BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 17-101

2 FEBRUARY 2017

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/CIO A6ZC

Certified by: SAF/CIO A6Z
(Peter E. Kim, AF CISO)

Supersedes: AFI33-210, 23 December 2008

Pages: 49

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*, 12 April 2016, AFPD 33-3, *Information Management*, 8 September, 2011, DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2014, and associated processes outlined on the AF RMF Knowledge Service (KS), for managing the life-cycle cybersecurity risk to Air Force Information Technology (IT) consistent with the Federal Information Security Modernization Act (FISMA) of 2014, DoDI 8500.01, *Cybersecurity*, 14 March 2014, and DoD Directive 8000.01, *Management of the Department of Defense Information Enterprise*, 10 February 2009. This instruction is consistent with Chairman Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*. Direct questions, comments, recommended changes, or conflicts to this publication through command channels using the AF Form 847, *Recommendation for Change of Publication*, to SAF/CIO A6.

This publication applies to all military and civilian AF personnel, members of the AF Reserve Command (AFRC), Air National Guard (ANG), third-party governmental employee and contractor support personnel in accordance with appropriate provisions contained in memoranda support agreements and AF contracts.

The authorities to waive requirements in this publication are identified with a Tier number (T-0, T-1, T-2, T-3) following the compliance statement. See 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. Send any supplements to this publication to SAF/CIO A6 for review, coordination, and approval prior to publication. Unless otherwise noted, the SAF/CIO A6 is the waiver authority to policies contained in this publication. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) AFMAN 33-363, *Management of Records*, and disposed of IAW Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS).

SUMMARY OF CHANGES

This document is substantially changed and must be reviewed in its entirety. This instruction reissues, renames, supersedes, and rescinds AFI 33-210, *Air Force Certification and Accreditation Program,* to AFI 17-101, *Risk Management Framework for Air Force Information Technology*. This directive establishes the Risk Management Framework (RMF) for AF IT, establishes associated cybersecurity policy, and assigns responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to AF IT.

Chapter 1— PROGRAM OVERVIEW **5**

1.1. Purpose..... 5

1.2. Applicability. 5

Figure 1.1. Air Force IT Categories. 6

1.3. Objectives. 6

Chapter 2— ROLES AND RESPONSIBILITIES **7**

2.1. Secretary of the Air Force, Office of Information Dominance and Chief Information Officer (SAF/CIO A6). 7

2.2. Administrative Assistant to the Secretary of the Air Force (SAF/AA). 7

2.3. Secretary of the Air Force for Acquisition (SAF/AQ)..... 7

2.4. Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (AF/A2). . 8

2.5. Chief Information Security Officer (CISO), SAF/CIO A6Z. 8

2.6. Authorizing Official (AO). 9

2.7. Air Force Enterprise Authorizing Official (AF Enterprise AO). 10

2.8. AO Designated Representative (AODR). 10

2.9. Security Control Assessor (SCA). 10

2.10. Security Controls Assessor Representative (SCAR). 11

2.11. Agent of the Security Controls Assessor (ASCA). 11
2.12. Information System Owners (ISO). 12
2.13. Program Manager (PM). 13
2.14. Unit Communications Squadron Commander (CS/CC). 14
2.15. Information System Security Manager (ISSM). 14
2.16. Information System Security Officer (ISSO). 15
2.17. Information Systems Security Engineer (ISSE). 15
2.18. Information Owner (IO)/Steward. 16
2.19. MAJCOM Cybersecurity Office or Function. 16
2.20. User Representative (UR). 16
2.21. Additional Responsibilities. 17
Table 2.1. AF RMF Appointment Matrix. 17
2.22. Cybersecurity Forums. 17
Chapter 3— RMF METHODOLOGY 19
3.1. Overview. 19
Figure 3.1. RMF for AF IT. 19
3.2. RMF Step 1, CATEGORIZE System. 19
3.3. RMF Step 2, SELECT Security Controls. 21
3.4. RMF Step 3, IMPLEMENT Security Controls. 22
3.5. RMF Step 4, ASSESS Security Controls. 22
3.6. RMF Step 5, AUTHORIZE System. 22
3.7. Denial of Authorization to Operate (DATO). 23
3.8. RMF Step 6, MONITOR Security Controls. 23
3.9. Resources and Tools. 24
Chapter 4— APPROVAL TO CONNECT (ATC) PROCESS 25
4.1. Overview. 25
4.2. Duration and Expiration. 25
4.3. Connection to the DoDIN. 25
4.4. Connection to the Air Force Information Networks (AFIN). 25

4.5. Guest System Registration. 26
4.6. ATC Process for Air Force Functional/Mission Systems. 26
4.7. Continuous Monitoring. 26
4.8. Denial of Approval to Connect (DATC). 26
Chapter 5— SECURITY CONTROL OVERLAYS **28**
5.1. Overview. 28
5.2. Policy. 28
5.3. Development and Approval Process. 28
5.4. Review and Coordinate Finalized Overlay. 29
5.5. Coordinate with DISA to Implement Overlay in eMASS. 29
Chapter 6— TRANSFER OF IT BETWEEN AUTHORIZING OFFICIALS **30**
6.1. Overview. 30
6.2. Transition Process. 30
6.3. IT With No AO Assigned. 30
Chapter 7— RMF TRANSITION **32**
7.1. Overview. 32
7.2. Transition Timeline. 32
7.3. RMF Deviation Requests. 32
Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION **33**
Attachment 2— AF IT ASSESS ONLY REQUIREMENTS **40**
Attachment 3— FINANCIAL IMPROVEMENT AND AUDIT READINESS (FIAR) IT CONTROLS GUIDANCE (OPR: AF/FM) **42**

