artifacts to support the system?		
8. Does the SP System information match the information shown in eMASS?		
(System name, System acronym, Version/Release Number, DoD Information Technology Portfolio Repository (DITPR) Number, Authorizing Official, SCAR, SME, Initial Date, PM, ISSM)		
9. Are the information types applied to the eMASS record?		
10. Did the Program identify & select the Common Controls in eMASS?		
11. Were security controls selected that are available for inheritance?		
12. Was the established inheritances marked "Inherited"?		
13. Were common controls added to the baseline?		
14. Were CCPs identified (if applicable)?		
15. Were overlays applied to the baseline?		
AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) (Section 4.4.4)		

16. Was a tailoring process initiated for the control set that accounts for conditions affecting the system?		
AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) (Section 4.4.5)		
17. Does the C-I-A levels and Overlays match the eMASS record?		
18. Did the Program assign the correct overlay controls?		
19. Does the Program have a Cross Domain Solution (CDS)?		
If so, the refer to CNSSI 1253F Attachment 3 and DoDI 8540.01 Enclosure 4 explains the relationship between RMF and CDS. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/854001p.pdf . There should be a Certificate from the Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG) approved. Reference https://public.cyber.mil/connect/dsawg/ .		
20. Did the Program provide a Cybersecurity Service Provider (CSSP)?		
If the Program does have a CSSP, they should state how they protect, monitor and respond to incidents. If the Program does not have a CSSP, this should be stated within the system description.		
21. Did the system identify as an NSS?		
NIST SP 800-59, Guideline for Identifying an Information System as a National Security System		
22. Did the Program complete the NSS Checklist in eMASS?		
23. Did the Program provide an adequate system description?		
24. Did the Program identify the number of accounts, types of access Role Base Access Control (RBAC), Discretionary Access Control (DAC), or Mandatory Access Control (MAC)), and permission types (Read, Write, or Full Control) as follows for each System User Category?		
(i.e., 27 System Administrators, RBAC, Full Control, 5000 Standard Users, RBAC, Read)		
25. Did the Program provide a topology with all required information and indicated by a thick red dashed line (- - - - -) that surrounds only the items being assessed?		
(i.e., network devices must be labeled with make, model, IP address and operating system version, external connections and transmission protocols). Items should not be placed within the red dashed line if they are NOT part of your Authorization Boundary.		
26. Did the Program upload a hardware list in the Assets Module in eMASS?		
Ensure there are no unsupported products, and that the hardware list is accurate and that all components reside within the system authorization boundary. Review the Microsoft EOL list located at https://support.microsoft.com/en-us/lifecycle/search/ or Adobe EOL list located at https://helpx.adobe.com/support/programs/eol-matrix.html . If the Program has an extended license, upload the documentation in eMASS.		
27. Did the Program upload a software list in the Assets Module in eMASS?		
Ensure there are no unsupported products, and that the hardware list is accurate. Reference Committee on National Security Systems Instruction (CNSSI) 4009 for the definition of Information Assurance (IA)-enabled.		
28. Did the Program upload a PPS Worksheet into the Asset Module in eMASS?		
29. Did the Program provide an ISCM strategy?		
AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT) (Section 4.4.6 – 4.4.8)		
30. Did the Program inherit from USSF RMF-C?		
31. Did the Program provide an SLA, MOA / MOU if inherited from an external source?		

DoDI 4000.19, Support Agreements and NIST SP 800-47 Rev. 1, Managing the Security of Information Exchanges		
32. Did the Program identify <u>all</u> external systems that they connect to?		
NIST SP 800-47 Rev. 1, Managing the Security of Information Exchanges		
33. Did the Program provide a STIG applicability list?		
(Reference: https://iase.disa.mil/stigs/agct/Pages/index.aspx). STIG applicability can be assigned in eMASS if the program is using the Asset Module eMASS tools). Vulnerability Scans (if applicable, within 60 days), STIG Compliance scans (if applicable, within 60 days). The program should upload this file to eMASS Asset Module.		
34. Did the Program explain in specific detail how NA controls cannot be technically performed, implemented, and/or applied to a system?		
Controls that are being met due to implementation of other technical or procedural controls are "Compliant" not NA. <u>Programs This must be explained and justified this in their mitigation.</u>		
35. Did the Program identify that <u>all</u> controls have been answered?		
36. Did the Program provide a Security Assessment Report (SAR)?		
37. Did the Program verify the System Name is accurate in eMASS?		
38. Did the Program verify the System Type is accurate in eMASS?		
39. Is the system Public Facing in eMASS?		
The System is Public Facing if the System has a Public-Facing component and/or presence, if the System is accessible from the internet, if the System is accessible outside of the .mil and .gov domains.		
40. Did the Program upload the STIGS/Scans in the Asset Module of eMASS and verify the date of the STIGS/Scans?		
Vulnerability and Compliance scans (if applicable, within 60 days). STIG artifacts should be in the (.ckl) file format and Scans should be from ACAS in the (.nessus) file format.		
41. Did the Program complete and submit the Security Plan in eMASS?		
42. Were all fields of the security plan completed before submitting to the SCA?		
43. Did the SCAR review and approve the Security Plan?		
44. Is the Security Plan approved by the AODR?		
STEP 3. IMPLEMENTATION		
Program	Yes	No
1. Is the package in the correct workflow <u>in eMASS</u> ?		
2. Was the most current SAP used?		
3. Was a self-assessment conducted using the scans and applicable checklists per the SAP?		
4. Were system security vulnerabilities identified and documented?		
5. Were scan results uploaded in the Asset Module in eMASS?		
6. Were checklists and scans older than 60 days when submitted in eMASS?		
7. Did the Program identify the STIGs that <u>must</u> be implemented based on technology within the Authorization Boundary?		
If a STIG is not available, the Security Requirements Guide (SRG) may be used for configuration settings.		
8. Did the Program update the ECD in the Implementation Plan?		
If a control is Planned, the date <u>must</u> be in the future. If the control is Implemented, the date <u>must</u> be in the past.		
9. Were Test Results entered in eMASS?		
10. Were mitigation strategies developed?		

11. Were milestones identified?		
12. Were POA&M items completed for all NC controls?		
13. Was the eMASS Risk Assessment tab completed?		
14. Was the SCAR notified that the risk assessment was completed?		
15. Are there high-risk vulnerabilities?		
16. Are there unmitigated vulnerabilities not reflected in the POA&M?		
17. Are there incomplete or inconsistent status of security controls documented in eMASS?		
18. Did the Program submit a list of applicable STIGs as an artifact?		
19. Were signed policies and procedures provided?		
20. Was the document, page, section, and/or paragraph provided for the Compelling Evidence?		
21. If I-Assure templates were used, was additional information provided if the description requested process, procedures, implementation, etc.? This should not be a copy and paste from the description.		
22. Is there incomplete A&A documentation as identified in the SSC S6 ATO (or other) Prerequisites and Supporting Artifacts Checklist?		
STEP 4. ASSESS		
ASCA/SCAR	Yes	No
1. Is the Package in the correct workflow <u>in eMASS</u> ?		
2. Did the ASCA team make all controls official?		
3. Did the ISSM/ISSO review and sign the SAP?		
4. Are the controls implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system?		
5. Are Test Results executed and results documented in eMASS?		
6. Was the ISSM briefed on the findings of the SAP		
7. Were corrective actions (fixes/remediations) proposed by the ISSM accomplished within the SCAR/ASCA timeline?		
8. Did the ASCA team provide the CRA with Risk Determination and recommended ATO duration?		
9. Did the ASCA team upload the POA&M?		
10. Did the <u>Program ASCA/SCAR ensure that a enter a Test Result is entered</u> that shows the Policy/Plan, Chapter, and Page Number for the compelling evidence? If this is <u>not</u> completed and we are unable to locate the compelling evidence, our office will likely make this control NC and a POA&M item will need to be created.		
11. Did the <u>Program ASCA/SCAR verify that the complete the Security Control Description and provide</u> artifact(s) <u>were provided</u> for the Recommended Compelling Evidence? <u>The Program must state the</u> exact location of the compelling evidence in the Test Results (Documentation, Page Number, Section, etc.).		
12. -Were the STIGs/Scans provided and reviewed?		
<u>13. Were there High or Very High STIG findings?</u> <u>13. Reference AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT)</u>		
14. -Did the Program provide a STIG Applicability list?		
15. <u>Did the Program</u> Were -upload all supporting artifacts <u>uploaded</u> in eMASS to show compelling evidence, including policies, plans, procedures, etc.? If you reference any of the documents (ex. PWS, NIST guidance, Office of Management and Budget (OMB), etc.) include these documents as an artifact. If there is no compelling evidence to support the CCI/control the control will be marked NC.		
16. Did the ASCA verify that there were no missing POA&M items?		
17. Was the CRA signed by the ASCA team?		
18. Was the CRA sent to the Program stakeholders?		
19. Did the SCA determine a level of risk?		

STEP 5. AUTHORIZE		
Program	Yes	No
1. Is the Package in the correct workflow in eMASS ?		
2. Did the Program provide Was a mitigation for all the NC controls? This will help our office when determining the Risk. Do not copy and paste the Test Result that was provided by our office. A mitigation statement that identifies risk reducing controls/ countermeasures/factors that directly reduce the likelihood and impact of this specific NC finding from being exploited. Physical security (gates, guards, and guns) shouldn't be your only mitigation throughout the POA&M.		
3. Verify that there are no NC and NA controls missing POA&M items? If there are missing POA&M items, the Program will need to create a POA&M for those items.		
4. Verify there are no POA&M item conflicts.		
5. Verify that there are no excluded Inherited Controls.		
6. If an ATO is granted, did the ASCA deliver the CRA to the Program?		
7. Did the ISSM review the Terms and Conditions of the authorization decision document ?		
7. NIST SP 800-37r2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy		
8. Is the signed ADD uploaded in eMASS?		
8-9. Were actions and scheduled completion dates added to the POA&M?		
9-10. -Were authorization documents made available to organizational officials?		
11. Were activities that address the Terms and Conditions documented in eMASS?		
10. NIST SP 800-37r2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy		

STEP 6. MONITOR		
Program	Yes	No
1. Did the Program conduct the Annual Control Validation? Refer to Appendix P for ACV memo template. ACV will be due 6 months from the date the ATO was approved. NIST SP 800-137A Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations		
2. Is the correct workflow selected for the Annual Security Review (ASR) in eMASS?		
3. Did the Program provide boundary network device configuration files?		
4. Did the Program provide updated and signed Access Control, Audit and Accountability, Configuration Management and Incident Response plans and policies?		
5. Did the Program provide their Information System Continuous Monitoring Strategy?		
6. Were all the Red Controls reviewed by the Program?		
7. Were all the Yellow Controls reviewed by the Program?		
8. Did the Program select the remaining White Controls to make the required 50%?		
9. Did the Program provide scans?		

