DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

AFI17-101_DAFGM2024-01

5 September 2024

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CN
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: Department of the Air Force Guidance Memorandum (DAFGM) to Air Force Instruction (AFI) 17-101, *RISK MANAGEMENT FRAMEWORK (RMF) FOR DEPARTMENT OF THE AIR FORCE INFORMATION TECHNOLOGY (IT)*

By Order of the Secretary of the Air Force, this DAFGM immediately changes AFI 17-101, *RISK MANAGEMENT FRAMEWORK (RMF) FOR AIR FORCE INFORMATION TECHNOLOGY (IT)*, 6 February 2020. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with DAFI 90-160, *Publications and Forms Management*. Ensure all records generated as a result of processes prescribed in this publication adhere to Department of the Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

AFI 17-101 is hereby updated to reflect multiple changes contained within the "Summary of Changes" section of the attached DAFGM.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon incorporation by interim change to, or rewrite of AFI 17-101, whichever is earlier**.**

VENICE M. GOODWINE, SES, DAF
Chief Information Officer

Attachment:
Interim Guidance to AFI 17-101, *RISK MANAGEMENT FRAMEWORK (RMF) FOR DEPARTMENT OF THE AIR FORCE INFORMATION TECHNOLOGY (IT)*

SUMMARY OF CHANGES

This guidance provides interim modifications to policy concerning the Department of the Air Force (DAF) implementation of the Department of Defense (DoD) Risk Management Framework. This guidance applies to Chapter 1, *Program Overview, by* documenting policies specific to the Special Access Program (SAP) community; Chapter 3, *RMF Roles and Responsibilities*, by updating Authorization Official (AO) responsibilities, grade definition, and grade requirements, Information System Owner (ISO), Program Manager (PM), and Information System Security Manager (ISSM) responsibilities, and privacy information identification requirements; and Chapter 4, *RMF Methodology*, by introducing the DAF Organizational Risk Tolerance Baseline (ORTB), documenting policies specific to the SAP community; updating references to multiple documents; modifying references, abbreviations and acronyms, and terms; incorporating changes in leadership with update to Signature block and an organizational name change from Deputy Chief, Information Officer to Chief Information Officer; and revising purpose paragraph records management statement.

The rewrite of AFI 17-101 will change the product number and title to a Department of Air Force (DAF) Instructions to incorporate this DAFGM information.

PURPOSE

*** References to AF changed to read DAF throughout where applicable.**
*** References to "Deputy Chief Information Officer" changed to read "Chief Information Officer" throughout.**
*** References to "SES" changed to read "CSE" throughout.**

(DELETE) Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Information Management System.

(ADD) Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

(MODIFY) 1.1 Purpose. This AFI provides instructions for the implementation of the Risk Management Framework (RMF) for Department of the Air Force (DAF) Information Technology (IT) in accordance with AFPD 17-1, and AFI 17-130, *Cybersecurity Program Management*.

(MODIFY) 1.2.1. This includes IT supporting research, development, test and evaluation (T&E), and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD. DAF IT (see Figure 1.1) includes, but is not limited to, the following: information systems (major applications and enclaves), platform information technology (PIT) (PIT systems, PIT

subsystems, and PIT products), weapon systems, control systems, standalone systems, any other type of systems with digital capabilities, closed restricted networks, IT services (internal & external), IT products (software, hardware, and applications) and boundary requirements for assess and authorize and assess only (see Chapter 5).

(ADD)) 1.2.3.1. DAF IS processing sensitive compartmented information (SCI) or SAP data pertaining to intelligence sources, methods and activities will adhere to applicable DOD policy and Intelligence Community Directives. **(T-0)** For all other SAP-specific IT, DAF IS will follow applicable DoD / DAF policy and procedures, developed in coordination with SAF/AA. **(T-1)**

(MODIFY) 1.2.4. Authority for space mission systems rests with the United States Space Force (USSF) as delegated by United States Strategic Command and United States Space Command. DAF space systems follow DAF cybersecurity policy and processes; where exceptions exist, this Instruction is annotated accordingly. NOTE: Space systems supporting more than one DoD Component will follow cybersecurity policy and guidance in DoDI 8581.01, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*.

(MODIFY) 3.1. Department of the Air Force Chief Information Officer

(MODIFY) 3.1.1. Reports to the Secretary of the Air Force for accomplishment of DAF CIO responsibilities.

(DELETE) 3.1.6. Serves as the final approval authority for National Security System designations.

(MODIFY) 3.3.1. Must be a DoD official and a U.S. citizen. The DAF CIO may appoint AOs as Senior AOs (O-7 or CSE at a minimum) or Subordinate AOs (O-6 or GS-15 at a minimum) when a Senior AO exists within a boundary. This AO hierarchy will allow Senior AOs to manage all IT more efficiently and effectively within their boundaries. **(T-1)**

(ADD) 3.3.1.1. Subordinate AOs may sign authorization decision documents for residual risk of moderate to very low. **(T-1)**

(ADD) 3.3.1.2. Senior AOs must approve all plans of actions and milestones mitigating high / very high risk in accordance with AFI 17-101. **(T-1)**

(ADD) 3.3.1.3. Senior AOs must oversee any escalation to high / very high risk of previously approved moderate or low risk determinations. **(T-1)**

(MODIFY) 3.3.7. Must ensure verification through the DAF Ports, Protocols, and Services Office (af.pps@us.af.mil), that associated ports (internal and external), internet protocols, and data services of the DAF system comply with the requirements outlined in DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)*, including not overriding SCI and SAP policies. **(T-0)**

(MODIFY) 3.3.11. Will ensure a DD Form 2930, *Privacy Impact Assessment (PIA)* is completed for all DAF IT IAW AFI 33-332, *Air Force Privacy and Civil Liberties Program*. **(T-1)**

(ADD) 3.9.13. Will ensure, with coordination of the PM staff, periodic reviews, testing, or assessment of assigned IT are conducted at least annually, are properly documented, and IAW the system ISCM strategy. **(T-2)**

(ADD) 3.10.15. Will ensure Trusted Systems and Networks (TSN) and Supply Chain Risk Management (SCRM) requirements are addressed IAW AFI 63-101/20-101, *Integrated Life Cycle Management*. **(T-2)**

(ADD) 3.10.16. Will ensure the development of a Program Protection Plan (PPP) and evaluate key PPP measures (specifically addressing Supply Chain Risk Management, National Interest Determinations, and Defense Production Act) IAW AFI 63-101/20-101 and AFPAM 63-113, *Program Protection Planning for Life Cycle Management*. **(T-2)**

(ADD) 3.10.17. Will assert Trusted Systems and Network designations via the Information Technology Categorization & Selection Checklist (ITCSC) for DAF IT. **(T-3)**

(ADD) 3.10.18. Review all the data flows and data types associated with their system to determine if Personally Identifiable Information (PII) / Protected Health Information (PHI) data is stored, processed, or transmitted, or if a change is being proposed to the system that would add PII / PHI to a system.

(ADD) 3.10.18.1. In cases where no PII / PHI is present, the DAF ITCSC will serve as a conclusive determination that privacy requirements do not apply to the system. **(T-1)**

(ADD) 3.10.18.2. In cases where PII / PHI is present, a Privacy Impact Assessment (PIA) (DD Form 2930) must be completed in accordance with AFI 33-332, *Air Force Privacy and Civil Liberties Program*. **(T-0)**

(ADD) 3.10.19. Will ensure that once categorization of PII / PHI data is complete, the system will follow existing guidance on completing system security categorization. **(T-0)**

(MODIFY) 3.12.2. Completes and maintains required cybersecurity certification IAW AFMAN 17-1303. Individuals in this position must be U.S. citizens. **(T-0)**

(MODIFY)

Table 3.1. DAF RMF Appointment Matrix.

Role	Appointed / Identified By	Rank Minimum	Reference(s)
DAF CIO+	Secretary of the Air Force (established)	O-9 / CSE	Title 44 United States Code (USC) Section (§) 3506, *Federal Information Policy - Federal Agency Responsibilities*; HAFMD 1-26, *Chief Information Officer*
DAF CISO	DAF CIO	O-7 / CSE	44 USC § 3554, *Information Security - Federal Agency Responsibilities*; DoDI 8510.01
Mission Area Owner	Identified	O-7 / CSE	AFPD 16-14, *Security Enterprise Governance*; DoDI 8510.01
Senior AO*+	DAF CIO	O-7 / CSE	44 USC § 3554; DoDI 8510.01
Subordinate AO*+	DAF CIO	O-6 / GS-15	44 USC §3554; DoDI 8510.01
AODR	AO	O-5 / GS-14	DoDI 8510.01
SCA*+	DAF CISO	O-4 / GS-13	44 USC §3554; DoDI 8510.01
SCAR	SCA	Any	AFI 17-101
PM+	For programs of record, Service Acquisition Executive (SAE) (as applicable); otherwise, ISO performs duties.	Any government official	DoDI 5000.02
ISO*+	For programs of record, SAE (as applicable); otherwise, HAF/SAF 3-letter or MAJCOM 2-letter (as applicable)	Any	CNSSI No. 4009, *Committee on National Security Systems Glossary*

IO / Steward	Identified by the ISSM	Any	DoDI 8500.01, NIST SP 800-37 Revision 2 (800-37r2), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*

ISSE+	PM	Any	DoDI 8510.01
ISSM*+	PM or ISO	Any	DoDI 8510.01
ISSO+	ISSM	Any	DoDI 8510.01
UR	ISO	Any	DoDI 8510.01
1. * Denotes minimum system-level RMF positions **2. + Denotes additional responsibilities and authorities assigned in Attachments**			

(MODIFY) 4.1. **Overview.** The 7-Step RMF process is based on the process outlined in NIST SP 800-37r2 and DoDI 8510.01 and is illustrated in Figure 4.1. Where possible, this Instruction also identifies steps required for the "Assess Only" (see Chapter 5) process. This process is iterative throughout the entire lifecycle for IT IAW DoDI 5000.02, and the DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle (DoD PM Guidebook).

(MODIFY) 4.3.1. Begin this step by completing the DAF ITCSC and DD Form 2930. During this process, the impact of confidentiality, integrity, and availability is categorized into one of three designations (low, moderate, or high) to address the impact of a potential loss of data.

(MODIFY) 4.3.2. If the program's primary mission is not represented on the form's authorization boundary list, the PM or ISO will check "Other" on the ITCSC and submit the document to the DAFRMC for disposition; send to SAF/CNZR Cybersecurity Division, SAF.CNZR.CNZR.Workflow@us.af.mil.

(MODIFY) 4.3.3. IAW AFI 17-110, the Program Manager / Project Manager must register the IT in DAF IT Investment Portfolio Suite (ITIPS), as the governance tool for the DAF CIO, with the exception of those identified by other policy (i.e., special access programs, space, nuclear command, control, and communication, Joint) to be registered in another repository. **(T-2)**

(MODIFY) 4.3.5. The dual-signed ITCSC will be posted to ITIPS as an artifact upon initial registration or when a substantial modification or update is planned or completed. The dual-signed ITCSC documents PM and AO concurrence on RMF CATEGORIZE and SELECT elements. **(T-1)**

(MODIFY) 4.4. SELECT Security Controls. References DoDI 8510.01, CNSSI No.1253, NIST SP 800-30, NIST SP 800-53 Revision 5 (800-53r5), and the DoD and DAF RMF KS (OPR: PM / ISO).

(MODIFY) 4.4.1. The process for selection of security controls is documented at DoDI 8510.01. (Users are advised to consult the DoD and DAF RMF KS, and / or the DAF SAP Cybersecurity Office milSuite website located at **https://www.milsuite.mil/book/groups/usaf-cybersecurity-for-sap/overview** until static references are updated).

(MODIFY) 4.4.2.2. Air Combat Command, the DAF Enterprise AO and common control provider, provides Tier 2 Common Controls (Inheritance) available in eMASS for DAF IT use.

(MODIFY) 4.4.5. Tailor controls as required. Every selected control must be accounted for by one of the following: the organization, ISO, or PM / ISSM. If a control is added or de-selected from the baseline (i.e., tagged as not applicable), then a risk-based rationale must be documented in the security plan and POA&M. Note: Special Access Programs must consult the *Joint Special Access Program (SAP) Implementation Guide* (JSIG) located in the RMF Policy and Guidance section at

https://www.dcsa.mil/Portals/69/documents/io/rmf/JSIG_2016April11_Final_(53Rev4).pdf to determine and manage non-tailorable controls.