Chapter 1

PROGRAM OVERVIEW

1.1. Purpose. This AFI provides implementation instructions for the Risk Management Framework (RMF) methodology for Air Force (AF) Information Technology (IT) according to AFPD 17-1, *Information Dominance Governance and Management*, and AFI 17-130, *Air Force Cybersecurity Program Management*, which is only one component of cybersecurity.

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

1.1.2. The RMF aligns with SAF/CIO A6's AF Information Dominance Flight Plan key concept of increasing cybersecurity of AF information systems; therefore, robust risk assessment and management is required.

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. Effective implementation and resultant residual risk associated with security controls implementation is assessed and mitigated, aligns with DoDI 8510.01, and as documented in the RMF security authorization package for AF IT.

1.1.5. Discrete classes of systems (i.e., AF financial systems) are subject to additional requirements contained in Attachment 3 to this document. Guidance contained in Attachment 3 are intended to supplement, but not replace, the policy limits articulated in this Instruction.

1.2. Applicability.

1.2.1. This publication is binding on all military, civilian and contract employees, and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force, who develop, acquire, deliver, use, operate, support, or manage AF IT. This publication applies to all networked or standalone IT used to receive, process, store, display, or transmit AF information (or Government information where the AF agreed to manage the information/infrastructure), as well as DoD partnered systems where it is agreed that DoD standards are followed. AF IT (see Figure 1.1) includes but is not limited to: information systems (IS) (major applications and enclaves), platform information technology (PIT) (PIT systems, PIT subsystems, and PIT products), IT services (Internal & External), and IT products (software, hardware, and applications).

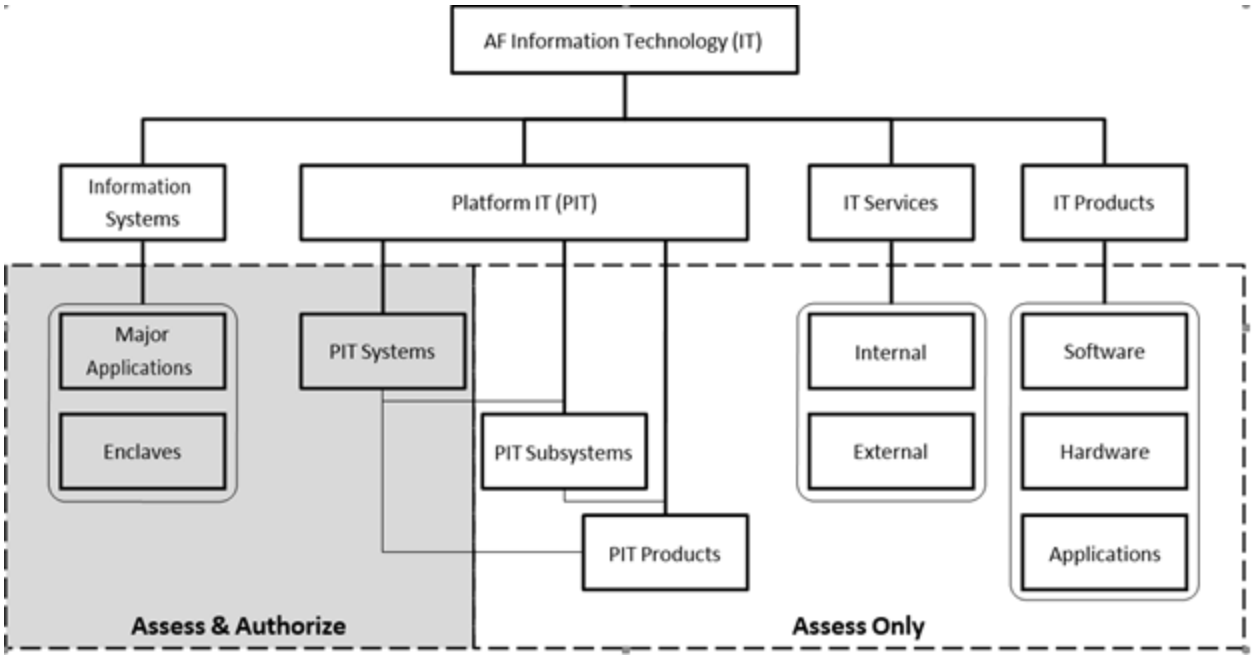
1.2.2. This AFI does not apply to the protection of Sensitive Compartmented Information (SCI) systems or intelligence, surveillance, reconnaissance mission and mission support systems or higher authoritative guidance governing Special Access Program (SAP) systems.

1.2.3. Authority for AF space systems rests with AF Space Command (AFSPC) as delegated by United States Strategic Command (USSTRATCOM). 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*.