Scans should be conducted every 30 days. Scans should be submitted 60-days prior to submittal of an ACV.		
10. Were continuous monitoring activities updated in the POA&M?		
11. Are the Test Results uploaded in the Workflow?		
Test results will need to be up to date.		
12. Is the security control status maintained IAW SSC S6 system-level continuous monitoring strategy?		
13. Are security controls (technical, managerial, operational, and inherited) assessed assessed, and an SIA performed IAW the SSC S6 system-level continuous monitoring strategy?		
14. Did the ISSM/ISSO respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in the POA&M?		
15. Did the ISSM/ISSO maintain system and environment changes that complies with terms and conditions that accompany the ATO?		
16. Did the ISSM/ISSO notify SSC S6 SCA/SCAR when significant changes in the Chief Security Officer (CSO) risk posture occurs?		
16. <u>Appendix Q, Security Impact Assessment (SIA) Memo and NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems</u>		
17. Did the ISSM/ISSO perform POA&M management by addressing, mitigating and eliminating discovered vulnerabilities?		
18. Did the ISSM/ISSO perform key security updates and documents updates?		
IATT		
ASCA/Program	Yes	No
1. Is the IATT in the correct workflow in eMASS?		
2. Did the Program upload a SCA Signed ITCSC Memo?		
3. Did the Program upload an AODR Signed eMASS Registration and Security Plan?		
4. Did the Program upload a Topology/Authorization Boundary?		
Refer to Appendix I for further information.		
5. Did the Program upload a Hardware list from the eMASS template into the Asset Module?		
6. Did the Program upload a Software list template from eMASS into the Asset Module?		
7. Did the Program upload a Security Technical Implementation Guide (STIG) Applicability List?		
8. Did the Program upload a Ports, Protocols, and Services Matrix (required) and Registration Number (if applicable) into the Asset Module? _____ _____		
<u>8.</u>		
9. Did the Program upload a System and Cybersecurity Test Plans and Schedule?		
The Program should define what , when and how the system will be tested to include cybersecurity testing.		
10. Did the Program upload Cybersecurity Test Results (e.g., vulnerability scans, STIG check results)?		
11. Did the Program upload and address all applicable security controls related to System and Service Acquisition (SA) in the system eMASS record?		
12. Did the Program answer all the controls?		
If this is a second IATT, all controls must be answered. If this is the 1 st IATT, only the SA controls will need to be answered unless otherwise requested by the ASCA team.		
13. Did the Program upload a Cybersecurity Strategy (applicable to ACAT designated system)?		
ATC		

Program	Yes	No
1. Is the package in the correct workflow in eMASS?		
2. Were all supporting artifacts uploaded in eMASS IAW the ATC guidance memo?		
3. The system acronym/name in eMASS for an ATC should be the name of the external system and the name of the SSC S6 AO system in parentheses. For example, when connecting an external CDC system to an SSC S6 AO system, the eMASS name should read CDC (system).		
4. Did the Program upload a Signed Authorization Decision Document (i.e. IATT, ATO)?		
5. Did the Program create/update the test results in eMASS?		
6. Did the Program upload a Risk Assessment Report with SCA final risk determination?		
7. Did the Program provide a System Description?		
8. Did the Program upload a Plan of Action and Milestones?		
9. Did the Program upload a Completed Ports Protocols and Services Matrix (including all interconnection details) in the Asset Module?		
10. Did the topology include all interconnection details? Refer to Appendix I for further information.		
11. Did the Program ensure that the hardware list matches the components that are on the topology? Refer to Appendix I for further information.		
12. Did the Program upload a Sponsor Memorandum, only for systems requesting connection from outside the Air Force Information Network (AFIN)?		
13. Did the Program provide an SIA? Refer to Appendix Q.		
eMASS		
Program	Yes	No
1. Did the Program submit the package to the correct Step? All packages must go through Steps 1-6. Reference the eMASS Functionality Guide (available on eMASS) and eMASS Process Guide.		
<u>2.</u> Are the correct personnel assigned to the PAC and CAC roles in eMASS?		
<u>2-3.</u> Did the Program ensure that there are no unassigned controls?		
<u>3-4.</u> Did the Program verify that there are no duplicate POA&M items? When importing the POA&M back into eMASS, matching should be selected.		
<u>5.</u> Did the Program use the Hardware/Software Template? <u>4.</u> Reference the eMASS Functionality Guide (available on eMASS) and eMASS Process Guide.		
<u>5-6.</u> Did the Program upload the Hardware (HW)/Software (SW) list in eMASS under the Asset Module?		
<u>6-7.</u> Did the Program ensure that the correct inheritance package was selected USSF RMF-C? Programs cannot inherit from expired or decommissioned systems.		
<u>7-8.</u> Did the Program verify that no errors were indicated in eMASS before submitting?		
<u>8-9.</u> Did the Program ensure that there were no missing NC or NA POA&M items?		
<u>9-10.</u> Did the Program ensure that the Ports, Protocols, and Services (PPS) was submitted in eMASS under the Asset Module?		
<u>10-11.</u> Did the Program ensure that the STIGs were uploaded in the Asset Module?		

<u>11.12.</u> Did the Program remove any Legacy documentation (anything more than 1 year old) and replace it with a new document?		
Policies should be updated annually.		
<u>12.13.</u> Did the Program complete all the required entries in eMASS to include (User Categories, etc.)?		
<u>13.14.</u> Did the Program ensure there were no Compliant controls that were ongoing in the POA&M?		
TOPOLOGY		
Program	Yes	No
1. Did the Program ensure that the Topology is readable?		
Refer to Appendix I for further information.		
2. Did the Program ensure that the Topology shows all the interconnection details (such as boundary devices, firewalls, routers, switches, demilitarized zones (DMZs), etc.)?		
Refer to Appendix I for further information. DAF Risk Management Framework (RMF) Knowledge Service at https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx		
3. Did the Program ensure that all the components on the Topology match the Hardware/Software List?		
If the Program is inheriting protection mechanisms, those devices should be displayed on your topology outside of the System Authorization Boundary regardless of where it sits physically.		
<u>4. Did the Program upload the Topology in eMASS?</u>		
ARTIFACTS		
Program	Yes	No
1. Did the Program provide signed and dated Policies/Plans?		
Ensure that the Policies and Plans provide the information the description is asking for. The description should not be copied and pasted directly into the policy and procedure. NIST SP 800-53r5 states that "Simply restating controls does not constitute an organizational policy or procedure". See NIST SP 800-53r5, AC-1, Access Control Policies and Procedures.		
2. Did the Program upload completed Policies/Plans? If the I-Assure template was added to the Policies/Plans are all checkboxes checked?		
If the security control description requests a process/implementation/procedure this should be provided within the Policy/Plan. The checkbox should be checked if there is a process and a description of (example, who, what, when, where, why, and how the process is taking place).		
3. Did the Program ensure that the uploaded Policies/Plans are current?		
Policies/Plans should be updated annually.		
4. Did the Program ensure that the referenced supporting artifacts are uploaded?		
Reference Appendix I.		
5. Did the Program ensure that the uploaded supporting artifacts are readable?		
6. Did the Program ensure that the uploaded supporting artifacts can be opened?		
<u>7. Did the Program upload the artifacts in eMASS?</u>		
POA&M		
Program	Yes	No

1. Did the Program ensure that there are no duplicate POA&M items?		
When importing the POA&M back into eMASS, matching should be selected.		
2. Did the Program ensure that the Scheduled Completion Date is not past due?		
3. Did the Program ensure that there are no missing POA&M items?		
4. Did the Program ensure there is a POA&M item for every NC control?		
5. Did the Program ensure that there is not a POA&M item for a status of Compliant or Completed?		
6. Did the Program provide mitigation statements for all POA&M entries?		
<u>E</u>The Program <u>should</u> explain ways <u>they</u>that <u>are</u> alternatively or partially <u>are</u> meeting controls or what measures <u>they</u>are <u>being</u> taken<u>ing</u> to protect against those vulnerabilities? By providing detailed mitigations, this will give the ASCA team a better understanding of the system's cybersecurity posture, which will help lower the Residual Risk of the system.		
7. Are STIG findings addressed in the POA&M?		
STIG/SCANS		
Program	Yes	No
1. Did the Program upload SCANS in eMASS Asset Module?		
The maximum file size when importing scans is 30 MB.		
2. Did the Program verify that there are no Very High or High Controls that can be mitigated? Explain ways that are alternatively or partially meeting controls or what measures are taken to protect against vulnerabilities.		
3. Did the Program provide a STIG applicability list?		
Reference https://iase.disa.mil/stigs/agct/Pages/index.aspx		
4. Did the Program provide scans that are no more than 60 days old?		
STIG and Scan Guidance is located at https://public.cyber.mil/stigs/		
QUARTERLY POA&MS		
Program	Yes	No
1. Did the Program submit their Quarterly POA&Ms in conjunction with the next ATO?		
The Program should submit 60 days prior to the next ATO. For further guidance, reference the following: OMB 02-01, Guidance for Preparing and Submitting Security Plans of Actions and Milestones DoDI 8510.01, Risk Management Framework for DoD Systems NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy		
ANNUAL CONTROL VALIDATION		
Program	Yes	No
1. Did the Program conduct an ACV?		
Reference Appendix P.		
2. Is the correct workflow selected for the Annual Security Review in eMASS?		
3. Were all the Yellow Controls reviewed by the Program?		
4. Were all the Red Controls reviewed by the Program?		
5. Did the Program select 50% of the White Controls?		
6. Did the Program provide updated documentation?		

Any other supporting documentation should be uploaded as an artifact.		
7. Did the Program provide scans? Scans should be conducted every 30 days. Scans should be submitted 60 days prior to submittal of an ACV.		
8. Is the Test Results uploaded in the Workflow? Test results will need to be up-to-date.		