(MODIFY) 4.5. IMPLEMENT Security Controls. References DoDI 8510.01, NIST SP 800-53r5, applicable security technical implementation guides, security requirements guides, the DAF ORTB, and the DoD and DAF RMF KS. (OPR: ISO / PM).

(ADD) 4.5.1. The DAF ORTB is an organizational tool that provides scoping considerations such as prioritization and importance, and introduces the order in which security controls or control enhancements are to be implemented. Areas of consideration for the DAF ORTB include policy / regulatory, technology, physical infrastructure, system component allocation, operational / environmental, public access, scalability, common control, and security objective.

(ADD) 4.5.2. Control implementation focuses on identifying and managing the most critical IT risks as early in the process as possible. The ORTB leverages the Control Criticality Rating schemes in eMASS to facilitate and provide visibility of this requirement and establish an implementation order.

(ADD) 4.5.3. Every selected control must be accounted for by one of the following: the organization, ISO, or PM / ISSM. If a selected control is not implemented, then the rationale for not implementing the controls must be documented in the security plan and POA&M. **(T-1)**

(MODIFY) 4.7. **AUTHORIZE System.** After reviewing the security authorization documentation, the AO or Subordinate AO formally accepts or rejects risk by authorizing the IT through an interim authority to test (IATT), authorization to operate (ATO), or a denial of authorization to operate (DATO). (OPR: AO / Subordinate AO).

(ADD) 4.7.2.5. For SAP systems, AOs ensure ISSMs, ISOs, and PMs follow amplifying guidance contained in the most current Risk Posture Guidance for DAF SAP Information Technology (IT) letter located at **https://www.milsuite.mil/book/docs/DOC-662288**.

(MODIFY) 4.8. **Denial of Authorization to Operate (DATO).**

(MODIFY) 4.8.1. If risk is determined to be unacceptable when compared to the mission assurance requirement, the AO or Subordinate AO, in collaboration with all program stakeholders, will issue a DATO. If the system is already operational, the responsible AO will issue a DATO and operation of the system will cease immediately. Network connections will be immediately terminated for any system that is issued a DATO. **(T-0)**

(MODIFY) 4.8.2. Upon issuing the DATO, the AO will provide a copy of the issued document to SAF/CN via email: SAF.CNZR.CNZR.Workflow@us.af.mil. **(T-1)**

(DELETE) 4.10.2. Air Force Information Assurance Platform Information Technology (PIT) Guidebook. The PIT Guidebook provides clarity on the information cybersecurity activities required for all PIT. This includes weapon systems, medical systems, industrial control systems, armament systems, test systems, etc., that qualify as PIT. The Guidebook should be used to

develop local procedures, as enhancement to RMF for PIT that correspond with the product being developed or procured. The Guidebook suggests best practices to be followed in ensuring cybersecurity is "built-in" to the product, but allows local variations. The primary use of the Guidebook is for acquisition of new PIT and to provide guidance on applicability of the RMF to legacy PIT.

(ADD) 4.10.10. Cybersecurity professionals will use the Joint Special Program Implementation Guide (JSIG), located in the RMF Policy and Guidance section at **https://www.dcsa.mil/Portals/69/documents/io/rmf/JSIG_2016April11_Final_(53Rev4).pdf** for enhanced cybersecurity configurations and processes.

References

(ADD) 44 USC § 3506, *Federal Information Policy - Federal Agency Responsibilities*

(ADD) 44 USC § 3553, *Information Security - Authority and Functions of the Director and the Secretary*

(ADD) 44 USC § 3554, *Information Security - Federal Agency Responsibilities*

(ADD) Office of Management and Budget Memorandum**,** *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices***,** 14 September 2022

(REPLACE) DoD Instruction 8510.01, *Risk Management Framework for DoD Systems*, 19 July 2022

(ADD) Department of Defense (DoD), Version 1.0, *Cybersecurity Reciprocity Playbook*, March 2024

(ADD) DoD, *Department of Defense (DoD) Joint Special Access Program (SAP) Implementation Guide (JSIG)*, 11 April 2016

(ADD) DoD, *Department of Defense Information Security Continuous Monitoring Strategy*, January 2023

(ADD) Deputy Secretary of Defense Memorandum, *Resolving Risk Management Framework and Cybersecurity Reciprocity Issues*, 2 May 2024

(ADD) DoD CIO Memorandum, *Cybersecurity Reciprocity Processes and Collaboration Tools*, 20 October 2023

(ADD) DoD CIO Memorandum, *Guidance for the Procurement and Integration of Information and Communications Technology Components into Critical Information and Networks,*

(ADD) DoD CISO Memorandum, *Adoption of NIST SP 800-53 and CNSSI 1253 Revision 5*, 16 October 2023

(ADD) DoD CISO Memorandum**,** *Supporting Guidance on the Reissuance of DoD Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Systems,* 29 March 2023

(ADD) DoD Senior Information Security Officer Memorandum, "*Authorizations to Operate Extensions and Cybersecurity Function Prioritization Guidance*," 3 April 2020

(ADD) DAF Deputy CIO Memorandum, *Cybersecurity Risk Authorization Guidance*, 8 April 2020

(ADD) SAF/AA and SAF/CN Dual Signed Memorandum, *"Risk Posture Guidance for DAF Special Access Program (SAP) Information Technology (IT),"* 25 August 2021

(ADD) Defense Information Systems Agency AO Memorandum**,** *Department of Defense (DoD) Memorandum of Reciprocity for FedRAMP Authorized Moderate Baseline Cloud Service Offerings (CSO) at Impact Level 2 (IL2)*, 15 August 2019

(ADD) NIST SP 800-218, Version 1.1, *Secure Software Development Framework (SSDF): Recommendations for Mitigating the Risk of Software Vulnerabilities*, 24 March 2016

(ADD) NIST SP 800-53r5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020

(DELETE) NIST SP 800-53Ar4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, 18 Dec 2014

(DELETE) NIST SP 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 22 January 2015

Abbreviations and Acronyms

(ADD) 800-53r5—800-53 Revision 5

(ADD) 800- 37r2—800- 37 Revision 2

(ADD) CNSS—Committee on National Security Systems

(ADD) CNSSI—Committee on National Security Systems Instruction

(ADD) CSE—Civilian Senior Executive

(ADD) DATO—Denial of Authorization to Operate

(ADD) ORTB—Organizational Risk Tolerance Baseline

(**ADD) PHI**—Protected Health Information

(ADD) PII—Personally Identifiable Information

(ADD) SCI—Sensitive Compartmented Information

Terms

(MODIFY) Chief Information Security Officer (CISO)—Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Modernization Act (FISMA) and serving as the CIO's primary liaison to the agency's Authorizing Officials (AO), information system owners (ISO), and information systems security officers (ISSO). NOTE: Also known as senior information security officer (SISO) or senior agency information security officer (SAISO).

(ADD) DAF Organizational Risk Tolerance Baseline (ORTB) -
The DAF ORTB is a "Control Baseline," the set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements as well as address protection needs for the purpose of managing risk.

Additional information about the DAF ORTB can be found in the DAF ORTB Implementation Guide located on the DAF RMF KS at **https://rmfks.osd.mil/rmf/Collaboration/Component%20Workspaces/AirForce/Pages/Documents.aspx?RootFolder=%2Frmf%2FCollaboration%2FComponent%20Workspaces%2FAirForce%2FAir%20Force%20Shared%20Document%20Library%2FBase%2FDAF%20ORTB&FolderCTID=0x0120008CEFE2A54FED0C4D8435348C1B283FC5&View=%7BE0F6B4EF%2D0419%2D466B%2DBsEBC%2DB499D12939F3%7D.**

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 17-101

6 FEBRUARY 2020

Cyberspace

RISK MANAGEMENT FRAMEWORK (RMF) FOR AIR FORCE INFORMATION TECHNOLOGY (IT)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: SAF/CNZ

Certified by: SAF/CNZ (Ms. Wanda E. Jones-Heath)

Supersedes: AFI17-101, 23 January 2020

Pages: 41

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*, AFPD 33-3, *Information Management*, and associated processes outlined on the AF RMF Knowledge Service (KS), for managing the life-cycle cybersecurity risk to Air Force Information Technology (IT). This instruction is consistent with Chairman Joint Chiefs of Staff Instruction 6510.01F, *Information Assurance* (*IA*) *and Support to Computer Network Defense (CND)*. This publication applies to all military (active, reserve, guard), civilians, and contractors. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the Office of Primary Responsibility listed above using the Air Force Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility listed above for coordination prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See Air Force Instruction (AFI) 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication Office of Primary Responsibility (OPR) for non-tiered compliance items.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include integration of Special Access Programs into the 17-series, updates to the IT Categorization and Selection Checklist (ITCSC) processes, and the incorporation of Air Force Guidance Memorandum 2018-01 in its entirety.

Chapter 1

PROGRAM OVERVIEW

1.1. Purpose. This AFI provides implementation instructions for the implementation of the Risk Management Framework (RMF) methodology for Air Force (AF) Information Technology (IT) in accordance with AFPD 17-1, and AFI 17-130, *Air Force Cybersecurity Program Management*.

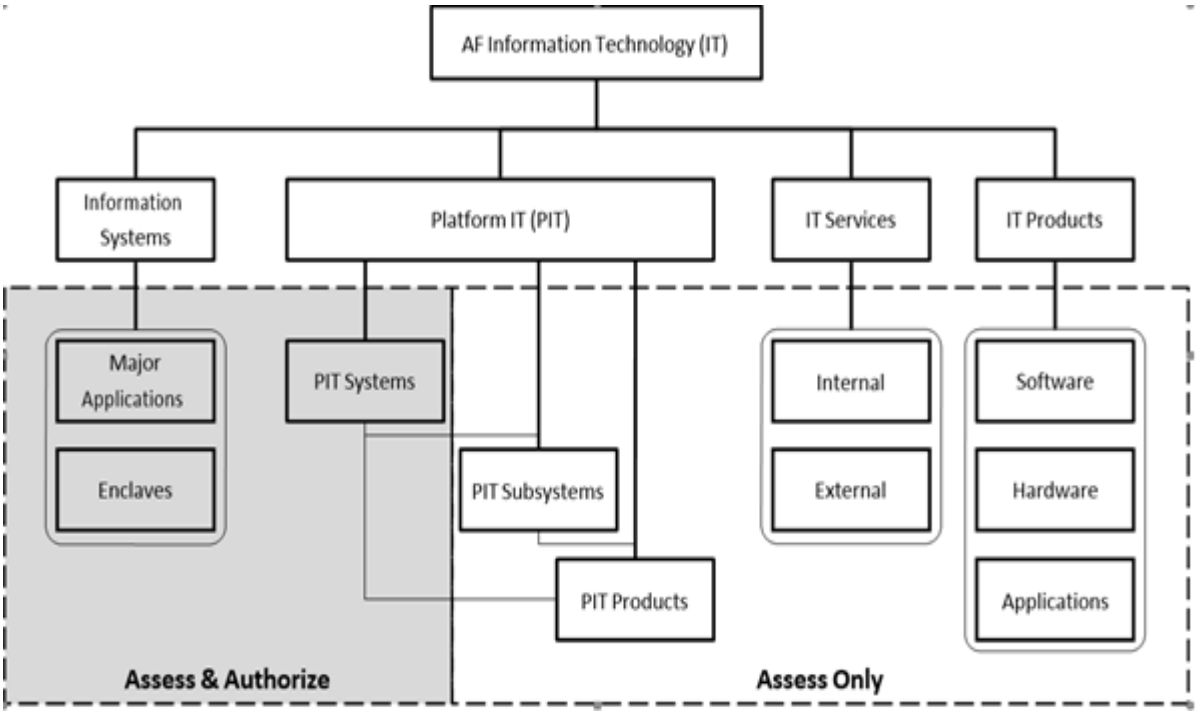
1.1.1. The RMF incorporates strategy, policy, awareness/training, assessment, continuous monitoring, authorization, implementation, and remediation.

1.1.2. The RMF aligns with Secretary of the Air Force/ Deputy Chief Information Officer (SAF/CN) strategic goals and objectives key concept of cybersecurity that works which requires robust risk assessment and management.