1.2.4. For IT not centrally managed or 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 2.1) required to comply with RMF. The duties shall include the roles and responsibilities for reporting, oversight, and risk management to the AF.

Figure 1.1. Air Force IT Categories.



1.3. Objectives.

1.3.1. The RMF replaces the DIACAP and manages the life-cycle cybersecurity risk to AF IT. 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 changes the traditional focus of certification and accreditation (C&A) as a static, procedural activity to a more dynamic approach to more effectively manage mission and cybersecurity risks in diverse environments of complex, evolving, and sophisticated cyber threats and vulnerabilities.

1.3.2. The RMF ensures AF IT assets are assessed for cybersecurity risk to the AF, the discovered weaknesses are documented in a plan of action and milestones (POA&M) to mitigate residual risk, and an AO, supported by the RMF team members, identified at Table 2.1, accepts the risk to the AO's area of responsibility, IAW AFPD 16-14, *Security Enterprise Governance,* and DoDI 8510.01.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Secretary of the Air Force, Office of Information Dominance and Chief Information Officer (SAF/CIO A6). The SAF/CIO A6 will:

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

2.1.2. Maintain visibility of the cybersecurity posture for AF IT through automated tools or designated repositories in support of DoD CIO and appointed AOs. **(T-0)**

2.1.3. Provide guidance to organizations on how to implement solutions for operational requirements in support of established National, DoD, Joint Chiefs of Staff (JCS), or AF security controls for IT and remain within established risk tolerance levels. **(T-0)**

2.1.4. Appoint AOs in coordination with the appropriate Mission Area Owner (MAO).

2.1.5. Ensure an Information System Owner (ISO) is appointed for all AF IT.

2.1.6. Appoint the AF Chief Architect with responsibility for the AF Cybersecurity Architecture IAW AFI 17-140, *Air Force Architecting*.

2.1.7. Define cybersecurity performance measurements and metrics to identify enterprise-wide cybersecurity trends and status of mitigation efforts, IAW NIST SP 800-55, *Performance Measurement Guide for Information Security*. **(T-0)**

2.1.8. Be responsible for the security controls implemented across the IT enterprise.

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

2.2.1. Works with the CISO to oversee the establishment of risk tolerance and security controls for IT owned by Headquarters Air Force (HAF) organizations without a functional CIO (HAF Portfolio).

2.2.2. Provides guidance to organizations on how to implement solutions for operational requirements for the HAF Portfolio.

2.2.3. Maintains visibility of the cybersecurity posture of HAF Portfolio IT through automated assessment and authorization tools.

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

2.3.1. Acquires all AF electronic systems through organic programs within the AF, commercial-off-the-shelf (COTS) systems, or non-developmental item (NDI) programs. The PM shall pursue comprehensive integrated risk analysis throughout the life cycle of all programs and shall prepare and maintain a risk management plan.

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 solutions for operational requirements.

2.3.3. Ensures all cyber /IT security controls are translated into security requirements via systems security engineering and are written into the System Requirement Document (SRD) on all acquisitions.

2.3.4. Ensures system security engineering is accomplished through the acquisition process for all new and upgrade capability developments.

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

2.4.1. Maintains visibility of the cybersecurity posture of AF SCI and the DoD portion of the Intelligence Mission Area (DIMA) IT through automated assessment and authorization tools.

2.4.2. Oversees the establishment of risk tolerance and baseline security controls for AF SCI and DIMA IT. Consults with SAF/A6 CISO as appropriate. Provides RMF implementation guidance to AF ISR systems and network organizations.

2.5. Chief Information Security Officer (CISO), SAF/CIO A6Z. 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/CIO A6. As a CISO, the role requires individuals be a DoD official (O-7 or SES at a minimum) and a United States citizen. **(T-1)** The CISO will:

2.5.1. Complete training and maintain cybersecurity certifications IAW AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*. **(T-1)**

2.5.2. Monitor, evaluate, and provide advice to the SAF/CIO A6 regarding AF cybersecurity posture.

2.5.3. In coordination with the SAF/CIO A6 and AOs, ensure the cybersecurity risk posture, risk tolerance levels, and risk acceptance decisions for AF IT meet mission and business needs, IAW Commander, USSTRATCOM, 24 AF/CC, and AFI 10-1701, *Command and Control* (C2) *for Cyberspace Operations,* while also minimizing the operations and maintenance burden on the organization.

2.5.4. Perform as the Security Control Assessor (SCA) or appoint SCAs.

2.5.5. Provide guidance and direction on Agent of the Security Control Assessor (ASCA) establishment and licensing in support of RMF requirements. **(T-1)**

2.5.6. Oversee establishment and enforcement of the AF RMF, roles, and responsibilities; review approval thresholds and milestones within the RMF. **(T-1)**

2.5.7. Chair the Air Force Risk Management Council (AFRMC). **(T-1)**

2.5.8. Participate in Federal, Joint, DoD, and AF cybersecurity and RMF technical working groups and forums (e.g., Defense Information Assurance Security Accreditation Working Group (DSAWG)).