Appendix D: Typical RMF Step Outputs for an ATO

RMF Step	Associated Outputs
----------	--------------------

Prepare:	• System acquisition requirements • Concept of Operations • Statement of risk tolerance • System description • System Security Classification Guide (if applicable) • RMF role appointment letters • DITPR / SNAP system registration • eMASS training completion certificates • Submit eMASS account request (DD Form 2875) to: ssc.cio.cyber@spaceforce.mil • Registered system in eMASS
Categorize:	• Information Types Identified • CIA Levels Determined • Kick-off Meeting or discussion with SSC S6 A&A Branch Completed • Categorization Concurrence from SCA • ISSM Signs ITCSC / Uploaded to eMASS
Select:	• Baseline of Security Controls • Initial SSP • Initial / Draft ISCM Plan / Strategy • System Architecture / Topology • Boundary Diagrams • Data Flow Diagrams • HW/SW Baseline • Previous Assessment Results • Test Results (Scans, Config Files, Etc.) • PPSM
Implement:	• Vulnerability Scans Completed • Scan Results Uploaded to eMASS • System POA&M Initiated • Other Evidentiary Documents Submitted (As Required) • AO Determination Brief
Assess:	• Authorization Path Finalized • Schedule Determined • Operational Use Perspective Brief • Penetration Test Results • CRA
Authorize	• Risk Recommendation Letter • ATO/ATD Dates Identified • AO Authorization memo / Decision Document • Signed Authorization Decision Document Uploaded to eMASS
Continuous Monitoring	• Continuous Monitoring and Risk Evaluation • Required Evidence of Security Posture Maintenance • 14-15. Decommission Memo (if applicable) • Updated POA&M and eMASS Test Results • SIA (template)

Appendix E: Appointment of Information System Security Manager (ISSM), Information System Officer (ISSO) Template

{Insert Date}

MEMORANDUM FOR RECORD

FROM: Program Manager

SUBJECT: Appointment of Information System Security Manager (ISSM), Information System Security Officer (ISSO)

1. In accordance with AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT), I hereby appoint the following individuals as the ISSMs, and ISSOs for the

Rank/Name	Role	IAM Level	Citizenship	DSN Phone	Email Address
	ISSM	II			
	Alt ISSM	II			
	Alt ISSM	II			
	ISSO	I			
	ISSO	I			
	ISSO	I			

2. Pursuant to this appointment, the ISSM must meet the following requirements:
 - a. In accordance with AFI 17-101, the appointed will obtain and maintain an IAM Level II certification in accordance with AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*. Proof of training (e.g., certificate) will be included as an artifact in the Assessment and Authorization package. Certifications are required within six months of appointment for civilian/military and upon hire for contractors.
 - b. In accordance with AFI 17-101, ISSMs and ISSOs will be a US citizen.
 - c. In accordance with AFI 17-130, *Cybersecurity Program Management*, act on behalf of the Authorizing Official (AO) to maintain authorization of the system throughout its lifecycle; therefore, if the ISSM is not qualified to serve, the AO or the Authorizing Official Designated Representative (AODR) may request the PM designate a suitable replacement.
3. Duties of the ISSM include, but are not limited to the following:
 - a. Implement and maintain the cybersecurity program. Ensure the integration of cybersecurity into and throughout the lifecycle of IT within the enclave.
 - b. Ensure all AF IT cybersecurity-related documentation is current and accessible to proper authorized individuals.
 - c. Support the PM in maintaining connection (ATC) and authorization (ATO) approvals and provide support to the PM in implementing correcting actions identified in the POA&M.
 - d. Coordinate, with the PM and AO staff, development of an ISCM strategy and monitor any proposed or actual changes to the system and its environment.

- e. Continuously monitor the IT and information environment for security-related events, assess proposed configuration changes for potential impact to the cybersecurity posture, and assess the quality of cybersecurity controls implementation against performance indicators such as security incidents, feedback from external inspection agencies, exercises, and operational evaluations.
 - f. Ensure cybersecurity-related events or configuration changes that impact AF IT authorization or adversely impact the security posture are formally reported to the AO and other affected parties, such as information owners/stewards and AOs of interconnected IT.
 - g. Appoint Information System Security Officers (ISSOs) in writing, as required, and provide oversight to ensure continued compliance with cybersecurity policies and procedures.
 - h. Ensure ISSOs and privileged users receive necessary training and obtain cybersecurity certifications, in accordance with Air Force Manual (AFMAN) 17-1303 and maintain proper clearances, in accordance with DoDI 8500.01, *Cybersecurity*.
 - i. Ensure that AF IT is acquired, documented, operated, used, maintained, and disposed of properly IAW DoDI 5000.02 and DoDI 8510.01.
4. Your duties as ISSOs include, but are not limited to the following:
- a. Implement and enforce all AF cybersecurity policies, procedures, and countermeasures.
 - b. Complete and maintain required cybersecurity certification IAW AFMAN 17-1303.
 - c. Ensure all users have the requisite security clearances and need-to-know, complete annual cybersecurity training, and are aware of their responsibilities before being granted access to the IT according to AFMAN 17-1303.
 - d. Maintain all authorized user access control documentation IAW applicable AF Records Information Management Systems (AFRIMS).
 - e. Ensure software, hardware, and firmware complies with the appropriate security configuration guidelines (e.g., Security Technical Implementation Guides (STIGs)/Security Requirements Guides (SRGs)).
 - f. Ensure proper configuration management procedures are followed prior to implementation and contingent upon necessary approval. Coordinate changes or modifications with the system-level ISSM, SCA, and/or the Wing Cybersecurity office.
 - g. Initiate protective or corrective measures, in coordination with the security manager, when a security incident or vulnerability is discovered.
 - h. Report security incidents or vulnerabilities to the system-level ISSM and Wing Cybersecurity office according to AFI 17-130.
 - i. Initiate exceptions, deviations, or waivers to cybersecurity requirements.

5. The PM maintains authority to revoke this appointment based on lack of due diligence, non-compliance with aforementioned policies and other security-related infractions. Direct any questions or concerns to {insert POC} at {insert Phone Number}.

{Insert signature}

PM, USSF

Appendix F: Enterprise Mission Assurance Support Service (eMASS)

Per DoDI 8500.01 Section 9(1)(b), “All systems will be reported in either the eMASS or Enterprise Reporting System (ERS). Components using alternate tools for system data are required to work with the DoD CIO to ensure required system data can be regularly imported to ERS via an application programming interface or other method in accordance with Reference

(y). New systems will be reported in the eMASS or ERS at the beginning of the system development life cycle.”

Per Defense Information Systems Agency (DISA), “eMASS is a web-based Government off-the-shelf and software as a service (SaaS) capability that automates a broad range of processes for comprehensive, fully integrated cybersecurity management, including dashboard reporting, workflow automation, and continuous monitoring supporting RMF for A&A. As a cybersecurity governance, risk, and compliance (GRC) tool, eMASS provides an integrated suite of authorization capabilities to improve cybersecurity risk management. This suite also includes the context to understand how establishing process control mechanisms for obtaining ATO decisions impact DoD missions.

eMASS provides automated, configurable workflows for managing essential security functions at the enterprise level down to system control activities. These workflows support the management of all cybersecurity compliance activities and automation from system registration through system decommissioning.”

The DISA website provides the above and additional information here: www.disa.mil (requires CAC).

For answers to frequently asked eMASS questions:

https://airforce.emass.apps.mil/Content/Help/eMASS_FAQ.pdf

Contact the eMASS support team for information regarding policy and best practices:

disa.meade.id.mbx.emass-tier-iii-support@mail.mil

For detailed instructions on how to acquire eMASS:

<https://rmfks.osd.mil/rmf/HelpAndResources/References/Reference%20Library/Instructions%20for%20Acquiring%20eMASS.pdf>

eMASS Training and Access

Computer Based Training (CBT) on eMASS functionality is available here:

<https://rmfks.osd.mil/rmfresources/eMASS/CBT/index.html>

This course serves as an introduction to eMASS with an overview of registering a system, managing a system, importing assets, initiating a package, and generating system and enterprise level reports.

The CBT takes approximately 2 hours to complete, requires Adobe Flash Player 10 and must be completed in one session. Users who close their browsing session will be required to restart the CBT from the beginning.

At the end of the final exam, a certificate will display on the screen. Certificates use an image background; please ensure your organization allows you to view external images. Users may screenshot or print to pdf to save their certificate.

Once eMASS training is complete, new users shall submit an eMASS account request using a DD Form 2875 to: ssc.cio.cyber@spaceforce.mil

For Non-Classified Internet Protocol Router Network (NIPRNet) eMASS, visit the eMASS website: <https://airforce.emass.apps.mil> to complete the automated online account request

process. Once your .mil email address is verified, the SSC S6 AO eMASS System Administrator will review your account request.

For Secret Internet Protocol Router Network (SIPRNet) eMASS, visit the eMASS website: <https://emass-airforce.csd.disa.smil.mil/> to complete the automated online account request process. Once your SIPRNet email address has been verified, the SSC S6 AO eMASS System Administrator will review your account request.

Questions about the eMASS CBT should be directed to the eMASS Help Desk at disa.meade.id.mbx.emass-tier-iii-support@mail.mil

eMASS Resources

eMASS provides up-to-date user guides and job-aids to assist cybersecurity stakeholders through the many eMASS processes and functions. Once training is accomplished and an account established, the guides are available on the eMASS website.

Appendix G: Information Technology Categorization Selection Checklist (ITCSC) located at AF RMF Knowledge Service (See Resources and Tools)

PLACEHOLDER (ITCSC
Screenshot)

Appendix H: Assess Only

The purpose of the Assess Only Process Guide is to clarify existing DoD guidance Assess Only process for the RMF. Reference the Assess Only Process Guide v2.0.pdf located at AF RMF KS <https://rmfks.osd.mil>.

Appendix I: Topology Guide

1 INTRODUCTION

Space Systems Command (SSC), headquartered in Los Angeles, California, develops, acquires, equips, fields, and sustains critical and resilient space capabilities for warfighters. As part of fielding, SSC is responsible for launch operations, on-orbit checkout, developmental testing, sustainment, and maintenance of military satellite constellations and other Department of Defense (DoD) space systems.

As the premier space capability delivery organization for the United States Space Force (USSF) and the DoD, SSC is laser-focused on countering the very real threats in the present and future contested space domain. Through unity of effort across commercial industry, joint forces, government agencies, and academic and allied partnerships, SSC is developing resilient system-of-systems joint force space capabilities to maintain the nation's strategic advantage in space.

To meet the SSC's initiatives, the SSC S6 provides effective, innovative, and cyber-secure information technology (IT) solutions across all programs to meet warfighter and business needs.

2 OVERVIEW

Network configuration (or topology) is key to performance and security. Providing an accurately depicted functional topology of an information system (IS) or enclave during assessment and authorization (A&A) is a core federal, DoD, and Agency security requirement.