1.1.3. The RMF process encompasses life cycle risk management to determine and manage the residual cybersecurity risk to the AF created by the vulnerabilities and threats associated with objectives in military, intelligence, and business operations.

1.1.4. Privacy and security controls are implemented based on the assessed and mitigated residual risk. The controls align with Department of Defense Instruction (DoDI) 8510.01, R*isk Management Framework* (*RMF*) *for DoD Information Technology* (*IT*) and are documented in the RMF security authorization package for AF IT.

Figure 1.1. Air Force IT Categories.



1.2. Applicability.

1.2.1. This includes IT supporting research, development, test and evaluation (T&E), and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD. AF IT (see **Figure 1.1**) includes but is not limited to: information systems (major applications and enclaves), platform information technology (PIT) (PIT systems, PIT subsystems, and PIT products), IT services (internal & external), IT products (software, hardware, and applications) and boundary requirements for assess and authorize and assess only (see **Chapter 5**).

1.2.2. Risk management authorities for special access programs rest with SAF/CN and are executed via this instruction unless higher level guidance exists, in which case compliance will default to the more restrictive policies and directives. The responsible office in support of special access programs IT risk management is the Administrative Assistant to the Secretary of the Air Force and Air Force Senior Security Official (SAF/AA).

1.2.3. This AFI does not apply to the protection of sensitive compartmented information systems (IS) or intelligence, surveillance, reconnaissance mission and mission support systems.

1.2.4. Authority for AF space systems rests with AF Space Command as delegated by United States Strategic Command. AF space systems follow AF cybersecurity policy and processes; where exceptions exist, this Instruction is annotated accordingly. **NOTE**: Space systems supporting more than one DoD Component will follow cybersecurity policy and guidance in DoDI 8581.01, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*.

1.2.5. For IT not centrally managed or that has yet to be assigned an authorizing official (AO), the unit responsible for ownership or operation of the IT shall assign duties for the minimum RMF relevant roles (see **Table 3.1**) required to comply with RMF. The duties shall include the roles and responsibilities for reporting, oversight, and risk management to the AF.

1.3. Objectives.

1.3.1. The RMF provides a disciplined and structured process to perform AF IT security and risk management activities and to integrate those activities into the system development life cycle. 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.

1.3.2. The RMF ensures AF IT assets are assessed for cybersecurity risk. Discovered weaknesses are documented in a plan of action and milestones (POA&M) to mitigate residual risk. An AO, identified at Table 3.1**,** who is supported by an RMF team, accepts the risk for his/her area of responsibility, in accordance with DoDI 8510.01, and the Air Force RMF Knowledge Service (See **Resources and Tools**).

Chapter 2

COORDINATING ROLES AND RESPONSIBILITIES

2.1. Under Secretary of the Air Force (USecAF). The Under Secretary of the Air Force serves as the Department of the Air Force's Chief Information Officer (CIO) and serves as SecAF's agent in assigned policy and program domains.

2.2. Administrative Assistant to the Secretary of the Air Force (SAF/AA).

2.2.1. Works with the Air Force Chief Information Security Officer (CISO/ SAF CNZ) to oversee the establishment of risk tolerance and security controls for IT owned by Air Force organizations.

2.2.2. Provides cybersecurity implementation guidance to the CISO in support of Air Force operational requirements.

2.2.3. Supports identification and oversight of tools to maintain visibility of the security posture of IT throughout the Air Force.

2.3. Secretary of the Air Force for Acquisition (SAF/AQ).

2.3.1. Acquires AF electronic systems including: commercial-off-the-shelf systems, or non-developmental item programs.

2.3.2. Works with the CISO to oversee the establishment of risk tolerance and security controls for AF IT. Provides guidance to organizations on how to implement cybersecurity solutions for operational requirements.

2.3.3. Ensures all security controls are translated into security requirements via systems security engineering and are written into the system requirement document (SRD) on all new and upgrade capability developments.

2.4. Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (AF/A2/6).

2.4.1. Maintains visibility of the cybersecurity posture of AF sensitive compartmented information and the DoD portion of the intelligence mission area IT through automated assessment and authorization tools.

2.4.2. Oversees the establishment of risk tolerance and baseline security controls for AF sensitive compartmented information and DoD portion of the Intelligence Mission Area IT.

2.4.3. Consults with SAF/CNZ as appropriate.

2.4.4. Provides RMF implementation guidance to AF intelligence surveillance and reconnaissance systems and network organizations.

Chapter 3

RMF ROLES AND RESPONSIBILITIES

3.1. Secretary of the Air Force (SAF), Office of the Deputy Chief Information Officer (SAF/CN). SAF/CN:

3.1.1. Reports directly to USecAF for accomplishment of SAF/CN responsibilities.

3.1.2. Provides direction, policy, guidance and oversight for all matters pertaining to the formulation, review, and execution of plans, policies, programs, and budgets in support Air Force Cybersecurity program and Risk Management Framework (RMF) implementation.

3.1.3. Appoints the Chief Information Security Officer (CISO) who develops, implements, maintains, and enforces the AF Cybersecurity Program.

3.1.4. Appoints AOs in coordination with the appropriate mission area owner.

3.1.5. Provides guidance to organizations on how to implement cybersecurity solutions for operational requirements in support of established national, DoD, Joint Chiefs of Staff, or AF security controls for IT and remain within established risk tolerance levels.

3.1.6. Serves as the final approval authority for National Security System designations.

3.1.7. Maintains visibility of the cybersecurity posture for AF IT through automated tools or designated repositories in support of Air Force CIO and appointed AOs.

3.1.8. Ensures an IS owner (ISO) is appointed for all AF IT.

3.1.9. Appoints the AF Chief Architect with responsibility for the AF Cybersecurity Architecture IAW AFI 17-140, *Architecting*.

3.1.10. Is responsible for common control identification and implementation across the Air Force Information Networks.

3.2. Chief Information Security Officer (CISO), SAF/CNZ. Will develop, implement, maintain, and enforce the AF Cybersecurity Program and the RMF process, roles, and responsibilities. The CISO will advocate for any budgets associated with duties below and advocate for AF-wide cybersecurity solutions through the planning, programming, budget and execution process on behalf of the SAF/CN. The CISO is required to be a DoD official (O-7 or SES at a minimum) and a United States citizen. (**T-1**) The CISO:

3.2.1. Completes training and maintains cybersecurity certifications IAW AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*.

3.2.2. Monitors, evaluates, and provides advice to the SAF/CN regarding AF cybersecurity posture.

3.2.3. Coordinates with the SAF/CN and AOs, ensure the cybersecurity risk posture, risk tolerance levels, and risk acceptance decisions for AF IT meet mission and business needs.

3.2.4. Serves as the security control assessor (SCA) or appoints SCAs.

3.2.5. Provides guidance and direction for the agent of the security control assessor (ASCA) establishment and licensing in support of RMF requirements.

3.2.6. Oversees the establishment and enforcement of the AF RMF, roles, and responsibilities; review approval thresholds and milestones within the RMF.

3.2.7. Serves as the chair of the Air Force Risk Management Council.

3.2.8. Participates in Federal, joint, DoD, and AF cybersecurity and RMF technical working groups and forums (e.g., Defense Information Assurance Security Accreditation Working Group).

3.2.9. Adjudicates IT determinations, when a conflict in the IT determination process is identified, in coordination with the Air Force Risk Management Council.

3.2.10. Appoints AF members to the DoD RMF Technical Advisory Group.

3.2.11. Reviews and approves Privacy Impact Assessments (PIAs) submitted IAW AFI 33-332, *The Air Force Privacy and Civil Liberties Program*. The approval of the privacy impact assessment cannot be delegated.

3.2.12. Ensures AF RMF guidance is posted to the AF Component Workspace portion of the DoD Knowledge Service and is consistent with DoD policy and guidance.

3.3. Authorizing Official (AO). The AO is the official with the authority and responsibility for accepting risk for an IT system. With the exception of unmitigated "Very High" and "High" risk, (see **Terms**) the AO balances the level of risk for a system with mission requirements. The AO is the only person with authority to grant authorization decisions within their area of responsibility. All AOs have the flexibility in augmenting, executing, and implementing RMF for systems in their AOR. For example, an AO can create a community-specific guidebook to better clarify guidance. AOs:

3.3.1. Must be a DoD official (O-7 or SES at a minimum) and a U.S. citizen. (**T-1**).

3.3.2. Will complete training and certification requirements IAW AFMAN 17-1303. (**T-1**).

3.3.3. Are appointed by SAF/CN, in coordination with the appropriate Mission Area Owner. The appointment grants authority to authorize IT as defined in the AO appointment memo.

3.3.4. Advocate for cybersecurity-related positions in accordance with DoDI 8500.01, (T-0) AFI 17-130, and AFMAN 17-1303. (**T-2**)

3.3.5. Must ensure an IS owner is appointed prior to issuing an authorization decision. (**T-1**)

3.3.6. Ensure ISOs participate throughout the RMF process and understand the risk imposed on the mission due to operating the IT.

3.3.7. Must ensure verification through the AF Ports, Protocols, and Services Office (**af.pps@us.af.mil**) that internet protocols, data services, and associated ports (internal and external) of the system/enclave comply with the requirements outlined in DoDI 8551.01 *Ports, Protocols, and Services Management (PPSM)*. (**T-0**)

3.3.8. Assist the SAF/CN in providing guidance to organizations on how to implement solutions for operational requirements exceeding the established National, DoD, Joint Chiefs of Staff, or AF baseline controls for IT.

3.3.9. Will approve initial National Security System designations via the Information Technology Categorization & Selection Checklist for AF IT. (**T-1**) **NOTE**: The IT Categorization and Selection Checklist (ITCSC) is available on the Air Force RMF Knowledge Service (See **Resources and Tools**).

3.3.10. Must render authorization decisions that balance mission needs with security concerns for IT within the AO's area of responsibility. The authorization decision documentation will be digitally signed and generated via Enterprise Mission Assurance Support Service (eMASS). Any exceptions to, or conditions of, the authorization decision must be articulated within the authorization decision document. (**T-1**)

3.3.11. Will ensure a *Privacy Impact Assessment* (DD Form 2930) is completed for all IS. (**T-3**)

3.3.12. Will review the security assessment report, risk assessment report, and plan of actions and milestones to ensure there is a clearly defined course of action (see also National Institute of Standards (NIST) Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*). An AO may downgrade or revoke an authorization decision at any time. (**T-3**)

3.3.13. Will review and approve the security assessment plan, the security plan, and system-level Information Security Continuous Monitoring (ISCM) strategy. (**T-3**)

3.3.14. Must ensure all AF IT comply with DoD and AF connection approval processes. See **Chapter 5**, Approval to Connect (ATC) Process. (**T-1**)

3.3.15. Will not delegate authorization decision authority (i.e., to formally accept risk for a system) in accordance with DoDI 8510.01. (**T-0**)

3.3.16. **Note:** Appointment letters and AO boundaries are located on the AF RMF Knowledge Service.

3.4. Air Force Enterprise Authorizing Official (AF Enterprise AO). The AF Enterprise AO is the only authority permitted to grant an approval to connect (ATC) to Air Force Information Networks. ATC authorities for other AF appointed AO's may be approved by SAF/CN in coordination with the Enterprise AO. In addition to the AO responsibilities in **paragraph 3.3** above, the Enterprise AO:

3.4.1. Will establish acceptable security controls and risk tolerance for connecting to the Air Force Information Network and provide guidance to implementing organizations to mitigate risk commensurate with established risk tolerance. (**T-1**)

3.4.2. Must, at a minimum, review the security authorization package for all requests to connect to the Air Force Information Network and assess the impact to enterprise community risk. (**T-2**)

3.4.3. Will render Air Force Information Network connection decisions in the form of an approval to connect (see **Chapter 6**) for non-AF systems and for AF systems falling under another AO. (**T-2**)

3.4.4. Expediently respond to urgent/emergency requests to connect to the Air Force Information Network. This may be delegated to an Enterprise AO designee.

3.5. AO Designated Representative (AODR). The AODR:

3.5.1. Will be appointed by the AO, and at a minimum, be an O-5 or GS-14. Appointments will be in writing (to include all duties and responsibilities) to support the RMF. Digital signatures are authorized for appointment letters. (**T-1**)

3.5.2. **Note:** This role can be supplemented with contractor support; however contractors are not permitted to make decisions on behalf of the government and may only provide advice and guidance.