2.5.9. Adjudicate IT determinations, in coordination with the AFRMC, when a conflict in the IT determination process is identified. **(T-1)**

2.5.10. Appoint AF members to the DoD RMF TAG.

2.5.11. Review and approve Privacy Impact Assessments (PIAs) submitted IAW AFI 33-332, *The AF Privacy and Civil Liberties Program*. The approval of the PIA cannot be delegated. **(T-1)**

2.5.12. Approve national security system (NSS) designations for AF IT. **(T-1)**

2.5.13. Ensure AF RMF guidance is posted to the AF Component Workspace portion of the DoD Knowledge Service (KS) and is consistent with DoD policy and guidance.

2.6. Authorizing Official (AO). The AO is the official with the authority responsible for accepting a level of risk for a system balanced with mission requirements, except for IT with unmitigated "Very High" and "High" risk. 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, AOs can create a community-specific guidebook for better clarifying guidance. AOs will:

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

2.6.2. Complete training and certification requirements IAW AFMAN 17-1303. **(T-1)**

2.6.3. Be appointed by SAF/CIO A6, in coordination with the appropriate MAO. The appointment grants authority to authorize IT as defined in the AO appointment memo.

2.6.4. Advocate for cybersecurity-related positions in accordance with DoDI 8500.01, **(T-0)** AFI 17-130, and AFMAN 17-1303. **(T-1)**

2.6.5. Ensure an Information System Owner (ISO) (i.e., the owner, operator, maintainer of the IT) is appointed prior to issuing an authorization decision. **(T-1)**

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

2.6.7. Ensure verification through the AF Ports, Protocols, and Services (PPS) 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)**

2.6.8. Assist the SAF/CIO A6 in providing guidance to organizations on how to implement solutions for operational requirements exceeding the established National, DoD, JCS, or AF baseline controls for IT.

2.6.9. 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), except PIT. Any exceptions to or conditions of the authorization decision must be articulated within the Authorization Decision Document. **(T-0)**

2.6.10. Review the security assessment report (SAR), risk assessment report (RAR), and POA&M to ensure there is a clearly defined course of action, see also NIST SP 800-30, *Guide for Conducting Risk Assessments*. An AO may downgrade or revoke an authorization decision at any time, if risk conditions or concerns so warrant. **(T-0)**

2.6.11. Review and approve the security assessment plan (SAP), the security plan, and system-level information security continuous monitoring (ISCM) strategy.

2.6.12. Ensure all AF IT comply with DoD and AF connection approval processes, see **Chapter 4**.

2.6.13. Not delegate authorization decision authority (i.e., to formally accept risk for a system). **(T-0)**

NOTE: Appointment letters and AO Boundaries are located on the AF RMF KS.

2.7. 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 the Air Force Information Networks (AFIN). The Enterprise AO may delegate this authority to appropriate deputies with concurrence of the SAF/CIO A6. In addition to the AO responsibilities in paragraph 2.6 above, the Enterprise AO will:

2.7.1. Establish acceptable security controls and risk tolerance for connecting to the AFIN and provide guidance to implementing organizations to mitigate risk commensurate with established risk tolerance.

2.7.2. Review the Security Authorization Package, as a minimum, for all requests to connect to the AFIN and assess the impact to enterprise community risk. **(T-1)**

2.7.3. Render authorization decisions in the form of an authorization to operate (ATO) for AF systems not falling under another AO. Render AFIN connection decisions in the form of an ATC (see **Chapter 4**) for non-AF systems and for AF systems falling under another AO. **(T-1)**

2.7.4. The Enterprise AO or designee will expediently respond to urgent/emergency requests to connect to the AFIN.

2.7.5. See AFI 17-130, for additional information in support of this position.

2.8. AO Designated Representative (AODR). The AODR will:

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

2.8.2. The AODR may 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.

2.8.3. Perform responsibilities as assigned by the AO. The AODR may perform any and all duties of an AO except for accepting risk by issuing an authorization decision.

2.8.4. Complete AO training and maintain cybersecurity certifications consistent with duties and responsibilities of an AO and IAW AFMAN 17-1303. **(T-1)**

2.8.5. Provide recommendations to the AO to render authorization decisions based on input from the SCA, ISO, PM, and other AOs and AODRs.

2.9. Security Control Assessor (SCA). The SCA will:

2.9.1. 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.

2.9.2. Complete training and maintain appropriate cybersecurity certification IAW AFMAN 17-1303. It is highly recommended SCAs complete both the AO training module and attain the Committee on National Security Systems Instruction (CNSSI) 4016, *National Information Assurance Training Standard for Risk Analysts,* certificate for supplemental training. **(T-1)**

2.9.3. Develop the SAP and ensure its integration into the program office's Test and Evaluation Master Plan (TEMP) IAW DoDI 5000.02, *Operation of the Defense Acquisition System*. **(T-0)**

2.9.4. Prepare the SAR documenting the issues, findings, and recommendations from the security control assessment, and reassess remediated controls, as required. **(T-0)**

2.9.5. Periodically assess security controls employed within and inherited by the IT IAW the Information Security Continuous Monitoring strategy. **(T-0)**

2.10. Security Controls Assessor Representative (SCAR). This position may be an organic or contracted resource. The SCAR works with the PM, ISSM, ISSO, and RMF team to assess security controls for the SCA. The SCAR will:

2.10.1. Complete training and maintain appropriate cybersecurity certification IAW AFMAN 17-1303. It is recommended SCARs also complete the AO training module and attain the CNSSI No. 4016 certificate for supplemental training. **(T-1)**

2.10.2. Serve as an active member of the RMF team from its inception, to assist with planning of cybersecurity requirements. The SCAR ensures security controls are implemented IAW the security plan and are assessed IAW the SAP. **(T-0)**

2.10.3. Validate assessment results from others' (e.g., ASCA or ISSM) hands-on, comprehensive evaluations of the technical and non-technical security controls for the IT, determine the degree to which the IT satisfies the applicable security controls.