A network topology is how a network or enclave is designed and configured including the physical or logical description of how links and nodes are set up to relate to each other:

- Physical:** A physical network topology shows the site name, location, type of physical media connecting each site, and speed the site link is running speed at which each site link operates. Topologies identify interconnections between systems; by themselves, they do not provide sufficient detail for the assessor to determine risk or allow the Authorizing Official (AO) to grant an authorization decision. A physical network topology is like a wiring topology except connection lines must define the communication technology type A physical network topology is similar to a wiring diagram, but it must also specify the type of communication technology used for each connection (e.g., Gigabit Ethernet, Radio Frequency (RF) coax, T1, OC-12, Serial). A physical network topology may include routers, switches, servers, channel service unit/data service unit devices, cable modems, and wireless access points, including the make and model.
- Logical:** A logical network topology depicts a network from a computer's point of view. Internet Protocol (IP) addressing, subnets, and security devices (e.g., firewalls, gateways, encryption devices, switches or routers, virtual private networks, edge devices, gateway routers, virtual local area network switches, logical network paths, and data flow directions (including internal and external connections) are included in logical network topologies. A logical network topology describes the broadcast domains and IP addresses for network devices with static IP addresses. Logical topologies show individual network devices but rarely show connections to individual

computers; rather, a logical network topology may feed into virtual local area networks and show dependency on cloud-based internet connections. Virtualization means a logical topology may seem noticeably different than a hardware/software list or a physical network topology. It is important to annotate virtual machine devices in a logical topology.

Physical and Logical Diagrams shall be accompanied with a Hardware and Software List

3 PURPOSE

The *SSC S6 AO Topology Guide* provides guidance for SSC S6 AO stakeholders and mission partners to annotate a system or enclave network topology in support of an Authorization to Operate (ATO) effort.

According to the *SSC S6 ATO Required Artifacts Memo*, a topology diagram in accordance with the DoD Architecture Framework (DoDAF) requirements will be provided to support an accurate and timely risk determination from the SSC S6 Security Control Assessor (SCA). Requirements are identified in [Section 4](#). Figure 4 **Error! Reference source not found.** shows an example topology diagram.

This guidance is compiled from multiple DoD requirements, industry best practices, and Defense Information Systems Agency (DISA) standards. These are identified in the References section (Appendix F). Additional resources are included within the section for more information.

4 AUTHORIZATION BOUNDARY (TOPOLOGY) GUIDANCE

The system authorization boundary diagrams should only include assets being assessed as part of the Risk Management Framework (RMF) package. Components outside the authorization boundary may need to be shown for security accountability and/or reference. For example, if a system inherits protection mechanisms, protection devices should be displayed on a topology outside the System Authorization Boundary regardless of where it physically resides in location to the system (See Figure 4).

System authorization boundary (topology) diagram requirements:

- Indicate a System Authorization Boundary with a thick red dashed line (- - - -) that surrounds items being assessed:
 - There can be multiple System Authorization Boundaries (red dashed lined boxes) for a single system indicated on a single topology.
 - Do not place items that are not part of an authorization boundary within the red dashed line
- The Artifact must be clearly dated within 6 months of submission for the ASCA to conduct a Security Controls Assessment.
- Clearly label Command Communications Service Designator (CCSD) identifiers (if applicable)
- Identify internal and external interfaces:
- Include external equipment or system that the system connects to or communicates with

- DISA requires circuits in a system with an internal and external CCSD to be listed in the authorization memo. This can be accomplished by adding circuits in enterprise

Mission Assurance Support Service (eMASS) under System > Details > Connectivity/CCSD.

- Clearly show and label the information flow of registered ports and protocols on the authorization boundary (topology) artifact; they must properly map to the ports, protocols, and services (PPS) worksheet:
 - Programs may submit a separate information flow artifact if adding information flows onto the topology makes it cluttered.
- Consolidate duplicate items to reduce clutter on topologies:
- Example: Three web servers with the same software version, hardware make/model, firmware version, and on the same subnet only need one icon, a list of hostnames, and an IP address range.
 - If a program has four or more duplicate items, indicate this with an ellipsis "..." after the third hostname.
- Devices must display the following:
 - Function name (e.g., Outlook Web Access [OWA] Server, web server, exchange server, intrusion detection system (IDS), intrusion prevention system (IPS), firewall, router, SharePoint server)
 - Hostname (e.g., owa23.us.af.mil, 45thwebsrv)
 - Software/operating system (OS) version (e.g., Server 2019, Windows 10, Oracle Database)
 - Hardware manufacturer (e.g., Dell, Hewlett Packard, Cisco)
 - Hardware make/model (e.g., PowerEdge 2950, ProLiant 2630, ISR 4221)
 - Firmware version (e.g., IOS 12.4 (25a), Phoenix Basic Input Output System 7.43a, NX-OS 6.2(2)) IP address or IP address range (e.g., 137.12.86.52, 137.12.86.52-99). If IPs are not included in the topology diagram, they must be identified within the ports, protocols, and services matrix (PPSM) and/or interconnection documentation.

If the system is classified, the document must be protected in accordance with the program's Security Classification Guidance (SCG). Providing IPs and specific technology may reveal system information that should be handled securely.

[illegible]

Figure 6. Hardware/Software List Template

***** CONTROLLED UNCLASSIFIED INFORMATION *****									
Date Exported:									
Exported By:									
Information System Owner:		POC Name:				Date Reviewed / Updated:			
System Name:		POC Phone:				Reviewed / Updated By:			
DITPR ID:		POC E-Mail:							
#	Port (Required)	Protocol (Required)	Data Service (Required)	Boundary (Required)	FQDN	Purpose			

Figure 7. PPSM/ Boundaries Information List Template

Appendix K: Penetration Testing

Per DODI 8531.01 *DOD Vulnerability Management* Section 1.2, the DoD vulnerability management process must be utilized “to manage and respond to vulnerabilities identified in all software, firmware, and hardware within the Department of Defense Information Network (DODIN).” When performing penetration testing, all DoD components will refer to the guidelines outlined in NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment*.

In summary, a penetration test is a form of authorized security testing performed on targets such as networks, applications, mission systems, and weapons platforms. The primary purpose is to find and exploit vulnerabilities to understand the associated security risks.

A Penetration test team utilizes tactics, techniques, and procedures (TTP) used by real-world threat actors. Automated and manual approaches are leveraged to methodically identify vulnerabilities and validate effectiveness of security control mechanisms and implementations. Every penetration test is different and, depending on the structure and format of the test, the testing team’s perspective and the test scope may vary. A penetration test may include:

- Reconnaissance and Information Gathering
- Scanning and Enumeration
- Vulnerability Scanning, Identification, and Analysis
- Exploitation
- Test Conclusion and Remediation Recommendations.

Penetration testing will not apply to all information systems. Under NIST SP 800-53 Rev. 5, penetration testing is applicable for High baseline systems. However, it is reasonable for the AO to require penetration testing for lower impact systems should assessment of risk identify the need (e.g., interconnected systems).

The following table lists the security controls applicable to penetration testing:

Control ID	Title	Security Control Baselines								
		C			I			A		
		L	M	H	L	M	H	L	M	H
CA-8	Penetration Testing			X			X			X
CA-8(1)	Penetration Testing Independent Penetration Testing Agent or Team			X			X			X
SA-11*	Developer Testing and Evaluation		X	X		X	X		X	X
SA-11(5)**	Developer Testing and Evaluation Penetration Testing									

*Penetration testing is not required but suggested as a method to test custom software applications.

**Implementation of SA-11(5) is required for Cross Domain Solutions (CDS). Refer to CNSSI No. 1253, CDS Overlay.

Appendix L: ATO Prerequisites and Supporting Artifacts

To support an accurate and timely risk determination from the SSC S6 SCA, all authorization requests to the SSC S6 AO shall include at a minimum the following artifacts uploaded to the eMASS.

- RMF Role (PM, ISSM, ISSO, ISSE) appointment letters have been uploaded to eMASS.
- SSC S6 A&A Branch (AO, SCA, SCAR) signed ITCSC.
- SSC AODR and SSC S6 SCA signed Security Plan.
- Topology diagram(s) in accordance with SSC S6 AO Topology Guide. See Appendix I.
- Hardware and Software list(s) will both be imported directly into the eMASS Assets tab utilizing the template exported from eMASS (Located at Assets > Import/Export > Hardware & Software Baseline Inventory). Include original list as an artifact.
- Boundary network device configuration files.
- Signed and dated Access Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Assessment and Authorization (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Incident Response (IR), System Maintenance (MA), Media Protection (MP), Physical and Environmental (PE), Security Planning (PL), Program Management (PM), Personnel Security (PS), Risk Assessment (RA), System and Services Acquisition (SA), System and Information Integrity (SI), System and Communications Protection Procedures (SC), and Concepts of Network Operations (CONOPS) plans or policies.
- Signed and dated plans and policies for privacy (if applicable) Authority and Purpose (AP), Accountability, Audit, and Risk Management (AR), Data Quality and Integrity (DI), Data Minimization and Retention (DM), Individual Participation and Redress (IP), Security (SE), Personally Identifiable Information (PII) Processing and Transparency (PT), Supply Chain Risk Management (SR), Transparency (TR), Use Limitation (UL).
- Security Technical Implementation Guide (STIG) applicability list (i.e., a listing of all STIGs applicable to the information system based on technologies and architecture). The system Program Office is also responsible to ensure the appropriate STIGs have been selected in eMASS at System > Categorization > STIGs, prior to submission. Include original list as an artifact.
- STIG compliance checklist (.ckl file) covering all applicable STIGs for each component type within the system will need to be imported directly into the eMASS Assets tab located at Assets > Import/Export > Import Device Scan.
- STIG benchmark scans for each component type within the system Assured Compliance Assessment Solution (ACAS) will need to be imported directly into the eMASS Assets tab located at Assets > Import/Export > Import Device Scan.
- Vulnerability Scans using ACAS for all assets will need to be imported directly into the eMASS Assets tab located at Assets > Import/Export > Import Device Scan within 60-days of submission.

- PPSM imported into the eMASS Assets tab located at Assets > Ports/Protocols > Add.

Note: For those systems with a connection to a Department of Defense Information Network system the PPS registration / tracking number will be required.- Include DoD PPS Registration Policy Documentation Worksheet as artifact.

- ISCM Strategy (In accordance with the SSC S6 A&A Branch ISCM and ACV Policy).

Per Air Force Instruction (AFI) 17-101 and Department of Defense Instruction (DoDI) 8510.01, **the SCA has the authority to request additional artifacts to clarify risks associated with system security control implementation.** The artifacts named in Appendix I are not a comprehensive list of all system documentation to support implementation of cybersecurity requirements, but rather the minimum requirements necessary for the SSC S6 AO to begin the authorization discussion. Program Managers, Information System Owners, Information System Security Managers, Operators, and Users are expected to address all cybersecurity implementation requirements within their program management, systems engineering, and operational procedure documents. System specific security control implementation and the validation test results should be entered into eMASS using the inherent implementation plan and test results functions respectively.

Information system authorization requests that include all applicable artifacts in Appendix I, meet AO risk tolerance, and are uploaded in eMASS at least **60 days** prior to Authorization Termination Date (ATD) shall receive an authorization decision prior to the ATD. Missing or incomplete documentation may affect authorization decision processing timelines and can result in a higher system risk recommendation.