3.5.3. Must complete AO training and any other training or certification requirements consistent with assigned duties and responsibilities. (**T-1**)

3.5.4. Will provide recommendations to the AO to render authorization decisions based on input from the SCA, ISO, Program Manager (PM), and other AOs and AO Designated Representative (AODR). (**T-3**)

3.5.5. Will perform any and all duties of an AO except for accepting risk by issuing an authorization decision IAW DoDI 8510.01. (**T-0**)

3.6. Security Control Assessor (SCA). The SCA:

3.6.1. Will be appointed by the CISO and will be at least an O-4 or GS-13 with the authority and responsibility for the assessment determination within their assigned area of responsibility. (**T-1**)

3.6.2. Must complete training and maintain appropriate cybersecurity certification IAW AFMAN 17-1303. (**T-1**) **Note**: It is highly recommended SCAs complete both the AO training module and attain the Committee on National Security Systems Instruction (CNSSI) No. 4016, *National Information Assurance Training Standard for Risk Analysts*, certificate for supplemental training (See **Resources and Tools**).

3.6.3. Will ensure the development of the security assessment plan and ensure its integration into the program office's Test and Evaluation Master Plan IAW DoDI 5000.02, *Operation of the Defense Acquisition System*. (**T-0**)

3.6.4. Must prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment, and reassess remediated controls, as required. (**T-3**)

3.6.5. Will periodically assess security controls employed within, and inherited by the IT IAW the Information Security Continuous Monitoring strategy. (**T-3**)

3.7. Security Controls Assessor Representative (SCAR). This position may be an organic or contracted resource. Should the security controls assessor representative be a contractor, they are not permitted to make decisions on behalf of the government but can only provide advice and guidance. The security controls assessor representative works with the Program Manager (PM), IS security manager (ISSM), IS security officer (ISSO), and RMF team to assess security controls for the security controls assessor. The security controls assessor representative:

3.7.1. Will complete training and maintain appropriate cybersecurity certification IAW AFMAN 17-1303. (**T-2**) **Note**: It is recommended that Security Controls Assessor Representatives **(**SCAR) also complete the AO training module and attain the CNSSI No. 4016 certificate for supplemental training.

3.7.2. Ensures security controls are implemented IAW the security plan and are assessed IAW the Security Authorization Package in accordance with DoDI 8510.01. (**T-0**)

3.7.3. Validates assessment results from others' (e.g., Agent of the Security Controls Assessor or ISSM) hands-on, comprehensive evaluations of the technical and non-technical security controls for the IT to determine the degree to which the IT satisfies the applicable security controls.

3.8. Agent of the Security Controls Assessor (ASCA). The Agent of the Security Controls Assessor **(**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. The ASCA:

3.8.1. Must achieve and maintain an ASCA license per the AF and Space ASCA Licensing Guide. (**T-1**)

3.8.2. Responds to PM, ISO, SCA SCAR, and AO requests for information regarding their respective systems.

3.8.3. Performs comprehensive evaluation of the technical and non-technical security controls for the IT to determine the degree to which the IT satisfies the applicable security controls, and provide mitigation recommendations.

3.8.4. Will perform assessment procedures for each applicable security control as outlined in the DoDI 8510.01. (**T-0**)

3.8.5. Will meet the intent of RMF independence between the PM or ISO and the individuals performing security control assessments; the ASCA reports only to the SCA. (**T-2**)

3.8.6. Will not be part of the development team or program office. The PM or ISO provides funding for organizations or contractors to perform ASCA responsibilities. The PM or ISO may not provide direction or oversight to organizations or contractors in support of ASCA responsibilities. (**T-1**)

3.8.7. Will document agreements that include safeguards to prevent a conflict of interests with the development team. (**T-2**)

3.9. Information System Owners (ISO). Official responsible for the overall procurement, development, integration, modification, and operation and maintenance of AF IT. (T-2) An ISO is appointed and performs all PM roles and responsibilities when a PM is not assigned. For AF-wide systems (e.g., Air Force Networks (AFNET) Headquarters Air Force (HAF) and Logistics Model), the ISO will be appointed by the HAF/SAF 3-letter responsible for the capability. For Major Command (MAJCOM)-level or base-level IT, to include base enclaves, and PIT, the appropriate MAJCOM 2-letter appoints the ISO. (**T-3**) No further appointment is required The ISO:

3.9.1. Will identify the requirement for the IT and request funds to operate and maintain the IT in order to assure mission effectiveness. (**T-2**)

3.9.2. Will ensure, with coordination of the PM staff, the development, maintenance, and tracking of the system security plan for the assigned IT. (**T-2**)

3.9.3. Must ensure, with coordination of the PM staff, the development of an ISCM strategy consistent with DoDI 8510.01. (**T-0**)

3.9.4. Reports the security status of the IT including the effectiveness of all implemented security controls in accordance with the ISCM strategy.

3.9.5. Will manage access control requirements, including privileged users, and ensure all personnel receive the requisite security training. (**T-3**)

3.9.6. Conducts the initial remediation actions on security controls based on the findings and recommendations of the security assessment report and work with the SCA to reassess remediated controls.

3.9.7. Ensures the plan of action and milestones is developed for all identified weaknesses and the appropriate steps to mitigate those weaknesses are identified.

3.9.8. Ensures appropriate steps are taken to reduce or eliminate identified weaknesses, then generates the security authorization package and submits the package to the SCA for assessment.

3.9.9. Must Ensure open plan of action and milestones items are updated and closed in a timely manner. (**T-2**)

3.9.10. Ensures consolidated RMF documentation is maintained for systems with instances at multiple locations.

3.9.11. Thoroughly reviews security controls assessment and risk assessment results before submitting the security authorization package to the AO, ensuring the system's cybersecurity posture satisfactorily supports mission, business, and budgetary needs (i.e., indicates the mission risk is acceptable).

3.9.12. Will ensure, with the assistance of the ISSM, and coordination with the PM staff, the system is deployed and operated according to the approved security plan and the authorization package (i.e., the AO's authorization decision). (**T-3**)

3.10. Program Manager (PM). The ISO is assigned the PM duties when no PM is assigned. The PM:

3.10.1. Must identify, implement, and ensure full integration of cybersecurity into all phases of the acquisition, upgrade, or modification programs, including: initial design, development, testing, fielding, operation, and sustainment IAW DoDI 8510.01, AFI 63-101_20-101, *Integrated Life Cycle Management*, and the *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*. (**T-0**) **NOTE**: The DoD Program Manager's Guidebook is available on the Air Force RMF Knowledge Service Administrative Assistant to the Secretary of the Air Force and Air Force Senior Security Official.

3.10.2. Will ensure the program management office is resourced to support IS security engineering requirements and security technical assessments of the IT for the SCA's recommendation, the AOs authorization decision, and other security-related assessments (e.g., Financial Improvement and Audit Readiness IT testing, Inspector General audits). (**T-2**)

3.10.3. Must ensure cybersecurity-related positions are assigned in accordance with Table 3.1 and AFMAN 17-1303. (**T-1**)

3.10.4. Will appoint an ISSM, IAW DoDI 8510.01 (**T-0**), for the program office and ensure the ISSM is certified IAW AFMAN 17-1303. (**T-1**)

3.10.5. Will ensure the IT is registered IAW AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control*. (**T-3**)

3.10.6. Will approve initial National Security System designations via the Information Technology Categorization & Selection Checklist for AF IT. (**T-1**)

3.10.7. Will ensure the development and implementation of a cybersecurity strategy for IT IAW AFMAN 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, and AFI 63-101_20-101. (**T-3**)

3.10.8. Will ensure applicable cyber tasking orders are received and acted upon per cyber tasking order directions. (**T-3**)

3.10.9. Ensures periodic reviews, testing, or assessment of assigned IT are conducted at least annually, and IAW the ISCM strategy.

3.10.10. Will ensure operational systems maintain a current authorization to operate and recommend to the AO that systems without a current authorization are identified for removal from operation. (**T-1**)

3.10.11. Ensures all system changes are approved through a configuration management process, are assessed for cybersecurity impacts, and coordinated with the SCA, AO, and other affected parties, such as IOs/Stewards and AOs of interconnected boundaries.

3.10.12. Will manage the corrective actions identified in the plan of action and milestones, in order to provide visibility and status to the ISO, information owner, AO, and CISO in accordance with DoDI 8510.01. (**T-0**)

3.10.13. Reports security incidents to stakeholder organizations and the SCA. Conduct root cause analysis for incidents and develop corrective action plans as input to the plan of action and milestones.

3.10.14. Will ensure a privacy impact assessment is completed (DD Form 2930) for all IS IAW AFI 33-332, *Air Force Privacy and Civil Liberties Program.* (**T-3**)

3.11. Unit Communications Squadron Commander (CS/CC). Serves as the PM or ISO for the base enclave and performs duties IAW DoDI 5000.02 and AFI 17-130.

3.12. Information System Security Manager (ISSM). The ISSM is the primary cybersecurity technical advisor to the AO, PM, and ISO. For base enclaves, the ISSM manages the installation cybersecurity program, typically as a function of the Wing Cybersecurity Office. That program ISSM may also serve as the system ISSM for the enclave and reports to the CS/CC as the PM for the base enclave. The ISSM:

3.12.1. Ensures the integration of cybersecurity into, and throughout the lifecycle of the IT, on behalf of the AO and in accordance with DoDI 8510.01. (**T-0**)

3.12.2. Completes and maintains required cybersecurity certification IAW AFMAN 17-1303. Individuals in this position must be U.S. citizens. (**T-1**)

3.12.3. Ensures all AF IT cybersecurity-related documentation is current and accessible to properly authorized individuals. (**T-3**)

3.12.4. Supports the PM or ISO in maintaining current authorization to operate, and approval to connect (if required), and in implementing corrective actions identified in the plan of action and milestones.

3.12.5. Coordinates, with the PM and AO staffs, development of an ISCM strategy and monitor any proposed or actual changes to the system and its environment.

3.12.6. Continuously monitors the IT and environment for security-relevant events, assess proposed configuration changes for potential impact to the cybersecurity posture, and assess the quality of security controls implementation against performance indicators. (**T-3**)

3.12.7. Ensures 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 IOs and stewards and AOs of interconnected IT.

3.12.8. Appoints IS Security Officers (ISSOs) and provides oversight to ensure ISSOs follow established cybersecurity policies and procedures IAW DoDI 8500.01. (**NOTE**: ISSO appointments are not required if the ISSM has purview over a small amount of IT, but ISSO appointments are advisable when the ISSM has purview over multiple IT). (**T-3**)

3.12.9. Ensures all ISSOs and privileged users receive necessary technical training and obtain cybersecurity certification IAW AFMAN 17-1301, *Computer Security (COMPUSEC),* AFMAN 17-1303 and maintain proper clearances IAW DoDI 8500.01. (**T-0**)

3.12.10. Ensures the AF IT is acquired, documented, operated, used, maintained, and disposed of properly and IAW DoDI 5000.02 and DoDI 8510.01. (**T-0**)

3.13. Information System Security Officer (ISSO). The ISSO is responsible for ensuring the appropriate operational security posture is maintained for the assigned IT. The ISSM will take on these responsibilities should no ISSO be assigned. This includes the following activities related to maintaining situational awareness and initiating actions to improve or restore cybersecurity posture. The ISSO:

3.13.1. Implements and enforce all AF cybersecurity policies, procedures, and countermeasures. (**T-3**)

3.13.2. Completes and maintains required cybersecurity certification IAW AFMAN 17-1303. Individuals in this position must be U.S. citizens. (**T-3**)

3.13.3. Ensures 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 17-1301. (**T-3**)

3.13.4. Maintains all authorized user access control documentation IAW the applicable AF Records Information Management System. (**T-3**)

3.13.5. Ensures software, hardware, and firmware complies with appropriate security configuration guidelines (e.g., security technical implementation guides /security requirement guides). (**T-3**)

3.13.6. Ensures 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. (**T-2**)

3.13.7. Initiates protective or corrective measures, in coordination with the ISSM, when a security incident or vulnerability is discovered.