2.10.4. Should the SCAR be a contractor, the SCAR is not permitted to make decisions on behalf of the government but can only provide advice and guidance.

2.11. Agent of the Security Controls Assessor (ASCA). The ASCA is a licensed 3rd-party agent assisting in assessment activities and provides an independent report for the SCA. This position cannot make decisions on behalf of the government but can only provide advice and guidance. The ASCA will:

2.11.1. Achieve and maintain an ASCA license per the *AF and Space ASCA Licensing Guide*. **(T-0)**

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

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

2.11.4. Perform assessment procedures for each applicable security control as outlined in the DoD RMF KS. **(T-0)**

2.11.5. 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.

2.11.6. The ASCA 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 does not provide direction or oversight to organizations or contractors in support of ASCA responsibilities.

2.11.7. All ASCA agreements must include safeguards to prevent a conflict of interests with the development team.

2.12. Information System Owners (ISO). Official responsible for the overall procurement, development, integration, modification, and operation and maintenance of AF IT. **(T-1)** An ISO is appointed and performs all PM roles and responsibilities when a PM is not assigned. For AF-wide systems (e.g., AFNET and LOGMOD), the ISO is appointed by the HAF/SAF 3-letter responsible for the capability. For MAJCOM-level or base-level IT, to include base enclaves, and PIT, the appropriate MAJCOM 2-letter appoints the ISO. **(T-1)** No further appointment is required. This ISO role is not the same as the TEMPEST ISO. The ISO will:

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

2.12.2. Ensure, with coordination of the PM staff, the development, maintenance, and tracking of the security plan for assigned IT. **(T-1)**

2.12.3. Ensure, with coordination of the PM staff, the development of an ISCM strategy to monitor the effectiveness of all security controls employed within or inherited by the system, and to monitor any proposed or actual changes to the system and its environment of operation. **(T-0)**

2.12.4. Report the security status of the IT including the effectiveness of security controls employed within and inherited by the system to the AO and other appropriate organizational officials on an ongoing basis in accordance with the ISCM strategy.

2.12.5. Decide, in coordination with the Information Owner (IO)/Steward, who has access to the system (and what types of privileges or access rights) and ensure system users and support personnel receive the requisite security training. **(T-2)**

2.12.6. Inform, based on guidance from the SCA and AO, appropriate organizational officials to conduct the Authorize and Assess process or the Assess Only process; ensure the necessary resources are available for the effort, and provide the required IT access, information, and documentation to the SCA.

2.12.7. Conduct the initial remediation actions on security controls based on the findings and recommendations of the SAR and work with the SCA to reassess remediated controls.

2.12.8. Ensure the POA&M is developed for all identified weaknesses and the appropriate steps to mitigate those weaknesses are identified. Take appropriate steps to reduce or eliminate weaknesses, then generate the security authorization package and submit the package to the SCA for assessment. **(T-0)**

2.12.9. Ensure open POA&M items are updated and closed in a timely manner. **(T-2)**

2.12.10. Ensure consolidated RMF documentation is maintained for systems with instances at multiple locations.

2.12.11. Thoroughly review the 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).

2.12.12. 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-0)**

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

2.13.1. 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 AFI 63-101, *Integrated Life Cycle Management*, and DoDI 8510.01, the *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*. **(T-0)**

2.13.2. Ensure the Program Management Office (PMO) is resourced to support information system security engineering (ISSE) 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-1)**

2.13.3. Ensure cybersecurity-related positions are assigned in accordance with Table 2.1 and AFMAN 17-1303. **(T-1)**

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

2.13.5. Ensure the IT is registered IAW AFI 17-110, *Air Force Information Technology Portfolio Management and Investment Review*. **(T-1)**

2.13.6. Develop and maintain a cybersecurity strategy for IT IAW AFMAN 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, and AFI 63-101/20-101. **(T-1)**

2.13.7. Ensure applicable Cyber Tasking Orders (CTO) are received and acted upon per the CTO directions. **(T-1)**

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

2.13.9. Ensure operational systems maintain a current ATO and recommend to the AO that systems without a current authorization are identified for removal from operation. **(T-1)**

2.13.10. Ensure 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.

2.13.11. Track and implement the corrective actions identified in the POA&M, in order to provide visibility and status to the ISO, IO, AO, and CISO. **(T-0)**

2.13.12. Report security incidents to stakeholder organizations and the SCA. Conduct root cause analysis for incidents and develop corrective action plans as input to the POA&M.

2.13.13. Ensure a PIA is completed (DD Form 2930) for IT that process and/or store Personal Identifiable Information (PII)/Personal Health Information (PHI) IAW AFI 33-332, *Air Force Privacy and Civil Liberties Program*. **(T-1)**

2.14. 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.