Appendix M: SSC S6 AO POA&M Policy Memo

PLACEHOLDER (Memo)

Appendix N: Service Level Agreement (SLA) Memorandum of Understanding (MOU)/ Memorandum of Agreement (MOA)

PLACEHOLDER (Memo)

Appendix O: Interconnected Systems

A system interconnection is defined as a direct connection between two or more systems in different boundaries for the purpose of exchanging information and/or allowing access to information, information services, and resources. Additionally, any physical connection that allows other systems to share data also constitutes an interconnection, even if the two systems connected do not share data between them. This includes any network or application interconnections. Interconnections can include permanent connections or temporary connections established for a specific period.

The Executive Summary of NIST SP 800-47 Rev. 1, *Managing the Security of Information Exchanges*, identifies the following four phases of information exchange management. Each phase is further detailed within Section 3 of SP 800-47 Rev. 1.

- “Planning the information exchange: The participating organizations perform preliminary activities; examine all relevant technical, security, and administrative issues; and develop an appropriate agreement to govern the management and use of the information and how it is to be exchanged (e.g., via a dedicated circuit or virtual private network, database sharing, cloud- or web-based services, or simple file exchange)”.
- “Establishing the information exchange: The organizations develop and execute a plan for establishing the information exchange, including implementing or configuring appropriate security controls and developing and signing appropriate agreements”.
- “Maintaining the exchange and associated agreements: The organizations actively maintain the security of the information exchange after it is established and ensure that the terms of the associated agreements are met and remain relevant, including reviewing and renewing the agreements at an agreed-upon frequency”. **Note:** These tasks fall outside the scope of this document since Interconnection Security Agreements (ISAs) can differ depending on the specific case, and organizations can choose the appropriate internal authority, tools, and methodologies.
- “Discontinuing the information exchange: Information exchange may be temporary, or at some point, the organizations may need to discontinue the information exchange. Whether the exchange was temporary or long-term, the conclusion of an information exchange is conducted in a manner that avoids disrupting any other party’s system. In response to an incident or other emergency, however, the organizations may decide to discontinue the information exchange immediately”. **Note:** This stage is out of scope for this document and is not addressed but is depicted from NIST SP 800-47 Rev. 1.

All systems planning to establish interconnection(s) should refer to NIST SP 800-47 Rev. 1, for *Interconnecting Information Technology Systems*, which outlines the specific requirements associated with each of the phases listed above.

It is important to note that the systems planned for interconnection must have already gone through the A&A process and received authorization from the organizations’ respective AO.

Additionally, before an interconnection can be established, the following documents should be established and approved by organizational officials (e.g., S6, Authorizing Official, Program Manager):

- Memorandum of Understanding (or Agreement) (MOU/A): This is a management document that defines, at a high level, each party's roles and responsibilities for the intended connection. The MOU/A does not include technical details and requirements of the interconnection. Such information is reserved for the Interconnection Security Agreement (ISA) which accompanies the MOU/A.
- Interconnection Security Agreement (ISA): The ISA is a technical document that outlines the technical requirements and security considerations for the interconnection identified during the Planning phase. The ISA should include the following sections:
 - **Section 1:** Interconnection Statement of Requirements – This section should establish the requirement for the interconnection, including the business/mission justification. The agencies/organizations initiating the requirement and the systems to be interconnected should be identified in this section.
 - **Section 2:** System Security Considerations – This section details the security considerations that are to be implemented to protect the confidentiality, integrity, and availability of the systems and the data involved. Contents of this section should be provided by both parties and mutually agreed upon. Technical POC, as well as POCs for incident reporting should be included in this section.
 - **Section 3:** Topology diagram – The topology diagram illustrates how the systems are interconnected and the logical location of all components used for the interconnection. All paths, circuits, and components to be used for the interconnection should be depicted in the drawing. Reference the SSC S6 AO Topology Guide 20240213.
 - **Section 4:** Signatory Authority – This section provides the signature lines for each agency/organization's approving authority. Additionally, the ISA's expiration date, periodic review requirements, and other statements as required should be included in this section. The ISA must be signed and dated by both parties.

Sample MOU/A and ISA templates, along with detailed explanation of items that should be included in each document, can be found in NIST SP 800-47 Rev. 1.

CUI

Appendix P: CCSD SIA Template

PLACEHOLDER (Template)

Appendix Q: Security Impact Assessment (SIA) Template

{Insert Letterhead}

MEMORANDUM FOR Space Systems Command (SSC)

FROM: SSC Authorizing Official (AO)
483 North Aviation Blvd
El Segundo, CA 90245

SUBJECT: United States Space Force Space Systems Command Authorizing Official Security Impact Analysis Policy Memo

References: (a) AFI 17-101, *Risk Management Framework (RMF) for Department of Air Force Information Technology (IT)*

(b) NIST SP 800-30 Rev. 1, September 2012, *Guide for Conducting Risk Assessments*

(c) NIST SP 800-37 Rev. 2, December 2018, *Risk Management Framework for Information Systems and Organizations*

(d) NIST SP 800-53 Rev. 5, September 2020, *Security and Privacy Controls for Information Systems and Organizations*

(e) NIST SP 800-128 August 2011, *Guide for Security-Focused Configuration Management of Information Systems*

(f) DoDI 8500.01 14 March 2014, *Cybersecurity*, as amended

(g) DoDI 8510.01 19 July 2022, *Risk Management Framework for DoD Systems*

(h) DoDI 8531.01 15 September 2020, *DoD Vulnerability Management*, Section 3

(i) CNSSI 1253 29 July 2022, *Security Categorization and Control Selection for National Security Systems*

(j) MEMORANDUM FOR SpOC, SSC and STARCOM, 24 Jan 2023, United States Space Force (USSF) Space Authorizing Official (AO) Security Impact Analysis (SIA) Policy

1. **Purpose:** The SSC S6 AO issues detailed implementation guidance on the Assess and Authorize (A&A) process. This memorandum has been coordinated with the USSF Security Control Assessor (SCA) and provides a process for documenting modifications to previously authorized USSF systems, as defined in reference (g), hereafter referred to as Information System (ISs), that impact the authorized IS baselines. SIA is a process to determine the effect(s) a proposed change can cause to the security posture of an IS. Conducting SIA is a mandatory process for all changes per reference (a) 3.10.11 and reference (d) control CM-4: *the organization analyzes changes to the information system to determine potential security and privacy impacts prior to change implementation.*

2. **Scope:** This memorandum covers all ISs under SSC S6 AO Risk Management Framework (RMF) authorization and directly aligns to RMF Step 6 *Monitor Security Controls* to determine the impact of changes to the system and environment. This memorandum is authoritative guidance on this subject and may be used as reference material in forthcoming authorization decisions. The depth and intensity of a SIA, along with associated documentation, varies directly with the scope of a proposed change. A SIA may require little time, or it may entail a detailed process, with security testing, scans, etc.

3. **Background:** The SSC AO requires visibility of an IS security posture in the context of its authorization to ensure changes that have occurred during its lifecycle have been documented, tested, assessed, and approved by the SSC AO or designated authority. Program Manager (PM) or Information System Owner (ISO) tracking changes to a previously approved IS ensures the appropriate risk functions have been executed by RMF stakeholders and ensures the USSF organization has operational visibility of risk within the USSF domain and USSF portion of the Department of Defense (DoD) Information Networks (DoDIN). Section 18.j of reference (f) directs Information Systems Security Managers (ISSM) to “Ensure that cybersecurity-related events or configuration changes that may impact DoD IS and PIT system authorization or security posture are formally reported to the AO and other impacted parties, such as information owners and stewards and AOs of interconnected DoD ISs.”

4. **Discussion:** This memorandum provides standard interpretation of broad DoD policy and documents clear implementation guidance of a tailored approach that ensures policy compliance and operational visibility into IS security baseline changes while avoiding cost and time associated with unnecessary or duplicative testing and organizational reviews. This memorandum is intended to improve efficiency and effectiveness of the continuous monitoring process and assists RMF stakeholders in determining authorization requirements for IS lifecycle upgrades, maintenance, and other out of cycle changes that may impact the IS security baseline.

Reference (c) defines a significant change as a change that is likely to substantively affect the security or privacy posture of a system. Significant changes to a system that may trigger an event-driven authorization action may include, but not limited to:

- Installation of a new or upgraded operating system, middleware component, or application;
- Modifications to system ports, protocols, or services (PPS);
- Installation of a new or upgraded hardware platform;
- Modifications to how information, including PII, is processed;
- Modifications to cryptographic modules or services;
- Changes in information types processed, stored, or transmitted by the system; or
- Modifications to security and privacy controls.

Significant changes to the environment of operation that may trigger an event-driven authorization action may include, but are not limited to:

- Moving to a new facility;
- Adding new core missions or business functions;
- Acquiring specific and credible threat information that the organization is being targeted by a threat source; or
- Establishing new/modified laws, directives, policies, or regulations.

5. Implementing Instructions. To standardize the review process for validating changes to IS security baselines, baseline change requests will be routed through the respective ISSM to coordinate and prioritize review by appropriate RMF stakeholders. All stakeholders must consider RMF processing timelines established by the SSC AO/SSC SCA in support of their project planning efforts. The ISSM will coordinate all activities between the PM/ISO and SSC AO/SSC SCA.

a. Review of any SIA level includes review of previous conditions documented in the Authorization to Operate (ATO) or Interim Authority to Test (IATT). Failure of a PM/ISO to comply with previously documented ATO conditions may preclude the baseline change approval pending adjudication of these discrepancies.

b. All SIA levels defined in this memorandum must have a recorded approval by the cognizant ISSM prior to implementation and review by the SSC AO/SSC SCA. The preferred method to document a baseline change for all levels is a memo signed by the ISSM and uploaded into the Enterprise Mission Assurance Support Service (eMASS) artifacts. For moderate changes to SSC information systems, the approved AFRL ITEC X009 SIA Memo template should be used and sent to the Security Control Assessor Representative (SCAR) for review and SCA routing. SIA level changes that affect separate and distinct authorizations shall be coordinated by program and stakeholders and consolidated into joint requests when appropriate to reduce resource requirements.

6. RMF SIA Levels. To assist the RMF community in determining the appropriate course of action for changes to ISs, the following SIA Levels are provided:

Summary of Change Approval Requirements		
Type	Approver	Documentation
Level 1 Patch	ISSM	AFRL SIA Memorandum, uploaded to eMASS or a signed email from the ISSM acknowledging and concurring on the change.
Level 1 Minor	ISSM	AFRL SIA Memorandum signed by ISSM and uploaded to eMASS. Notify SCAR of the change.
Level 2 Moderate	SCA	AFRL SIA Memorandum signed by PM/ISSM and sent to SCAR via Change Request

		Workflow for review and forward to SCA for signature.
Level 3 Significant	AO/AODR	Submission of eMASS package through Workflow 4.

a. **Level 1 “Patch” – SCA:** Changes that do not require notification to, or concurrence from the SSC AO or SSC AODR. These changes help to maintain up-to-date security posture and do not adversely affect the previously assessed and authorized security baseline.