3.13.8. Reports security incidents or vulnerabilities to the system-level ISSM and wing cybersecurity office according to AFI 17-203, *Cyber Incident Handling*. (**T-2**)

3.13.9. Initiates exceptions, deviations, or waivers to cybersecurity requirements. (**T-3**)

3.14. Information Systems Security Engineer (ISSE). IAW DoDI 5000.02, and NIST SP 800-160v1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, information system security engineering is an individual, group, or organization responsible for conducting information system security engineering activities. The information system security engineering entity or function:

3.14.1. Employs best practices when implementing security controls, including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques. (**T-3**)

3.14.2. Coordinates their security-related activities with the information security architect, ISSO, ISO, and common control provider. (**T-3**)

3.14.3. Completes training and maintain certification IAW AFI 17-1303. Personnel performing any information assurance Workforce System Architecture and Engineering specialty function(s) (one or more functions) at any level must be certified to the highest level function(s) performed. (**T-2**)

3.15. Information Owner/Steward. An organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, classification, collection, processing, dissemination, and disposal as defined in CNSSI No. 4009, *Glossary*. The Information Owner/Steward:

3.15.1. Provides input to the ISO regarding security requirements and security controls for the IT where the information is processed, stored, or transmitted. (**T-3**)

3.15.2. Establishes the rules for appropriate use and protection of the information, during processing, storage, transmission, and disposal.

3.15.3. Retains responsibility for the protection of the information even when the information is shared with or provided to other organizations. (**T-3**)

3.16. User Representative. The User Representative is the individual or organization that represents operational and functional requirements of the user community for a particular system during the RMF process. The User Representative supports the security controls selection, implementation, and assessment to ensure user community needs are met. While this role is not mandatory, it is highly recommended this role be used. The individuals in this role understand the operating environment, mission criticality, reliability and survivability requirements, etc., of the system.

3.17. Additional Responsibilities. Additional responsibilities and authorities relevant to the roles listed above can be found on the AF RMF KS.

Table 3.1. AF RMF Appointment Matrix.

Role	Appointed/ Identified By	Rank Minimum	Reference(s)
SAF/CN+	USecAF (established)	O-9	HAF MD1-26, *Deputy Chief Information Officer*
CISO	SAF/CN	O-7 / SES	Title 40 United States Code Section 3554; DoDI 8510.01
Mission Area Owner	Identified	O-7 / SES	AFPD 16-14, *Security Enterprise Governance*; DoDI 8510.01
AO*+	SAF/CN	O-7 / SES	40 USC §3506; DoDI 8510.01
AODR	AO	O-5 / GS-14	DoDI 8510.01
SCA*+	CISO	O-4 / GS-13	40 USC §3554; DoDI 8510.01
SCAR	SCA	Any	AFI 17-101
PM+	For programs of record, Service Acquisition Executive (SAE) (as applicable); otherwise, ISO performs duties.	Any government official	DoDI 5000.02
ISO*+	For programs of record, Service Acquisition Executive (SAE) (as applicable); otherwise, HAF/SAF 3-letter or MAJCOM 2-letter (as applicable)	Any	CNSSI No. 4009
IO/Steward	Identified by the ISSM	Any	DoDI 8500.01, NIST SP 800-37r2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*

ISSE+	PM	Any	DoDI 8510.01
ISSM*+	PM or ISO	Any	DoDI 8510.01
ISSO+	ISSM	Any	DoDI 8510.01
UR	ISO	Any	DoDI 8510.01
*** Denotes minimum system-level RMF positions** **+ Denotes additional responsibilities and authorities assigned in Attachments**			

3.18. Cybersecurity Forums. The AF leverages existing DoD and AF governance bodies (e.g., Air Force Security Enterprise Executive Board, Information Technology Governance Executive Board) to discuss cybersecurity risk topics and make organizational and mission area risk decisions. The following forums and online resources provide focused management and oversight of the AF Cybersecurity Program.

3.18.1. Air Force Cybersecurity Technical Advisory Group. The AF Cybersecurity Technical Advisory Group provides technical cybersecurity subject matter experts from across the MAJCOMs and functional communities to facilitate the management, oversight, and execution of the AF Cybersecurity Program. The AF Cybersecurity Technical Advisory Group examines cybersecurity-related issues common across AF entities and provides recommendations to the CISO and Defense Information Assurance Security Accreditation Working Group on changes to the minimally required security and privacy controls (for Air Force Information Network connection) or configurations.

3.18.2. Air Force Risk Management Council (AFRMC). The Air Force Risk Management Council (AFRMC) provides a forum for the senior cybersecurity professionals to discuss issues concerning cybersecurity risk from a mission and business perspective. The council reviews proposed Mission Area or AF RMF control overlays, and RMF guidance. The council standardizes the cybersecurity implementation processes for both the acquisition and lifecycle operations for IT. The Air Force Risk Management Council advises and makes recommendations to existing governance bodies. Finally, the Air Force Risk Management Council recommends assignment of IT to the appropriate AO for systems that fall outside of all defined authorization boundaries.

3.18.3. AF AO Summit. The AO Summit is not a governance body but rather an enabler for both an enterprise-wide and converged organizational perspective to cybersecurity policy development, oversight, implementation, and training. This venue provides the SAF/CN and AOs an opportunity to discuss issues relevant to the RMF, AO Boundaries, IT, AOs, and SCAs.

Chapter 4

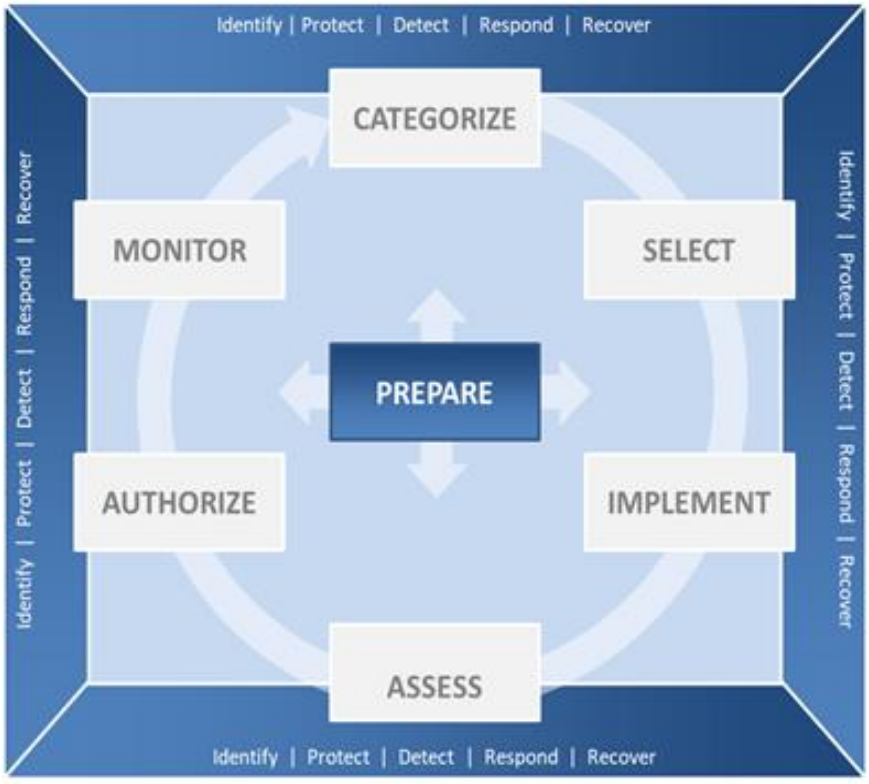
RMF METHODOLOGY

4.1. Overview. The 7-Step RMF process at is based on the process outlined in NIST SP 800-37r2 and DoDI 8510.01 and is illustrated in **Figure 4.1**. Where possible, this Instruction also identifies steps required for the "Assess Only" (see **Chapter 5**) process. This process is iterative throughout the entire lifecycle for IT IAW DoDI 5000.02 and the DoD Program Manager's *Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle (DoD PM Guidebook).*

4.1.1. The DoD RMF KS (**https://rmfks.osd.mil/rmf/Pages/default.aspx**) is the authoritative source for RMF implementation, planning, and execution.

4.1.2. This chapter highlights the AF-specific implementation, key AF roles in each step, and additional resources required to complete the process. This instruction is intended to be a companion to the DoD implementation instructions.

Figure 4.1. RMF for AF IT.



4.2. PREPARE. References CNSSI No.4009, NIST SP 800-37r2, and the DoD and AF RMF KS (OPR: PM/ISO). The purpose of *Prepare* step of the RMF is to identify essential activities of organization, mission and business processes. The program manager/ RMF team is required to fill out the ITCSC during this step to identify and prepare for the management of cybersecurity and privacy risks.

4.3. CATEGORIZE System. References DoDI 8510.01, CNSSI No.1253, *Security Categorization and Control Selection for National Security Systems*, NIST SP 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-60, Volume 1 and 2, *Guide for Mapping Types of Information and Information Systems to Security Categories*, and the DoD and AF RMF KS (OPR: PM/ISO).

4.3.1. Begin this step by completing the RMF ITCSC and DD Form 2930. During this process, the impact of confidentiality, integrity, and availability is categorized into one of three designations (low, moderate, or high) to address the impact of a potential loss of data.

4.3.2. If the program's primary mission is not represented on the form's authorization boundary list, the PM or ISO will check "other" on the ITCSC and submit the completed document to the AF risk Management Council for disposition; send to SAF/CNZR Cybersecurity Division, **usaf.pentagon.saf-cio-a6.mbx.a6zr-workflow@mail.mil**.

4.3.3. All AF IT, IAW AFI 17-110, the Program Manager/ Project Manager must register the IT in AF IT Investment Portfolio Suite (ITIPS), as the governance tool for the AF CIO, with the exception of those identified by other policy (i.e., space, nuclear command, control, and communication, Joint) to be registered in another repository. (**T-3**)

4.3.4. ITIPS will systematically assign a temporary registration number for each registered IT until the next scheduled replication with DoD Information Technology Portfolio Repository. A DoD Information Technology Portfolio Repository number will then be systematically assigned, and included in ITIPS as the permanent official IT registration number for all registered AF IT.

4.3.5. The dual signed ITCSC will be posted to ITIPS an artifact upon initial registration or when a substantial modification or update is planned or completed. The dual signed ITCSC documents PM and AO concurrence on RMF CATEGORIZE and SELECT elements. (**T-3**) **NOTE**: Posting of the ITCSC in eMASS is encouraged, but not required.

4.3.6. All AF IT will be registered in the appropriate eMASS instance: NIPRNet; SIPRNet; DoD Special Access Programs; or Joint Worldwide Intelligence Communications System. (**T-1**)

4.3.7. The organization's eMASS Account Manager/ Organizational System Administrator (See **Resources and Tools**) grants access to eMASS and grants required permissions based on duties and responsibilities. A listing of Account Managers for the AF organizations can be found on the AF RMF KS.

4.3.8. The minimum set of documentation required in support of an RMF authorization decision is the security authorization package and consists of:

4.3.8.1. The security plan

4.3.8.2. The security assessment report

4.3.8.3. The plan of action and milestones

4.3.8.4. The authorization decision document

4.3.9. **Note:** If the aggregation of information in any single document raises the classification beyond the limits of the registered eMASS instance, host that document in the appropriate eMASS instance consistent with the classification of the information therein. Protect all information commensurate with its classification and or applicable security classification guide.

4.3.10. All RMF documentation must be available upon request and will be regularly reviewed to ensure accuracy and completeness, and may be audited by SAF/CNZR, the AO, or SCA at any time.

4.4. SELECT Security Controls. References DoDI 8510.01, CNSSI No.1253, NIST SP 800-30, NIST SP 800-53r4, and the DoD and AF RMF KS (OPR: PM/ISO).

4.4.1. The process for selection of security controls is documented at DoDI 8510.01, Figure 3, RMF for IS and PIT Systems. (Users are advised to consult the DoD and AF RMF KS until static references are updated)

4.4.2. Common Control Identification (available via eMASS).

4.4.2.1. DoD/AF Tier 1and 2 (Inheritance model: Common Controls (Policy) **NOTE**: For information on the three-tiered approach to cybersecurity risk management see DoDI 8510.01, Enclosure 4, Figure 2 (See **Resources and Tools**).

4.4.2.2. Air Combat Command, the enterprise AO and common control provider, provides the Tier 2 Common Controls (Inheritance) available in eMASS for AF IT use.

4.4.2.3. Air Force Network Non-Secure Internet Protocol Router Network (NIPRNet) RMF Inheritance – Core Services; this AFNET RMF package provides inheritance for AFNET Core Services for NIPRNet systems.