2.15. 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 will:

2.15.1. Ensure the integration of cybersecurity into and throughout the lifecycle of the IT on behalf of the AO. **(T-0)**

2.15.2. Complete and maintain required cybersecurity certification IAW AFMAN 17-1303. Individuals in this position must be U.S. citizens. **(T-0)**

2.15.3. Ensure all AF IT cybersecurity-related documentation is current and accessible to properly authorized individuals. **(T-1)**

2.15.4. Support the PM or ISO in maintaining connection (ATC) and authorization (ATO) approvals and provide support to the PM or ISO in implementing corrective actions identified in the POA&M.

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

2.15.6. Continuously monitor 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 such as security incidents, feedback from external inspection agencies, exercises, and operational evaluations. **(T-0)**

2.15.7. Ensure cybersecurity-related events or configuration changes that impact AF IT authorization or adversely impact the security posture are formally reported to the AO and other affected parties, such as IOs and stewards and AOs of interconnected IT.

2.15.8. Appoint Information System Security Officers (ISSOs) and provide 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-0)**

2.15.9. Ensure 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)**

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

2.16. Information System Security Officer (ISSO). The ISSO is responsible for ensuring the appropriate operational security posture is maintained for 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. ISSOs (formerly system-level IA Officers) will:

2.16.1. Implement and enforce all AF cybersecurity policies, procedures, and countermeasures. **(T-1)**

2.16.2. Complete and maintain required cybersecurity certification IAW AFMAN 17-1303. Individuals in this position must be U.S. citizens. **(T-0)**

2.16.3. Ensure all users have the requisite security clearances and need-to-know, complete annual cybersecurity training, and are aware of their responsibilities before being granted access to the IT according to AFMAN 17-1301. **(T-1)**

2.16.4. Maintain all authorized user access control documentation IAW the applicable AF Records Information Management System (AFRIMS). **(T-1)**

2.16.5. Ensure software, hardware, and firmware complies with appropriate security configuration guidelines (e.g., Security Technical Implementation Guides (STIGs)/Security Requirement Guides (SRG)). **(T-1)**

2.16.6. Ensure proper configuration management procedures are followed prior to implementation and contingent upon necessary approval. Coordinate changes or modifications with the system-level ISSM, SCA, and/or the Wing Cybersecurity office. **(T-1)**

2.16.7. Initiate protective or corrective measures, in coordination with the security manager, when a security incident or vulnerability is discovered. **(T-3)**

2.16.8. Report security incidents or vulnerabilities to the system-level ISSM and wing cybersecurity office according to AFI 17-130. **(T-2)**

2.16.9. Initiate exceptions, deviations, or waivers to cybersecurity requirements. **(T-1)**

2.17. Information Systems Security Engineer (ISSE). The ISSE is an individual, group, or organization responsible for conducting information system security engineering activities. ISSE captures and refines information security requirements and ensures the requirements are effectively integrated into IT products and information systems through purposeful security architecting, design, development, and configuration. Reference DoDI 5000.02, and NIST SP 800-160, *Systems Security Engineering - A Multidisciplinary Approach to Building Trustworthy Resilient Systems*, for additional details on systems engineering and information systems engineering processes. The ISSE traces security controls (which are high-level cybersecurity capability needs), with the RMF team, to the actual system security requirements documented in the acquisition process (i.e., many security requirements are derived from security controls). The ISSE will:

2.17.1. Employ best practices when implementing security controls, including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques.

2.17.2. Coordinate their security-related activities with the information security architect, ISSO, ISO, and common control provider.

2.17.3. Complete training and maintain certification IAW AFI 17-1303**.** Personnel performing any IA Workforce System Architecture and Engineering (IASAE) specialty function(s) (one or more functions) at any level must be certified to the highest level function(s) performed. **(T-0)**

2.18. Information Owner (IO)/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. The IO/Steward will:

2.18.1. Provide input to the ISO regarding security requirements and security controls for the IT where the information is processed, stored, or transmitted. **(T-2)**

2.18.2. Establish the rules for appropriate use and protection of the information, during generation, collection, processing, dissemination, and disposal and retain that responsibility even when the information is shared with or provided to other organizations. **(T-1)**

2.18.3. Provide input to ISOs on the security controls selection (e.g., during system categorization and security controls tailoring) and on the derived security requirements for the systems where the information is processed, stored, or transmitted (A single IS, PIT system, or PIT subsystem may contain information from multiple IO/stewards.) **(T-1)**

2.19. MAJCOM Cybersecurity Office or Function. The MAJCOM Cybersecurity Office or Function will:

2.19.1. Develop, implement, oversee, and maintain a MAJCOM cybersecurity program that adheres to cybersecurity architecture, requirements, objectives, policies, processes, and procedures.

2.19.2. Tracks and reports Federal Information Security Modernization Act of 2014 (FISMA) metrics to SAF/CIO A6 Cybersecurity on a monthly, quarterly, and annual basis as required via Enterprise Information Technology Data Repository / Information Technology Investment Portfolio System (EITDR/ITIPS) or DoD Cyberscope (DCS).

2.20. User Representative (UR). 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 UR 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.