Note: Software/product version upgrades (i.e., V1.X to V2.X) that introduce new functionality, capabilities, or require security configuration of specified assets to be re-evaluated or implemented new configurations do not fall under Level 1 “Patch”.

(1) Examples of Level 1 “Patch” changes/upgrades include, but are not limited to:

(a) Routine system/network maintenance such as applying software or firmware security updates to remain in compliance with the Department of the Air Force (DAF) Information Assurance Vulnerability Management (IAVM) Program.

(b) Updating Anti-virus (AV)/Enterprise Security Solutions (ESS) signatures and Assured Compliance Assessment Solutions (ACAS) definitions.

(c) Implementing Internet Protocol (IP) Block/Domain Name System (DNS) Black Hole lists or actions required to meet conditions of authorization, if these activities do not meet the criteria of Levels 2 or 3.

(2) **PM/ISO/ISSM Action:** The PM/ISO, in coordination with the ISSM, must update all applicable RMF artifacts affected by the change, and update the “Assets” tab in the eMASS record with the new software version. All updates must be completed within 30 days of the successful change.

(3) **ISSM Action:** Once the change has been implemented, the ISSM will ensure all affected artifacts (Hardware/Software (HW/SW) lists, topology diagram, security plans, etc.) are updated in eMASS. If not addressed in a Vulnerability Management Plan, document concurrence of change through a memorandum, SIA, or signed email.

(4) **SSC AO or SSC AO Action:** None.

b. **Level 1 “Minor” – SCA:** An update to a current authorization where **minor** changes are made to the IS that either do not or minimally impact the IS security baseline as recommended by the PM or ISSM. SCA or AO approval is not required. A Level 1 “Minor” modification of the IS meets the intent of **minor** change, affecting the security posture but not the operation of the system or data types processed. The Level 1 “Minor” change shall

be documented with evidence of ISSM approval/concurrence (i.e., digitally signed Memorandum for Record (MFR) or Security Impact Assessment). The Level 1 “Minor” documentation shall clearly articulate the details of the updates including impact to the approved security baseline under the existing authorization (e.g., impact to HW/SW, operating system (OS), ports and protocols, security controls), and vulnerabilities introduced through vulnerability management. The ISSM shall upload the change documentation including supporting artifacts to the SIPR eMASS record of the affected system.

(1) Examples of Level 1 “Minor” changes/upgrades include, but are not limited to:

(a) Software version updates that do not have security implications that affect the security controls associated with the current authorization and security baseline (e.g., minor OS, version upgrades, software/firmware updates, registry, or permission changes, adding additional pre-existing system assets).

(b) A change to the IS name or other minor administrative type action that requires an ATO authorization update or move within the same physical location (i.e., same building).

(c) Additional hardware/software with the same configuration computing environment as approved in the existing authorization. For example, adding new servers or network devices with the same configuration or core build as those previously approved and within the same physical location (i.e., same building); noting the new servers or network devices may be the same similar model as replaced with more powerful computer components (e.g., upgraded processors, more memory) as normally takes place with a cyclical technical hardware refresh.

(2) **PM/ISO/ISSM Action:** The PM/ISO, in coordination with the ISSM and in the absence of an approved comprehensive Vulnerability Management Plan, will upload an SIA, or signed memo, using the approved AFRL ITEC X009 SIA Memo template, to eMASS along with supporting artifacts. The PM/ISSM must update all applicable RMF artifacts affected by the change and update the “Assets” tab in the eMASS record. All updates must be completed within 30 days of the successful change.

(3) **ISSM Action:** The ISSM is responsible to ensure the Level 1 “Minor” aligns with the ATO/IATT baseline, the IS change meets the intent of Level 1, testing evidence is available upon request, and has validated, by digital signature, that the Level 1, is appropriate and correct. The ISSM shall ensure ACAS scans are available upon request if required to support Level 1 determination. Once the change has been implemented, the ISSM will ensure all affected artifacts (HW/SW lists, topology diagram, security plans, etc.) are updated in eMASS and the SCAR has been notified of the completed change. All updates must be completed within 30 days of the successful change.

(4) **SCAR Action:** The SCAR may review any change documentation and updated artifacts to validate the impact of the change to the system. The SCAR will address any concerns or questions to the PM and/or ISSM.

(5) **SSC SCA or SSC AO Action:** None.

c. **Level 2 “Moderate” – SCA Change Request:** A baseline change to a current authorization for an IS undergoing lifecycle upgrades and/or incorporating **moderate** changes to the IS that do not fall within Level 1 change types. These changes affect the operation of the system and require ISSM and SSC SCA determination. Level 2 change requests must use the approved AFRL ITEC X009 SIA Memo template detailing the change and the analysis performed that determined the overall impact to the security baseline of the system.

(1) Examples of Level 2 “Moderate” changes/upgrades include, but are not limited to:

(a) Adding or removing hardware, software, or other IT that is not within the same configuration of existing devices, software, etc.

(b) OS major version upgrades. (e.g., Windows 7 upgrade to Windows 10)

(c) Modification of system ports, protocols, or services (PPS) using standard ports, and protocols. See Level 3 for non-standard ports and protocols.

(d) New local system connections (permanent or via removable media). Adding an external connection to another system will not require a Change Request eMASS workflow submission but must follow the SSC AO ATC memo and requires an ISSM-signed SIA memo.

(e) Major software application upgrades or a change in device platform (e.g., Juniper router to Cisco router)

(f) Introduction of new technologies not listed above, PPS (see para. 6.e), software/hardware/services not in the approved ATO baseline, technical capabilities, or functions in support of existing or new missions, enhanced features or operational environments that require the application of new STIGs, scans, or other configuration type guides to support a hardened IS and environment.

(2) **PM/ISO/ISSM Action 1:** The PM/ISO, in coordination with the ISSM, will submit an SIA, using the approved AFRL ITEC X009 SIA Memo template, via Change Request Workflow in eMASS. Once the change has been implemented, the ISSM will ensure all affected artifacts (HW/SW lists, topology diagram, security plans, etc.) are updated in

eMASS and the SCAR has been notified of the completed change. All updates must be completed within 30 days of the successful change.

(3) **PM/ISO/ISSM Action 2:** The PM/ISO/ISSM will initiate the eMASS Change Request Workflow up to the SCAR stage for review.

(4) **SCAR Action:** The SCAR shall review the Level 2 Change Request and coordinate with the SCA for further review and approval.

(5) **SCA Action:** The SCA, in the capacity of the Authorizing Official Designated Representative (AODR), will review the Level 2 SIA memo and pertinent documentation to make an approval or disapproval decision. If Level 2 is disapproved, the SCA will document the reason for disapproval and return it in eMASS. If Level 2 is approved, a Workflow Approval Document (WAD) will be generated with “Approve and Complete” workflow decision.

(6) **PM/ISO/ISSM Action 3:** Upon receipt of an approved Level 2 Change Request from the SSC SCA, the PM/ISO in coordination with the ISSM, will perform risk assessments based on approval requirements. The results must be analyzed to ensure proper security configuration is achieved and documented. The eMASS Plan of Action & Milestones (POA&M) must be updated to reflect the new and/or ongoing findings. All weaknesses associated with removed technologies will be closed with comments in the POA&M, and any newly discovered weaknesses will be appropriately documented. Ensure traceability is performed between historical deficiencies (e.g., findings associated with previous authorization, lifecycle management) in the Security Assessment Report (SAR) and POA&M, along with any new deficiencies identified, to assess the system risk after changes/upgrades have been incorporated. Once the change has been implemented, the PM/ISO/ISSM will ensure all affected artifacts (HW/SW lists, topology diagram, security plans, etc.) are updated in eMASS and the SCAR has been notified of the completed change. All updates must be completed within 30 days of the successful change.

d. **Level 3 “Significant” – AO Change Request:** Changes that require full re-authorization. These are significant changes that can include an update to currently authorized baseline that adversely affects the security baseline or a change that is so significant in size and scope that re-assessing risk on a subset of the system would not adequately or accurately reflect current security baseline and risk. All instances will be evaluated by the A&A stakeholders and Level 3 determinations will be made on a case-by-case basis.

(1) Examples of Level 3 “Significant” changes/upgrades include, but are not limited to:

(a) Changes to the System Categorization memo (e.g., update topology, system operational status, cloud deployment, applicable overlays, etc.) (RMF Step 1) and/or Control Selection (RMF Step 2). Submit System Categorization via the RMF Step 2

eMASS workflow instead of the Change Request workflow, as appropriate. *Note: Changes to overlays or Confidentiality, Integrity, and Availability (CIA) high water mark will require resubmission of the eMASS package via Workflow 2 to the SCAR.*

(b) Tech refresh including adding or removing hardware, software, or other IT that is not within the same configuration of existing devices, software, etc.

(c) Modification of system ports, protocols, or services (PPS) using non-standard ports and protocols, if the system is connected to the DoDIN. The DoD ports, protocols, and services (PPSM) office will require a DoD PPSM Emergency/Temporary Request Form signed by the SSC AO. The ports and protocols should match applicable Interface Control Documents (ICDs) approved connections.

(d) Consolidating two or more ATOs for eMASS record reduction efforts where the functions and capabilities have not changed and the ATO security baseline for each authorization can be coherently assimilated with each having like computing environments and risk assessments.

(2) **PM/ISO/ISSM Action:** Schedule meeting with all stakeholders, at a minimum should include the Information Systems Security Engineer (ISSE), ISSM, and PM, for determination.

(3) **SSC SCA or SSC AO Action:** If determination is to re-authorize, a new authorization decision document will be issued once re-authorization requirements have been met. The new authorization will be eligible for up to a full authorization period based on the outcome of the new testing, the SSC SCA risk determination, and other factors such as RMF assessment timelines.

e. **Ports, Protocols, and Services (PPS):** PPS changes require Level 2 and Level 3 process.

(1) **Level 2:** PPS changes/upgrades that modify existing connections that are approved under the current authorization, or a change to the PPS already registered to the information system/network will follow the Level 2 process. Examples include but are not limited to:

(a) Modifications requiring a boundary change request that does not change the security control baseline approved via the SSC AO authorization.

(b) Modifications to the port number used (e.g., adding port 8443/Hypertext Transfer Protocol Secure (HTTPS), in addition to 443/HTTPS) or modifications to the data service used (e.g., adding 80/OCSP, in addition to 80/ Hypertext Transfer Protocol (HTTP)), for IS that are connected to the DoDIN.