4.4.2.4. Air Force Network NIPRNet RMF Inheritance – Security; this AFNET RMF package provides inheritance for AFNET Security for NIPRNet systems.

4.4.2.5. Air Force Network NIPRNet RMF Inheritance – Transport; this AFNET RMF package provides inheritance for AFNET Transport Services for NIPRNet systems.

4.4.2.6. Air Force Network NIPRNet RMF Inheritance – Circuit Enclave (combined); this AFNET RMF package provides security, transport, and core inheritance for AFNET systems.

4.4.2.7. Air Force Network Secure Internet Protocol Router Network (SIPRNet) RMF Inheritance – Circuit Enclave (combined); this Air Force Network – SECRET (AFNET-S) RMF package provides security, transport, and core inheritance for AFNET-S systems.

4.4.3. The security control baseline is selected based on the IT categorization.

4.4.4. Identify and apply overlays that apply to the AF IT. See **Chapter 7**.

4.4.5. Tailor controls as required. Every selected control must be accounted for either by the organization or the ISO. If a control is added or de-selected from the baseline (i.e., tagged as not applicable), then a risk-based rationale must be documented in the security plan and POA&M.

4.4.6. ISCM strategy. Develop and document a system-level ISCM strategy for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system, and monitoring of any proposed or actual changes to the system and its environment of operation.

4.4.7. ISCM Capabilities. Ensure compliance with all applicable cyber tasking orders related to host based security system and assured compliance assessment solution tools in support of continuous monitoring.

4.4.8. ISCM strategy review and approval. The AO's staff will develop and implement processes whereby the AO (or designee) reviews and approves the security plan and ISCM strategy submitted by the PM or ISO.

4.5. IMPLEMENT Security Controls. References DoDI 8510.01, NIST SP 800-53r4, applicable security technical implementation guides, security requirements guides, and the DoD and AF RMF KS. (OPR: PM/ISO).

4.6. ASSESS Security Controls. References DoDI 8510.01, NIST SP 800-30, NIST SP 800-53Ar4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, applicable Security Technical Implementation Guide, Security Requirements Guides, and the DoD and AF RMF KS. Use DoDI 8510.01, enclosure 6 instructions for details for assessing security controls (OPR: SCA).

4.7. AUTHORIZE System. After reviewing the security authorization documentation, the AO formally accepts or rejects risk by authorizing the IT through an interim authority to test, authorization to operate, authorization to operate with conditions, or a denial of authorization to operate. References DoDI 8510.01, enclosure 6 (OPR: AO/AODR).

4.7.1. AOs will issue an interim authority to test, authorization to operate, or an authorization to operate with conditions for any risk determined not to be "Very High" or "High". (**T-0**)

4.7.2. Authorization to operate with conditions for unmitigated "Very High" or "High" risk.

4.7.2.1. The SAF/CN is the only Air Force authority that may grant an AO the approval to issue an Authorization to Operate (ATO) with "Very High" or "High" risk/ (formerly known as CAT I) non-compliant security controls that cannot be corrected or mitigated immediately, but where the overall risk is acceptable due to mission criticality. Delegation below the SAF/CN is not authorized. IT with "Very High" or "High" risk, which are authorized by other DoD Components connecting to the AF information networks require Component CIO approval, and a joint systems requires DoD CIO approval.

4.7.2.2. IT with unmitigated "Very High" or "High" risk non-compliant security controls must follow the Very High/High Package Submission Guide requiring the Authorizing Official to submit completed packages to the SAF/CN for approval prior to making an authorization decision. (**T-0**)

4.7.2.3. For "Very High" or "High" risk authorizations, the authorization to operate with conditions will be issued for up to 1 year. When a 1-year authorization to operate with conditions is issued, the authorization to operate with conditions must specify a review period that is within 6 months of the authorization termination date (ATD). (**T-1**)

4.7.2.4. If the system still requires operation with a level of risk of "Very High" or "High" after 1 year, the AF CIO must again grant permission for continued operation of the system. (**T-0**)

4.8. Denial of Authorization to Operate.

4.8.1. If risk is determined to be unacceptable when compared to the mission assurance requirement, the authorizing official, in collaboration with all program stakeholders, will issue a denial of authorization to operate. If the system is already operational, the responsible AO will issue a denial of authorization to operate and operation of the system will cease immediately. Network connections will be immediately terminated for any system that is issued a denial of authorization to operate. (**T-0**)

4.8.2. Upon issuing the denial of authorization to operate, the AO will provide a copy of the issued document to SAF/CN via **usaf.pentagon.saf-cio-a6.mbx.a6zr-workflow@mail.mil**.

4.9. MONITOR Security Controls. References DoDI 8510.01 and NIST SP 800-137, *Information Security Continuous Monitoring* (ISCM) *for Federal Information Systems and Organizations* (OPR: PM/ISO and ISSM).

4.9.1. DoDI 8510.01 and the DoD RMF KS for Continuous Monitoring provides a detailed framework on continuous monitoring, which should be used to augment the continuous monitoring program for the IT.

4.9.2. The objective of an Information Security Continuous Monitoring (ISCM) program is to determine if the complete set of planned, required, and deployed security controls within a system or inherited by the system continue to be effective over time in light of inevitable changes.

4.9.3. Documenting proposed or actual changes to a system or its environment of operation and subsequently assessing the potential impact those changes may have on the security state of the system or the organization is an important aspect of security control monitoring.

4.9.4. All implemented security controls, including management and operational controls, must be regularly assessed for effectiveness, even if monitoring them is not easily automated.

4.9.5. Authorizing Officials must consider how ISCM will be implemented organization-wide as one of the key components of the security life cycle represented by the RMF.

4.9.6. Individual system-level ISCM strategies must align with the organization's broader ISCM strategy.

4.9.7. **Note:** If the change results in a new "Very High" or "High" risk non-compliant security control(s) that can be corrected within 30 days or a new Moderate risk that can be corrected/satisfactorily mitigated within 90 days, the system can continue to operate under the existing authorization decision and connection approval as referenced in DoDI 8510.01.

4.10. Resources and Tools.

4.10.1. DoD PM Guidebook. *The DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework* (RMF) *into the System Acquisition Lifecycle*. The DoD PM Guidebook supports the policies in this AFI by providing specific procedures and is capable of implementing changes as industry and policy dictate.

4.10.2. *Air Force Information Assurance Platform Information Technology* (PIT) *Guidebook*. The PIT Guidebook provides clarity on the information cybersecurity activities required for all PIT. This includes weapon systems, medical systems, industrial control systems, armament systems, test systems, etc., that qualify as PIT. The Guidebook should be used to develop local procedures, as enhancement to RMF for PIT that correspond with the product being developed or procured. The Guidebook suggests best practices to be followed in ensuring cybersecurity is "built-in" to the product, but allows local variations. The primary use of the Guidebook is for acquisition of new PIT and to provide guidance on applicability of the RMF to legacy PIT.

4.10.3. Agent of the Security Control Assessor Licensing Guide. The number and complexity of AF IT may require the AF agent of the security control assessor to designate qualified entities as agent of the security control assessor to perform assessment actions. The AF SCA created the ASCA Licensing Guide to appoint licensed, qualified agents to provide accurate, consistent, and trusted AF and Space IT assessments.

4.10.4. Air Force Plan of Actions and Milestones (POA&M) Guidebook.

4.10.4.1. The IT security POA&M is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. For further POA&M information, refer to the Air Force POA&M Guidebook.

4.10.5. The Department of Defense (DoD) Issuances website is provided by the Executive Services Directorate and is located @ **https://www.esd.whs.mil/dd/**.

4.10.6. Information and references associated with the Committee on National Security Systems (CNSS) can be found @ **https://www.cnss.gov/CNSS/issuances/Instructions.cfm**.

4.10.7. Information and references associated with the National Institute of Standards and Technology (NIST) can be found on Computer Security Resource Center website @ **https://csrc.nist.gov/publications/sp**.

4.10.8. Information and references associated with eMASS or the eMASS Account Manager role can be found in the eMASS Online User's Guide @ **https://airforce.emass.apps.mil/Content/Help/eMASS_User_Guide.pdf**.

4.10.9. The Air Force RMF Knowledge Service (KS) is a dynamic online knowledge base that supports RMF implementation, planning, and execution by functioning as the authoritative source for Air Force RMF procedures and guidance consistent with applicable policy and guidance and is located @ **https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx**

Chapter 5

AF IT ASSESS ONLY REQUIREMENTS

5.1. PIT Subsystems, PIT Products, IT Services, and IT Products. IT categorized below the system level will not require an authorization decision. This IT will follow the Assess Only process. The IT below the system level must be securely configured (in accordance with applicable DoD policies and security controls), documented in an assessment package, and reviewed by the responsible ISSM, under the direction of the AO, for acceptance or connection into an authorized IS or PIT System. (**T-1**)

5.1.1. PIT**.** The PIT system owner (i.e., ISO) may determine that a collection of PIT rises to the level of a PIT System with the AO's approval. The ISSM (with the review and approval of the AO) is responsible for ensuring all PIT completes the appropriate RMF processes prior to incorporation into or connection to a system or enclave. PIT may be categorized using CNSSI No. 1253 with the resultant security control baselines tailored as needed. Otherwise, the specific cybersecurity needs of PIT must be assessed on a case-by-case basis and security controls applied as appropriate.

5.1.2. IT Services. Organizations that use internal IT services will complete the ITCSC to ensure the categorization of the system delivering the service is appropriate to the confidentiality, integrity, and availability needs of the information and mission. (**T-1**)

5.1.3. Organizations that use external IT services provided by a non-DoD federal government agency, except cloud services, must ensure the categorization of the system delivering the service is appropriate to the confidentiality, integrity, and availability needs of the information and mission, and that the system delivering the service is operating under a current authorization from that agency. (**T-2**)

5.1.4. Organizations contracting for external IT services in the form of commercial cloud computing services must comply with the DoD *Cloud Computing Security Requirements Guide* and applicable procedural guidance. (**T-0**)

5.1.5. IT Products. The system administrator will configure IT products in accordance with applicable security technical implementation guides under a cognizant ISSM and SCA. (**T-1**) security technical implementation guides are product specific and document applicable DoD policies and security requirements, as well as best practices and configuration guidelines. When a Security Technical Implementation Guide is not available for a product, a Security Requirements Guide will be used as applicable. (**T-1**)

5.1.6. IT Product, Software, and Application Certification Assessment. ISSMs have the responsibility to exercise due diligence on IT product software and applications (software products) that reside on their enclave/system. At a minimum, software products will be assessed for supportability, operability, compatibility, and security to ensure the products present an acceptable risk to the AFIN. (**T-1**) This can be accomplished via the following methods:

5.1.6.1. Assess and Authorize. ISSM's may incorporate software assessment and evaluation by integrating the Software Assessment Report into their system enclave's security authorization package. Follow the guidance and use the template on the DoD RMF KS.

5.1.6.2. Air Force Software and Application Certification Assessment. Software products may be assessed through the AF Software and Application Certification Assessment process managed by the Air Force Network Integration Center. The Enterprise SCA then certifies software products for inclusion on the AF Evaluated Products List. Testing may be accomplished by the Cyberspace Capabilities Center or by the organization sponsoring the software product. Software products are certified for use on computers running the Standard Desktop Configuration or DoD Server Core Configuration, applications, and approved mobile devices on the AFIN. Instructions, templates, and the testing methodology are located on the Software Certification Assessment home page.

5.1.6.2.1. The wing ISSM and or the responsible AO will endorse and submit the application request worksheet. (**T-3**)

5.1.6.2.2. Once the Application Request Worksheet is accepted by the Cyberspace Capabilities Center, testing is accomplished by either the sponsor or Cyberspace Capabilities Center. The Authorizing Official or sponsor must ensure that the testing is conducted on an environment external to the operational network. (**T-2**)

5.1.6.2.3. If the IT product presents an acceptable risk (e.g., moderate or below) to the information system, the major version of the product will be certified for up to 3 years by the AF Enterprise SCA and placed on the AF Evaluated Products List by the Enterprise Authorizing Official.(**T-1**) This certification is not an ATO. The system or enclave ISSM must implement any required mitigations to reduce the risk before placing the software product within the system or enclave. The ISSM must update the applicable system or enclave assessment and authorization documentation and hardware/software lists to reflect any solutions implemented. (**T-1**) This update will be considered a "no security impact" modification to the system authorization.