2.21. Additional Responsibilities. Additional responsibilities and authorities relevant to many of the roles listed above are contained in the attachments.

Table 2.1. AF RMF Appointment Matrix.

Role	Appointed/ Identified By	Rank Minimum	Reference(s)
SAF/CIO A6+	SecAF (established)	O-9	HAF MD1-26
CISO	SAF-CIO A6	O-7 / SES	DoDI 8500.01
MAO	Identified	O-7 / SES	AFPD 16-14
AO*+	SAF-CIO A6	O-7 / SES	AFI 17-130
AODR	AO	O-5 / GS-14	AFI 17-130
SCA*+	CISO	O-4 / GS-13	AFI 17-130
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	AFI 17-101
IO/Steward	Identified by the ISSM	Any	DoDI 8500.01, NIST SP 800-37r1
ISSE+	PM	Any	DoDI 8510.01
ISSM*+	PM or ISO	Any	DoDI 8510.01
ISSO+	ISSM	Any	AFI 17-130
UR	ISO	Any	DoDI 8510.01

*** Denotes minimum system-level RMF positions**

+ Denotes additional responsibilities and authorities assigned in Attachments

2.22. Cybersecurity Forums. The AF leverages existing DoD and AF governance bodies (e.g., Air Force Security Enterprise Executive Board (AFSEEB), Information Technology Governance Executive Board (ITGEB)) to discuss cybersecurity risk topics and make organizational and mission area risk decisions. This Instruction does not define the scope or responsibilities of these existing bodies. The following forums provide focused management and oversight of the AF Cybersecurity Program.

2.22.1. AF Cybersecurity Technical Advisory Group (AFCTAG**).** The AFCTAG provides technical cybersecurity subject matter experts (SMEs) from across the MAJCOMs and functional communities to facilitate the management, oversight, and execution of the AF

Cybersecurity Program. The AFCTAG examines cybersecurity-related issues common across AF entities and provides recommendations to the CISO and DSAWG on changes to the minimally required security controls (for AFIN connection) or configurations.

2.22.2. Air Force Risk Management Council (AFRMC**).** The 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 AFRMC advises and makes recommendations to existing governance bodies. Finally, the AFRMC recommends assignment of IT to the appropriate AO for systems that fall outside of all defined authorization boundaries.

2.22.3. 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/CIO A6 and AOs an opportunity to discuss issues relevant to the RMF, AO Boundaries, IT, AOs, and SCAs.

2.22.4. For additional information on these forums, please see the SAF/CIO A6Z Cybersecurity Division site, AFI 17-130, applicable charters, and process guides.

Chapter 3

RMF METHODOLOGY

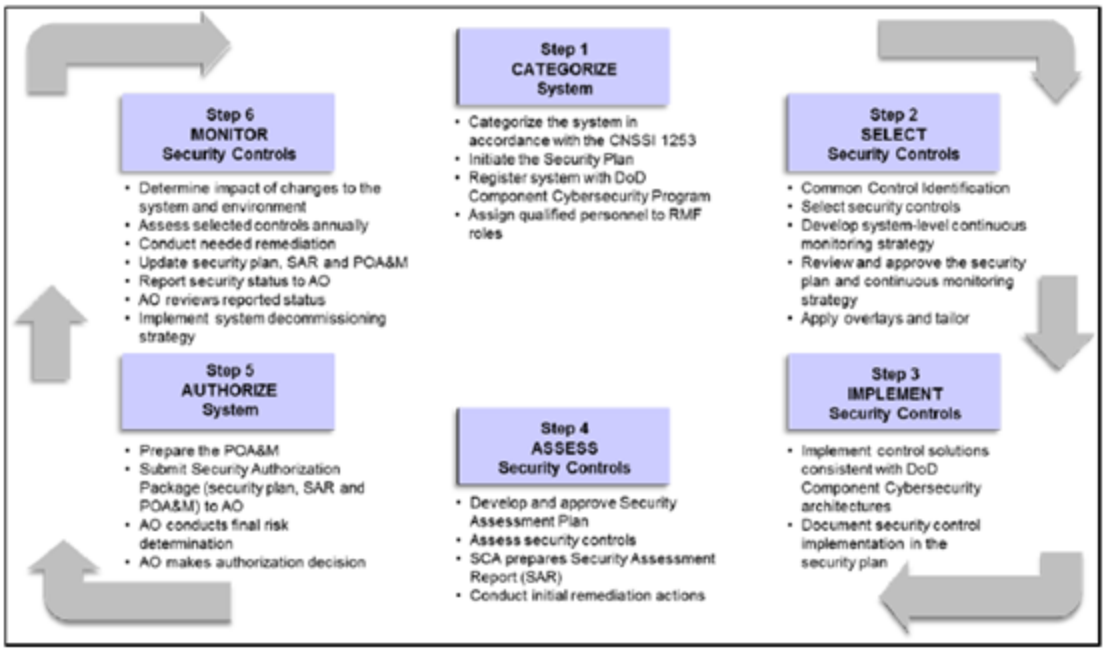
3.1. Overview.

3.1.1. The 6-Step RMF process at RMF Tier 3 (system level) is based on the process outlined in NIST SP 800-37r1 and DoDI 8510.01 and is illustrated in Figure 3.1. Where possible, this Instruction also identifies steps required for the "Assess Only" 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).