(2) **Level 3:** PPS changes/upgrades that introduce new technology, new software, or new hardware that were not previously approved in the current authorized baseline must follow the Level 3 process. Other examples include but are not limited to:

(a) Introduction of Windows Server/Active Directory, MS-SQL, Oracle PPS/interfaces, when the applicable testing was not completed/assessed and not listed in the Software List of the current A&A documentation.

(b) Establishing new connections to systems that cross DoD PPSM Category Assurance List (CAL) boundaries 7/8 or 13/14 that were not previously approved in the current authorized baseline.

(3) All PPS update/revisions for systems connected to the DoDIN are required to be reflected in the DoD PPSM registry.

7. My POC for this matter is {insert Gov POC}, {insert rank}, Security Control Assessor (SCA), SSC/S6 Cybersecurity Division/A&A, {insert contact number}, {insert email}

{Insert Signature}, {Rank}, USSF
Director, S6
Space Systems Command

Appendix R: Authority to Connect (ATC) Process

1. ATC requests, except for Cyber Protection Teams (CPTs), to the SSC/S6 AO shall be submitted in SIPR Enterprise Mission Assurance Support Service (eMASS). Guidance on submitting ATC requests resides within the *Online Functionality Guide* or *Job Aids* on the eMASS *Help* tab.
 - a. ATC decisions are not required for interconnections between systems if both systems are authorized by the same AO and properly documented in the current ATO for all involved systems. Systems under the same AO must have an Interconnection Security Agreement (ISA) signed by the system Information Systems Security Managers (ISSMs) as an artifact in the connected systems eMASS records.
 - b. Systems authorized by the SSC/S6 AO requiring an ATC to Space Force (SF) NIPRNet, SIPRNet, or other SF eMASS registered systems shall be registered in eMASS as “Functional” and use the *Manage ATC* function under the *System Management* tab within their existing eMASS record.
 - c. A system that is authorized by a non-SF AO or is owned by a non-SF organization requiring a connection to a Space system must register those external systems as a *Guest* system in eMASS. Aligned to reference (a), all external ATC requests will submit an ISSM-signed Security Impact Analysis (SIA) memo addressing risk concerns imposed by the connecting system.
 - d. Due to the ephemeral nature of CPT connections, an eMASS *Guest* system will not be registered. CPTs shall submit an ATC request memo to SSC S6 detailing the reason for the request, the Defensive Cyberspace Operations (DCO) mission description, all involved personnel from the CPT by Mission Elements (ME) and/or Support Elements (SE), the location(s) and duration of the connection(s), and the accredited system including identifying baseline tools.
 - e. All systems shall use the following naming convention when registering an ATC in eMASS:
 - (1) Acronym: “Other AO System (Space AO System)” (e.g., “CTE (TSTS)”)
 - (2) Name: “Other AO System connecting to Space AO System” (e.g., “Consolidated Test Environment connecting to Telecommunications Simulator Test Station”)
2. Missing and/or incomplete documentation will increase package processing timelines. The following artifacts from the connecting system shall be uploaded to the eMASS record:
 - a. Signed Authorization Decision Document (ADD) (i.e., Interim Authorization to Test (IATT), Authority to Operate (ATO))
 - b. Security Assessment Report (SAR) with Security Control Assessor (SCA) final risk determination
 - c. System and Connection Description (discussing specific connection details)
 - d. Plan of Action and Milestones (POA&M)

- e. Topology Diagram(s) (including all interconnection details such as boundary devices, firewalls, routers, switches, demilitarized zones (DMZs), etc.)
 - f. Completed PPSM (including all interconnection details)
 - g. Sponsor Memorandum, only for systems requesting connection from outside the Air Force Information Network (AFIN) per reference (a) Chapter 6, *ATC Process*
3. Additional considerations will be given to Special Access Program (SAP) or Sensitive Compartmented Information (SCI) systems requesting an ATC. SAP systems shall be authorized in accordance with (IAW) reference (j), and SCI systems IAW reference (k). SAP and SCI ATC requests must be routed through the respective special program office to support informed reciprocity.
4. The Authorization Termination Date (ATD) of the requesting system must be provided, otherwise the respective Space AO system ATD will be utilized. Blanket ATCs (i.e., three years from date of signature) are not authorized.
5. Systems utilizing a Risk Management Framework (RMF) application (e.g., eMASS, XACTA) on Joint Worldwide Intelligence Communications System (JWICS) shall upload artifacts at the Secret classification level or lower into SIPRNet eMASS. Artifacts classified as Top Secret shall be provided via JWICS email to the system portfolio SCA Representative (SCAR).
6. Our POC is {insert AODR}, {insert Org}, {insert Phone}.

{Insert Signature}, {Rank}, USSF
Director, S6

Space Systems Command~~Signature Block~~

Appendix S: United States Space Force (USSF) Information System Continuous Monitoring (ISCM) and Annual Control Validation (ACV) Policy for SSC Mission Systems

{Insert Date}

MEMORANDUM FOR SSC Space Systems Command

FROM: SSC Authorizing Official (AO)

483 North Aviation Blvd

El Segundo, CA 90245

SUBJECT: United States Space Force (USSF) Information System Continuous Monitoring (ISCM) and Annual Control Validation (ACV) Policy for SSC Mission Systems

References: (a) AFI 17-101, 5 September 2024, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*

(b) DoDI 8510.01, 19 July 2022, *RMF for DoD Systems*

(c) NIST SP 800-53 R5 *Security and Privacy Controls for Information Systems and Organizations*

(d) NIST SP 800-30 Rev. 1, September 2012, *Guide for Conducting Risk Assessments*

(e) DoDI 8531.01, September 2020, *DoD Vulnerability Management*, Section 3

(f) NIST SP 800-37 Rev. 2, December 2018, *Risk Management Framework for Information Systems and Organizations*

(g) CNSSI 1253 *Security Categorization and Control Selection for National Security Systems*, Table D-n

(h) United States Space Force (USSF) Information System Continuous Monitoring (ICSM) and Annual Control Validation (ACV) Policy for Space Mission Systems, 24 Jan 2023

(i) NIST SP 800-137, September 2011, *Information System Continuous Monitoring (ISCM) for federal Information Systems and Organizations*

(j) DoDI 8500.01, 7 October 2019, *Cybersecurity*

(k) DoDI 8581.01, 8 June 2010, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*

1. This policy supplements the current Risk Management Framework (RMF) continuous monitoring guidance, RMF Step 6, and streamlines continuous monitoring and testing requirements for ongoing authorization and maintenance of RMF requests. It also provides operational visibility, annual self-assessments on security control implementations, managed change control, and attentiveness towards incident response duties.
2. Effective immediately, all USSF entities must review and update their ISCM Strategy and the implementation plan in the eMASS system portfolio to reflect the ISCM plan. The ISCM Strategy will depict the method of monitoring controls which are tracked and assessed via automated, semi-automated and/or manual methods. The SSC AO ISCM policy defines the frequency for continuously monitored controls as follows:
 - a. Red Criticality Controls: Shall be reviewed daily and verified monthly by the Information System Security Manager (ISSM). Non-compliant Red Criticality controls require an immediate escalation to the Security Control Assessor (SCA) and AO for a risk management decision concerning disconnect or continued operations.
 - b. Yellow Criticality Controls: Shall be reviewed weekly and verified quarterly by the ISSM. Non-compliant Yellow Criticality controls do not require immediate SCA and AO notification but should be further investigated prior to escalation to the SCA who shall notify the AO for a risk management decision concerning disconnect or continued operations based on AO established process/procedures.
 - c. White Criticality Controls: Shall be reviewed monthly at a minimum and verified annually by the ISSM. Non-compliant White Criticality controls should be made compliant again in due course without escalating to the AO for a risk management decision concerning disconnect or continued operations. However, if non-compliance continues for an extended period, consideration should be escalated to the SCA who will notify the AO based on AO established process/procedures.
3. Effective immediately, programs submit the Annual Control Validation (ACV) via the Annual Security Review eMASS workflow. The controls shall be submitted to the SSC AO on a schedule provided by the SSC AO and/or from their Approved Authorization to Operate (ATO) conditions. The following mandatory controls will be submitted as a part of the 50% selection:
 - a. Red Criticality Controls: Are monitored daily and verified by the ISSM monthly, submit for AO office review annually: IR-9, SC-7, SC-7(14), SC-7(18), SC-8, SI-3, SI-4, SI-4(4) and SI-4(5).
 - b. Yellow Criticality Controls: Are reviewed weekly and verified by the ISSM quarterly. All Yellow controls shall be submitted as part of the program annual control validation submission.
 - c. White Criticality Controls: Are reviewed monthly and verified by the ISSM annually. A portion of these controls shall be submitted as part of the program semiannual control validation submission.

d. Selection Example: High impact baseline with Classified Overlay. The system has 511 baseline controls, 50% of the baseline is 256 baseline controls. The system has 10 Red Criticality and 176 Yellow Criticality controls. The program will have to select 70 additional White Criticality controls to meet the 50% threshold. The additional selection cannot contain any inherited controls.

4. Program Managers can use this process to continuously monitor their systems and maintain positive control of their system statuses. Programs who effectively use this process will be prepared for their next ATO and may be able to submit for authorization anytime during this process.

5. My POC for this matter is {insert Gov POC}, {insert Rank/Title}, SSC/S6 Cybersecurity Division/A&A, {insert Phone Number}, {insert Email}.