5.2. Reciprocity. For products not already assessed via the RMF or the AF software and application certification assessment process, the Enterprise AO allows ISSMs to use software products that are certified by another Federal/DoD AO or SCA.

5.3. Evaluated Products. A list of recognized sources can be found on the AF RMF KS. These software products are considered assessed and require no additional formal test or evaluation, so long as the actual environment, use, and configuration aligns with the intended environment, use, and configuration documented in the assessment package.

5.4. Contingencies. Compliance with this decision is contingent upon the following conditions:

5.4.1. The software product and major version is verified on one of the recognized sources.

5.4.2. Prior to implementation, the system/enclave ISSM must implement any required mitigations to reduce the security risk. (**T-1**)

5.4.3. The system/enclave ISSM must update their applicable RMF documentation and hardware/software lists to reflect any solutions implemented. This update will be considered a no security impact modification to the system authorization. (**T-1**)

5.5. Software Products Excluded from AF SACA. The following software products must be submitted through the AF Enterprise AO processes. (**T-2**)

5.5.1. Products whose main function is encryption, but does not have *Federal Information Processing Standard* 140-2 certification.

5.5.2. Software that does not have a vendor or sponsor responsible for developing security patches.

5.5.3. Software with immitigable Moderate (CAT II) or higher vulnerabilities.

5.5.4. Software that uses ports, protocols, or services not listed in the DoD Category Assurance List.

5.5.5. Unsupported freeware and shareware.

5.5.6. Open source software with no configuration/software support plan.

5.5.7. IA or IA-enabled products/software IAW Committee on National Security Systems Policy No. 11, *National Policy Governing the Acquisition of Information Assurance* (IA) *and IA-Enabled Information Technology Products*.(**T-2**)

5.5.8. Additional information about the Air Force Assess Only process can be found in the Air Force Assess Only guide located on the AF RMF KS.

Chapter 6

APPROVAL TO CONNECT (ATC) PROCESS

6.1. Overview. The approval to connect Approval to Connect (ATC) process is one instance of the AF's implementation of reciprocity between AOs. It is a formal evaluation of the risk of connecting systems to the receiving enclave; the ATC is a means to manage community risk. Having an ATO does not entitle systems to an ATC from the receiving AO.

6.2. Duration and Expiration. In order for a system to request an ATC from a site or enclave, both the AF system and the destination enclave must have a valid and current authorization. The system ATC expiration date will be no later than the authorization termination date of the ATO for that system. For a system under continual reauthorization, the connection authorization must be reevaluated upon a significant system modification, significant change to the threat or risk posture, or every 3 years; whichever comes first.

6.3. Note: Although this Instruction specifies the requirements for connections to the AF Information Networks, other AOs are encouraged to use this process to authorize connections to enclaves within their authorization (formerly accreditation) boundary

6.4. Connection to the DoD Information Network. For enclaves requiring a circuit connection from Defense Information Systems Agency, ISSMs must follow the DoD Information Network Connection Process Guide to ensure all required artifacts are provided on initial submission. Connection requests will be coordinated through the AF Enterprise AO.

6.5. Connection to the Air Force Information Networks (AFIN). The AF Enterprise AO is the only authority permitted to grant an ATC to the AFIN. ATC authorities for other AF appointed AO's may be approved by SAF/CN in coordination with the Enterprise AO.

6.5.1. AF systems authorized through the AF Enterprise AO will receive an ATC after the system is reviewed for compliance with the required security controls, and the community risk imposed by the connecting system is determined to be at an acceptable level.

6.5.2. AF systems authorized through another AF AO will submit the ATC request through eMASS.

6.5.3. Non-AF owned systems with approved authorizations (i.e., "Guest System", see **para 6.6**) are required to have an ATC request initiated in eMASS by the AF sponsor, the PM, or information system owner before the IT connects to the AFIN.

6.5.4. The AF Enterprise SCA will identify and maintain a listing of the Tier 1and 2 (common) security controls on the Air Force RMF Knowledge Service. Furthermore, the AF Enterprise SCA will specify continuous monitoring requirements for each of the identified common controls. (**T-1**)

6.5.5. Certain security controls are designated as required (to address community risk concerns) of all systems requesting a connection to the AFIN. Some of these required controls may be inherited from the Tier 1and 2 Common security controls. Required controls may not be tailored during the security control selection or tailoring steps. Regardless of the source (i.e., Tier 1and 2 inherited or provide by the system), a status of "Compliant" or "Non-Compliant" is required for each of these controls. The assessment of these controls and associated artifacts will determine whether the AF system poses an unacceptable risk to the AFIN or other systems

connected to or residing on the AFIN (i.e., imposes community risk). Furthermore, the AF Enterprise SCA will specify continuous monitoring requirements for each of the identified required controls.

6.5.6. The AF Enterprise AO will document the ATC decision in eMASS. (**T-1**)

6.6. Guest System Registration. A special case, limited registration of a system that is authorized by a non-AF Authorizing Official, or is owned by a non-Air Force organization but is hosted within the AFIN.

6.6.1. IT identified as a Guest System must provide the name of the AF sponsor to **usaf.pentagon.saf-cio-a6.mbx.a6zr-workflow@mail.mil**.

6.6.2. Guest system requests must provide: system acronym, system name, brief system description, authorization termination date, and organization that granted the authorization. If possible, identify the AF community that will use the system and a recommended sponsor.

6.6.3. SAF/CN will prepare a memo to document the appointed sponsor. The AF sponsor will then enter the system into eMASS and act as a liaison with the external customer. Systems authorized by another AO are required, as a minimum, to provide a topology and valid authorization document for the system being connected. Additionally, the following RMF artifacts or other equivalent are required: Sponsor memo; authorization decision document; port, protocol, and services listing; hardware/software list; security assessment report; and plan of action and milestones. Additionally, space systems identified as AF IT investments must register in ITIPS. (**T-1**)

6.7. ATC Process for Air Force Functional/Mission Systems.

6.7.1. AF functional/mission systems (e.g., A4, SAF/Financial Management (SAF/FM), program management offices) with an AF Authorization to Operate, interim authorization to test, or authorization to operate (ATO) with conditions signed by an AF AO (other than the AF Enterprise AO) require an ATC to the AF information networks.

6.7.2. The Functional/Mission System program manager or AO Staff is responsible for submitting requests for obtaining an ATC from the AF Enterprise AO. For systems/enclaves connecting to/through the AFIN, ATC requests are submitted to the AF Enterprise AO in eMASS as a "Guest System". For systems/enclaves connecting to/through the AFNET or AFNET-S, ATC requests are submitted to the AF Enterprise AO through the "Manage ATC" function in eMASS. Contact the AF Enterprise AO staff for additional connection (contractor, commercial internet service provider, direct) information and guidance.

6.8. Continuous Monitoring. AF IT ISSMs must ensure the controls identified as required for an ATC are monitored IAW the published continuous monitoring strategy guidance. The details will be included in the system-level ISCM strategy and evaluation and approved by the receiving AO. (**T-3**) If the system fails to meet the continuous monitoring requirements, a denial of approval to connect may be issued.

6.9. Denial of Approval to Connect. The AF Enterprise AO may issue a denial of approval to connect for any IT (connected to the AFIN or other AF enclave) at any time, if the Enterprise AO determines the risk to the receiving enclave is too high. The PM or information system owner is notified immediately of the denial of approval to connect.

6.9.1. If the system is already connected, the connection must be terminated when the denial of approval to connect is signed. (**T-3**)

6.9.2. All denial decisions must be signed by the hosting enclave AO, and cannot be delegated further. (**T-2**)

Chapter 7

SECURITY CONTROL OVERLAYS

7.1. Overview. Overlays provide communities of interest an opportunity for consistent tailoring of security controls based on risk specific to a type of information, system, or environment. They include characteristics and assumptions about the overlay topic, security control and control enhancement specifications, risk-based rationale for control specifications (tied back to the characteristics/assumptions) supplemental guidance, and tailoring guidance designed to refine the control selection and tailoring process.

7.2. Policy. The DoD may vet all AF overlays for consideration as a DoD or CNSS overlay. The responsible authorizing official for the type of information, system, or environment that is the subject of the overlay and who are principally impacted by the use of a proposed overlay will (with the support and concurrence of all affected parties) generate and approve overlays. The AF CISO will approve overlays that have AF-wide impact.

7.3. Development and Approval Process. The overlay development team should coordinate with SAF/CNZR, Cybersecurity Risk Management, throughout the development process.

7.3.1. Send topic to AF Cybersecurity Technical Action Group (TAG) Chairs. (OPR: Overlay Proposer) All potential topics for overlays are submitted to the AF Cybersecurity TAG Chairs for validation. Topics should be sent to **usaf.pentagon.saf-cio-a6.mbx.a6zr-workflow@mail.mil**. The topics should include the following information: Name of proposed overlay; use case for overlay application; summary of the unique characteristics that drive the need to tailor controls; applicable laws, regulations, or directives governing the application of the overlay; and point of contact information.

7.3.2. Validate Topic. (OPR: AF Cybersecurity TAG) The TAG Chairs will provide the proposed overlay information to TAG members for an electronic vote. The TAG will consider whether the proposed overlay is relevant to AF IT, as well as ensure there are no conflicts with overlays in development, approved, or disapproved previously. Adjustments to the topic may be made in coordination with the overlay proposer.

7.3.3. Support Overlay Development. (OPR: overlay proposer/ overlay development team; OCR: SAF/CN, Cybersecurity) The overlay proposer is responsible for identifying an overlay development team to build the overlay and supporting documentation. SAF/CNZR, Cybersecurity Division, can assist with the policy requirements for the overlay.

7.3.4. Develop Overlay. (OPR: Overlay Proposer, Overlay Development Team, OCR: ISSM, AF CISO) Use the template provided in CNSSI No. 1253, Appendix F, attachment 2, to develop the overlay. In addition to the specified controls, the Overlay Development Team must include any adjustments to implementation guidance, assessment procedures, and specific assignment values for the selected controls. (**T-3**)

7.3.5. The tailoring guidance must clearly state any limitations or restrictions to guide application of the overlay. All security control specifications must be justified based on the risk specific to the type of information, system, or environment that is the topic of the overlay, and that risk must trace back to a characteristic and/or assumption clearly stated in the front matter of the overlay. (**T-3**)

7.4. Review and Coordinate Finalized Overlay.

7.4.1. OPR: SAF/CNZR, Cybersecurity Division. When the Overlay Development Team has completed required actions, the overlay and overlay approval memorandum is provided to SAF/CNZR for review and posting, as applicable (mission system use, AF or other use, and dissemination). SAF/CNZR will review the selected controls, implementation guidance, assessment procedures, specific assignment values, and tailoring guidance for compliance with the CNSSI No. 1253 format. If there are discrepancies in the overlay, the submitting organization must address those prior to gaining final approval. (**T-3**)

7.4.2. OPR: Overlay proposer. Overlays are developed to address risks specific to the type of information, system, or environment; therefore, as the risk changes so should the overlay. Ensure review and modification of the overlay are captured in the security plan and other applicable documentation.

7.5. Coordinate with Defense Information Systems Agency to Implement Overlay in eMASS. (OPR: SAF/CN, Cybersecurity) SAF/CNZR, Cybersecurity Division, will coordinate with the Defense Information Systems Agency to implement the approved overlay on the NIPRNet and or SIPRNet instances of eMASS. Restrictions on use approved by the Mission Area Owner will be communicated to Defense Information Systems Agency. (**T-1**)

Chapter 8

TRANSFER OF IT BETWEEN AUTHORIZING OFFICIALS

8.1. Overview. SAF/CN must ensure that Every IT system is properly aligned to an AO. (**T-1**) The overall objective is to ensure the transition process is standard and consistent. The transition process is defined as the transfer of IT to include documentation from one AO to another AO. It is a collaborative process executed by the owning AO and coordinated with the receiving AO. *The Request Transfer of Information Technology to Another Authorizing Official* Form (available on the AF RMF Knowledge Service) will be used to facilitate an orderly and timely transfer of IT. Transferring IT, projected transfer dates, and system transfer preconditions will be coordinated with the applicable AOs and their staffs. The AOs will ensure process accountability and situational/stakeholder awareness throughout this process. (**T-3**)

8.2. Transition Process. The transition process steps are as follows:

8.2.1. The owning AO staff, in coordination with the PM or ISO, if no PM is assigned, identifies the IT to transfer from an owning AO to the receiving AO.

8.2.2. As the AO staff identifies IT for transfer, it is important to include the MAJCOM portfolio manager (PfM) (See **Terms**) of the IT in this identification process, as the PfM has an integral role in all IT transfer actions.

8.2.3. The owning AO reviews and approves the proposed IT to transfer to the receiving AO.

8.2.4. The PM or ISO of the IT completes the *Request Transfer of Information Technology to Another Authorizing Official* Form for each IT.

8.2.5. The owning AO staff, in coordination with the PM/ISO and PfM, contacts the receiving AO staff/PM to discuss the proposed IT transfer.

8.2.6. The receiving AO staff completes the Assessment/Notes section of *Request Transfer of Information Technology to Another Authorizing Official* Form.

8.2.7. The owning AO and receiving AO agree to the transfer (skip to paragraph 8.2.9).

8.2.8. If the receiving AO disagrees with the transfer, the owning AO staff will request assistance from the AFRMC by sending the *Request Transfer of Information Technology to Another Authorizing Official* Form to SAF/CNZR workflow at **usaf.pentagon.saf-cio-a6.mbx.a6zr-workflow@mail.mil**. The AFRMC will adjudicate the inclusion/transfer of the IT and provide a recommendation to the CISO as the final decision authority.

8.2.9. Once both AOs agree to the IT transfer, the owning AO and receiving AO sign the *Request Transfer AO to AO* Form.

8.2.10. The PM/ISO, in coordination with the PfM, will make required changes in ITIPS and eMASS.

8.3. IT With No AO Assigned. Systems not currently under any AO's authority, not fitting into an authorization boundary, or not accepted by the gaining AO are addressed by the AFRMC. If the ITCSC identifies the IT should be assigned in the "other" AO Authorization Boundary, then SAF/CNZR, Cybersecurity Division, retains the IT until the new AO Authorization Boundary is created and an AO is assigned. If an existing boundary is determined, the submitted ITCSC is returned to the PM/ISO for staffing to and approval by the determined AO.

Chapter 9

FINANCIAL IMPROVEMENT AND AUDIT READINESS (FIAR) INFORMATION TECHNOLOGY (IT)

9.1. Overview. This Financial Improvement and Audit Readiness (FIAR) Information Technology (IT) attachment applies to individuals at all levels who manage FIAR IT resources including the Air Force Reserve and Air National Guard except where noted otherwise. Audit ready IT resources are defined by SAF/FM and are generally described as systems which have some level of impact on the Air Force Financial Statements. This attachment provides guidance specific to FIAR/ Federal Information System Controls Audit Manual RMF implementation and should be used in concert with higher level Air Force and DoD policies and procedures.

9.2. Definition. Financial Improvement and Audit Readiness (FIAR) systems are defined as core financial systems, mixed-systems, non-financial systems, and micro-applications that support key financial processes (i.e., general ledger management, funds management, payment management, receivable management, and cost management). These include systems that are relevant to financial statement disclosures, and that must operate reliably to protect the integrity of financial statement assertions. The list below describes characteristics that place a system in-scope for FIAR:

9.2.1. Security controls within the system are identified as key controls in the internal controls assessment;

9.2.2. Systems are used to generate or store original key supporting documentation;

9.2.3. Reports generated by the system are utilized in the execution of key controls; or

9.2.4. Systems are relied upon to perform material calculations (i.e., to compute payroll).

9.3. Responsibilities. The following assignments of responsibility are additions to the responsibilities outlined in **Chapter 3**, rather than substitutions.

9.3.1. SAF/FM FIAR Validator. The SAF/FM FIAR Validator will define and oversee Financial Management (FM) Validator activities.

9.3.2. Authorizing Official (AO). AOs assigned to AF FIAR information systems will assess and determine the level of overall system cybersecurity risk before authorizing such systems to process, store, display, or transmit financial or financially-related information. AOs will coordinate with the SAF/FM FIAR Validator for deficiencies associated with key FIAR controls.

9.4. FM Security control Implementation Guidance.

9.4.1. RMF security control baselines align closely with the controls that are intended to protect the integrity of financial information and processes as noted in the Government Accountability Office (GAO), GAO-09-232G**,** *Federal Information System Controls Audit Manual*. Successfully executing the RMF and implementing related controls is tantamount to satisfying most FM IT General Controls.

9.4.2. Secretary of the Air Force/Financial Management (SAF/FM) developed and manages FM supplemental guidance to augment and extend the RMF controls baseline. This control guidance is intended to be used in conjunction with the RMF process with the goal being to manage cybersecurity and Federal Information System Controls Audit Manual risk simultaneously. FM controls implementation guidance is found on: **https://cs2.eis.af.mil/sites/12802/FIAR%20IT%20Public/FM%20Control%20Implementation%20Guidance.xlsx**

WILLIAM E. MARION, II, SES
Deputy Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 40 United States Code Section 3554

HAF MD1-26, *Chief, Information Dominance and Chief Information Officer,* 5 February, 2015

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

AFI 17-130, *Air Force Cybersecurity Program Management*, 31 August 2015

AFI 17-203, *Cyber Incident Handling*, 16 March 2017

AFI 33-332, *The Air Force Privacy and Civil Liberties Program,* 12 January 2015

AFI 33-360, *Publications and Forms Management,* 1 December 2015

AFI 17-140, *Architecting*, 29 June 2018

AFI 63-101_20-101, *Integrated Life Cycle Management*, 9 May 2017

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 10 February 2017

AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*, 20 March 2015

AFMAN 33-363, *Management of Records*, 1 March 2008

AFMAN 17-1402, *Air Force Clinger-Cohen Act* (*CCA*) *Compliance Guide*, 20 June 2018

AFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016

AFPD 16-14, *Security Enterprise Governance*, 24 July 2014

AFPD 33-3, *Information Management*, 8 September 2011

CJCSI 6510.01F, *Information Assurance* (IA) *and Support to Computer Network Defense* (CND), 9 February 2011

CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems,* 27 March 2014

CNSSI No. 4009, *Committee on National Security Systems* (CNSS) *Glossary,* 6 April 2015

CNSSI No. 4016, *National Information Assurance Training Standard for Risk Analysts,* November 2005.

Committee on National Security Systems Policy No. 11, *National Policy Governing the Acquisition of Information Assurance* (IA) *and IA-Enabled Information Technology Products*, 10 June 2013

DoD *Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework* (RMF) *into the System Acquisition Lifecycle* v1.1, September 2015

DoDI 5000.02, *Operation of the Defense Acquisition System*, 7 January 2015

DoDI 8500.01, *Cybersecurity*, 14 March 2014

DoDI 8510.01, *Risk Management Framework* (RMF) *for DoD Information Technology* (IT), 12 March 2014

DoDI 8551.01, *Ports, Protocols, and Services Management* (PPSM), 28 May 2014

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

U.S. Code, Title 44 United States Code Subchapter II

Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules,* 25 May 2001

GAO-09-232G, *Federal Information System Controls Audit Manual* (FISCAM), February 2009

NIST SP 800-30, *Guide for Conducting Risk Assessments,* 17 September 2012

NIST SP 800-37r2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, 20 December 2018

NIST SP 800-53Ar4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, 18 Dec 2014.

NIST SP 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 22 January 2015

NIST SP 800-60, *Volume 1*: *Guide for Mapping Types of Information and Information Systems to Security Categories*, 1 August 2008

NIST SP 800-60, Volume 2: *Guide for Mapping Types of Information and Information Systems to Security Categories*: *Appendices*, 1 August 2008

NIST SP 800-137, *Information Security Continuous Monitoring* (ISCM) *for Federal Information Systems and Organizations*, 30 September 2011

NIST SP 800-160v1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* 21 March 2018

The DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) *into the System Acquisition Lifecycle,* 26 May 2015

Air Force Information Assurance Platform Information Technology (PIT) *Guidebook*, 13 December 2013

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

DD Form 2930, *Privacy Impact Assessment* (PIA), *Request Transfer of Information Technology to Another Authorizing Official* Form

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFIN—Air Force Information Networks

AFMAN—Air Force Manual

AFNET—Air Force Network - The AF's underlying Non-Secure Internet Protocol Router Network (NIPRNet)

AFNET-S—Air Force Network – SECRET - The Air Force's underlying Secure Internet Protocol Router Network (SIPRNet)

AFRMC—Air Force Risk Management Council

AO—Authorizing Official

CIO—Chief Information Officer

CISO—Chief Information Security Officer

CNSSP—Committee on National Security Systems Policy

DoD—Department of Defense

DoDI—Department of Defense Instruction

eMASS—Enterprise Mission Assurance Support Service

HAF—Headquarters Air Force

IAW—In Accordance With

IS—Information System

ISCM—Information Security Continuous Monitoring

ISSM—Information System Security Manager

ISO—Information System Owner

ISSO—Information System Security Officer

IT—Information Technology

ITCSC—IT Categorization and Selection Checklist

ITIPS—Information Technology Investment Portfolio Suite

MAJCOM—Major Command

NIPRNet—Non-Secure Internet Protocol Router Network

NIST-SP—National Institute of Standards and Technology – Special Publication

OPR—Office of Primary Responsibility

PIT—Platform Information Technology

PM—Program Manager

POA&M—Plan of Actions and Milestones

RMF—Risk Management Framework

SAF—Secretary of the Air Force

SCA—Security Control Assessor

SIPRNet—Secret Internet Protocol Router Network

TAG—Technical Advisory Group

US—United States

Terms

Agent of the Security Control Assessor—The licensed person or organization that acts as an independent trusted agent of the SCA, providing fact-based security analysis.

Approval to Connect—The official management decision given by a senior organizational official to authorize connection of an information system to an enclave and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Authorization to Operate (ATO)—The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Boundary—Physical or logical perimeter of a system.

Chief Information Security Officer (CISO)—Official responsible for carrying out the chief information officer responsibilities under the Federal Information Security Modernization Act and serving as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers. **NOTE**: Also known as senior information security officer (SISO) or senior agency information security officer (SAISO).

Common Control—A security control that is inherited by one or more information systems.

Common Control Provider—An organization or official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).

eMASS Account Manager/ Organizational System Administrator—The eMASS Account Manager role is Synonymous with the "Organizational System Administrator" identified in the eMASS user guide at url: **https://airforce.emass.apps.mil/Content/Help/eMASS_User_Guide.pdf**. The eMASS Organizational System Administrator is the main point of contact for users within an organization's eMASS instance and provides the first tier of support for user requests, questions, and or issues. eMASS Organizational System Administrators are appointed by the AO, SCA, or MAJCOM with role and permissions consistent with the eMASS user guide. A current listing of eMASS account managers can be found in the AF RMF KS.

Enterprise—An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. **Guest System**—A special case, limited registration of a system that is authorized by a non-AF Authorizing Official, or is owned by a non-Air Force organization but is hosted within the AFIN and must complete the process to acquire an approval to connect (ATC) from the AF Enterprise AO. A Guest System is a type of external information system (see CNSSI No. 4009).

High and Very High Risk Determination—IT risk, including High and Very High risk determination, is continually assessed by the Air Force Chief Information Security Officer through evaluation of Likelihood and Impact findings and in concert with CNSSI No.1253; NIST SP 800-30; and NIST SP 80053r4, Appendix D.

Impact—The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.

Likelihood—A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

MAJCOM Portfolio Manager (PfM)—Serves as the advisor to a Program Manager and/or Project manager (if established) IAW AFI 17-110.

Mission Area Owner—The Mission Area Owner role is consistent with the PAO role described in DoDI 8510.01 in that an owner is identified/ appointed and responsible for security/ cybersecurity issues for each of the DoD Mission Area's. IAW AFPD 16-14, EIEMA (CIO); BMA (MG); DIMA (A2); WMA (AF A3/5).

Platform Information Technology (PIT)—Information technology (IT), both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

PIT Product—Individual hardware or software components, including, but not limited to, operating systems, commercial or government software, or individual hardware that support specific mission functionality. IT Products, when purposed for PIT, become PIT Products.

PIT Subsystem—A collection of PIT that does not rise to the level of a PIT system.

PIT System—A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Risk Management Framework (RMF)—The Risk Management Framework is a structured approach used to oversee and manage risk for an enterprise.