{Insert Signature}, {Rank}, USSF
Director, S6
Space Systems Command

Appendix T: AO to AO Transfer Memo

PLACEHOLDER (Memo)

CUI

Appendix U: ~~Appendix T:~~ Decommission Memo

PLACEHOLDER (Memo)

Appendix V: ~~Appendix U~~ References

AFI 17-101, Risk Management Framework for Department of The Air Force Information Technology (IT), (5 September 2024)

AFI 17-110, Information Technology Portfolio Management and Capital Planning and Investment Control, (May 23, 2018)

AFI 17-130, Cybersecurity Program Management, (13 February 2020)

Agency Authorization Playbook, [Agency Authorization Playbook.pdf](#)

Agency Authorization Roles and Responsibilities for FedRAMP CSPs and Agencies (1), [Agency Authorization Roles and Responsibilities for FedRAMP CSPs and Agencies \(1\).pdf](#)

Agency Guide for Multi-Agency Continuous Monitoring, [Agency Guide for Multi-Agency Continuous Monitoring.pdf](#)

Air Force Instruction 17-101 Sections 1.2, 1.6, Risk Management Framework (RMF) For Air Force Information Technology (IT), February 2020

Air Force Instruction (AFI) 17-110, Information Technology Portfolio Management and Capital Planning and Investment Control, 23 May 2018

Chairman of the Joint Chiefs Staff Instruction (CJCSI) 6211.02D, Defense Information Systems Network (DISN) Responsibilities, (24 January 2012)

Cloud Service Provider (CSP) Security Requirements Guide (SRG), Version 1, Release 1, 14 June 2024

CNSSI 1253, Security Categorization and Control Selection for National Security Systems, (29 July 2022)

Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, March 2014

CSP Continuous Monitoring Strategy Guide, [CSP Continuous Monitoring Strategy Guide.pdf](#)

Defense Federal Acquisition Regulation Supplement, Subpart 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting, Revised January 31, 2023

Department of Defense Information Technology Portfolio Repository (DITPR),
<https://ditpr.dod.mil> (CAC required)

DISA Training Catalog: <https://cyber.mil/cyber-training/training-catalog/>

DISA Website: www.disa.mil

DoD Cloud Computing SRGv1r4, <https://public.cyber.mil/stigs/>

DoD Cyber Exchange: <https://public.cyber.mil/dccs/dod-cloud-authorization-process/>

DoD Directive 8140.03, Cyberspace Workforce Qualification and Management Program,
February 15, 2023

DoD Instruction 8500.01, Cybersecurity, March 14, 2014

DoD Instruction 8510.01, Risk Management Framework for DoD Systems, July 19, 2022

DoD Instruction 8582.01, Security of Unclassified DoD Information on Non-DoD Information
Systems, June 6, 2012

DoD Manual 8530.01, Cybersecurity Activities Support Procedures, May 31, 2023

DoD Chief Information Office Memorandum, Department of Defense Cybersecurity Activities
Performed for Cloud Service Offerings, November 2017

DODI 5200.48, Controlled Unclassified Information

DODI 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, (Incorporating Change 1,
August 11, 2017)

DoDI 8500.01, Cybersecurity, (Incorporating Change 1, October 7, 2019)

DoDI 8510.01, Risk Management Framework for DoD Systems, (July 19, 2022)

DoDI 8531.01, DoD Vulnerability Management, Section 3, (September 2020)

DODI 8540.01, Cross Domain (CD) Policy, (Incorporating Change 1, August 28, 2017)

eMASS Process Guide for RMF Practitioners

eMASS Functionality Guide

eMASS, <https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/enterprise-mission-assurance-support-service>

Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical
Infrastructure, May 11, 2017

FedRAMP, <https://www.fedramp.gov/federal-agencies/>

FedRAMP ATO Letter Template (1), [FedRAMP-ATO-Letter-Template \(1\).docx](#)

FedRAMP ATO Process Guide

FedRAMP Agency Guide for Multi-Agency Continuous Monitoring v3.0 (11DEC2020)

FedRAMP Baselines Rev5 Transition Guide, [FedRAMP_Baselines_Rev5_Transition_Guide.pdf](#)

FedRAMP Documents-Templates, <https://www.fedramp.gov/documents-templates/>

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, (February 2004)

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, (March 2006)

I-assure Control Family Templates, [i-Assure Control Family Templates](#)

ICD 503, 21 July 2015, Intelligence Community Information Technology Systems Security Risk Management

[IT Investment Portfolio Suite \(dps.mil\)](#) (CAC required)

Max.gov (FedRAMP Document Repository)

National Cross Domain Strategy and Management Office (NCDSMO)- G-00032-001_00 CDS 101, An Introduction to Cross Domain Solutions

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, Information System Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, (September 2011)

NCDSMO-G-00043-001_00: Implementation Guidance for DOD Suspension of Point-to-Point CDS and Migration to Enterprise Cross Domain Services

NCDSMO-R-00009-001_00, Criteria for Determination of Enterprise Cross Domain Service Provider, (12 December 2019)

NIST SP 500-291Version-2 2013 June 18 FINAL.pdf, [NIST SP-500-291 Version-2 2013 June18_FINAL.pdf](#)

NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems, (February 2006)

NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, (September 2012)

- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information System, (November 2010)
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, (2 December 2018)
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, (March 2011)
- NIST SP 800-47 Rev. 1, Managing the Security of Information Exchanges, (July 2021)
- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, (December 2020)
- NIST SP 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations, (January 2022)
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, (December 2020)
- NIST SP 800-59, Guideline for Identifying an Information System as a National Security System, (August 2003)
- NIST SP 800-60 Volume 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories, (August 2008)
- NIST SP 800-60 Volume 2 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices, (August 2008)
- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, (August 2012)
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, (30 September 2008)
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information System, (10 October 2019)
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-137A, Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment, (May 2020)
- NIST SP 800-160, Volume 1, Rev. 1, Engineering Trustworthy Secure Systems, (November 2022)
- NISTIR 8011, Automation Support for Security Control Assessments: Multiple Volumes

NISTIR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems, (January 2017)

Reusing Authorizations for Cloud Products Quick Guide,
[Reusing Authorizations for Cloud Products Quick Guide.pdf](#)

Risk Management Framework (RMF) Knowledge Service: <https://rmfks.osd.mil>

RMF Knowledge Service: <https://rmfks.osd.mil/>

Space Systems Command S6 Cloud Assessment and Authorization Process Guide, 8 Apr 2024

SSC S6 FedRAMP ATO Letter Template, [Draft SSC S6 FedRAMP ATO Letter Template.docx](#)

SSC S6 ISCM and ACV Memo, [Draft SSC S6 ISCM and ACV Policy Memo.docx](#)

System Network Approval Process (SNAP), <https://snap.dod.mil> (CAC required)

Appendix W: ~~Appendix V:~~ NIST / RMF Training Resource Links

- [eMASS Training](#)
- [I-Assure](#)
- [RMF Knowledge Service](#)
- [Introduction to RMF at Security Awareness Hub](#)
- [RMF for the DoD - NICCS](#)
- [BAI RMF Training](#)
- [NIST RMF Online Introductory Courses](#)

Appendix W: Acronyms List

Acronym	Definition
A&A	Assessment and Authorization
AC	Access Control
ACAS	Assured Compliance Assessment Solution
ACV	Annual Control Validation
ADD	Authorization Decision Document
AF	Air Force
AFI	Air Force Instruction
AFIN	Air Force Information Network
AFMAN	Air Force Manual
AFRIMS	Air Force Records Information Management System
AFRL	Air Force Research Lab
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
AOR	Area of Responsibility
AP	Assessment Procedure
AP	Authority and Purpose
AR	Accountability, Audit, and Risk Management
ASCA	Agent of the Security Control Assessor
AT	Awareness and Training
ATC	Authority to Connect
ATD	Authorization Termination Date
ATO	Authority to Operate
AU	Audit and Accountability
C	Compliant
CA	Assessment and Authorization
CAC	Common Access Card
CAC	Control Approval Chain
CAL	Category Assurance List
CBT	Computer Based Training
CCA	Clinger-Cohen Act
CCB	Configuration Control Board
CCI	Control Correlation Identifier
CCP	Common Control Provider
CCSD	Command Communications Service Designator
CDES	Cross Domain Enterprise Service
CDR	Commander
CDS	Cross Domain Solution
CGRC	Governance, Risk, and Compliance
CIA	confidentiality, integrity, and availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CJCSI	Chairman Joint Chiefs of Staff
ckl	checklist
CM	Configuration Management
CMP	Continuous Monitoring Plan
CMP	Configuration Management Plan
CND	Computer Network Defense

CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
CP	Contingency Planning
CPT	Cyber Protection Teams
CRA	Cybersecurity Risk Assessment
CSO	Chief Security Officer
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
DAF	Department of the Air Force
DAFGM	Department of the Air Force Guidance Memorandum
DATO	Denial of Authorization to Operate
DCO	Defensive Cyberspace Operations
DI	Data Quality and Integrity
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITPR	Defense Information Technology Portfolio Repository
DM	Data Minimization and Retention
DMZ	Demilitarized Zones
DNS	Domain Name System
DoD	Department of Defense
DoDAF	Department of Defense Air Force
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
DRP	Disaster Recovery Plan
ECD	Estimated Completion Date
eMASS	Enterprise Mission Assurance Support Service
EO	Executive Order
EoL	End of Life
ERS	Enterprise Reporting System
ESS	Enterprise Security Solutions
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GO	General Officer
GRC	governance, risk, and compliance
H	high
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol - Secure
HW	Hardware
IA	Information Assurance
IA	Identification and Authentication
IATT	Interim Authority to Test
IAVM	Information Assurance Vulnerability Management
IAW	in accordance with
ICD	Initial Capabilities Document
IDS	Intrusion Detection System
IL	Impact Level
IO	Information Owner
IoT	Internet of Things
IP	Individual Participation and Redress

IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
IS	Information System
ISA	Interconnection Security Agreement
ISC2	Information System Security Certification Consortium
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISSE	Information System Security Engineer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITCSC	Information Technology Categorization and Selection Checklist
ITEC	Integration Testing and Evaluation Center
ITIPS	Investment Portfolio Suite
JWICS	Joint Worldwide Intelligence Communications System
KS	Knowledge Service
L	low
M	moderate
MA	System Maintenance
ME	Mission Elements
MFR	Memorandum for Record
MO	Mission Owner
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Mission Partner
MP	Media Protection
N/A	not applicable
NC	Non-Compliant
NCDSMO	National Cross Domain Strategy and Management Office
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Reports
NSS	National Security System
OS	Operating System
OWA	Outlook Web Access
PAC	Package Approval Chain
PE	Physical and Environmental
PHI	Protected Health Information
PIA	Privacy Impact Analysis
PII	Personally Identifiable Information
PIT	Platform Information Technology
PL	Security Planning
PM	Program Manager
PM	Program Management
POA&M	Plan of Action & Milestones
POC	point of contact
PPSM	Ports, Protocols, and Services Matrix
PS	Personnel Security
PT	Processing and Transparency
RA	Risk Assessment
RF	Radio Frequency
RMF	Risk Management Framework

CUI

SA	System and Services Acquisition
SaaS	software as a service
SAP	Security Assessment Plan
SAP	Special Access Program
SAR	Security Assessment Report
SC	System and Communications Protection Procedures
SCA	Security Control Assessor
SCAR	Security Control Assessor Representative
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SCTM	Security Controls Traceability Matrix
SE	Support Elements
SE	Security
SES	Senior Executive Service
SF	Space Force
SI	System and Information Integrity
SIA	Security Impact Assessment
SIPR	Secret Internet Protocol Router
SIPRNet	Secret Internet Protocol Router Network
SISO	Senior Information Security Officers
SLA	Service Level Agreement
SNAP	Systems/Network Approval Process
SORN	System of Records Notice
SP	Special Publication
SP	Security Plan
SR	Supply Chain Risk Management
SRG	Security Requirements Guide
SSC	Space Systems Command
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SW	Software
tbd	to be determined
TR	Transparency
ttp	tactics, techniques, and procedures
U	Unclassified
UL	Use Limitation
USSPACECOM	United States Space Command
USSF	United States Space Force