3.1.2. The DoD RMF KS is the authoritative source for RMF implementation, planning, and execution.

3.1.3. 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. Specific implementation guidance is available on the DoD RMF KS. Additionally, supplementary guidance concerning the execution of RMF steps for discrete classes of AF systems (e.g., financial systems) is contained in the Attachments.

Figure 3.1. RMF for AF IT.



3.2. RMF Step 1, CATEGORIZE System. References DoDI 8510.01, CNSSI No.1253, NIST SP 800-53r4, NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, and the DoD RMF KS.

3.2.1. Begin this step by completing the RMF IT Categorization and Selection Checklist and DD Form 2930, Privacy Impact Assessment. During categorization, the impact to confidentiality, integrity, and accessibility is categorized into one of three designations (low, moderate, or high) to address the impact of a loss. 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 IT Categorization Checklist and submit the completed document to the AFRMC for disposition; send to SAF/CIO A6ZC Cybersecurity Division, **usaf.pentagon.saf-cio-a6.mbx.a6sc-workflow@mail.mil**. SAF/CIO A6ZC retains the IT categorized as "other" until the new AO Authorization Boundary is created or an AO is assigned. If an existing boundary is determined, the Checklist is returned to the PM/ISO for staffing to and approval by the determined AOs.

3.2.2. Each AF IT, IAW AFI 17-110, must be registered in EITDR, 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 (NC3), Joint) to be registered in another repository. **(T-1)** EITDR/ITIPS will systematically assign a temporary registration number for each registered IT until the next scheduled replication with DoD Information Technology Portfolio Repository (DITPR). A DITPR number will then be systematically assigned and included in EITDR/ITIPS as the permanent official IT registration number for all registered AF IT.

NOTE: The EITDR system is transitioning to ITIPS by the end of 2nd quarter of 2017. When this system, or any future tracking system, is implemented, the EITDR registration requirements still apply in the current tracking system. All instances within this Instruction that reference EITDR is equivalent to ITIPS; consider these names interchangeable.

3.2.3. PMs or ISOs deploying systems across DoD/AF Components will register the system and post the categorization checklist to Enterprise Mission Assurance Support Service (eMASS).

3.2.4. For programs where the sensitivity of information may present a cybersecurity concern, the program (e.g., Aircraft, C2, and Weapons Systems) is required to upload only the following information/documentation into eMASS: PM and System Information eMASS fields, IT Categorization and Selection Checklist document, Cybersecurity Strategy document, Authorization Decision Memo document, and a Statement in the POA&M comments section (eMASS field) indicating the number of POA&M entries for the system. All documentation will be regularly reviewed to ensure accuracy and completeness, which may be audited by SAF/CIO A6ZC, Cybersecurity, the AO, or the SCA at any time.

3.2.5. Register all IT in the appropriate eMASS instance: NIPRNet eMASS or SIPRNet eMASS. Both instances have the same capabilities. Please note, SIPRNet eMASS is not certified to store TOP SECRET, SCI, or SAP/SAR artifacts or implementation details. NIPRNet eMASS is not certified to store SECRET artifacts or implementation details. The assigned SCA protects artifacts with special handling requirements. In those cases, the implementation plan or test results should simply state a 0 level (Compliant or Non-Compliant) and a reference to where the associated artifacts can be located.

3.2.6. The organization's eMASS Account Manager 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 SAF/CIO A6ZC Cybersecurity eMASS site.

3.3. RMF Step 2, SELECT Security Controls. References DoDI 8510.01, CNSSI No.1253, NIST SP 800-30, NIST SP 800-53r4, and the DoD's RMF KS.

3.3.1. The process for selection of security controls is: common control identification; security control baseline and overlay selection; tailoring (modification); ISCM strategy; and security plan and ISCM strategy review and approval.

3.3.2. Common Control Identification (available via eMASS).

3.3.2.1. DoD/AF Tier I/II Inheritance model: Common Controls (Policy).

3.3.2.2. AFSPC, the Enterprise AO and Common Control Provider, provides the Tier II Common Controls (Inheritance) available in eMASS for AF IT use.

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

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

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

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

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

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

3.3.4. Identify and apply overlays that apply to the AF IT. See **Chapter 5**.

3.3.5. 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. Also, if a selected control will not be implemented, document a risk-informed rationale (i.e., using a cost/benefit analysis) for not planning to implement the control must be documented in the security plan and POA&M.

3.3.6. Operational Technology (OT) is more sensitive to the application of cyber security measures and controls that can affect its availability. Many forms of OT are categorized as types of PIT systems, PIT subsystems, or PIT products. An AO with OT within their authorization boundary is responsible for managing the risk for OT and may tailor controls to balance security and availability.

3.3.7. 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.

3.3.8. ISCM Capabilities. CTOs were issued to implement Host Based Security System (HBSS) and Assured Compliance Assessment Solution (ACAS) tools in support of continuous monitoring.

3.3.9. 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.

3.4. RMF Step 3, IMPLEMENT Security Controls. References DoDI 8510.01, NIST SP 800-53r4, applicable Security Technical Implementation Guides (STIG), Security Requirements Guides (SRG), and the DoD's RMF KS**.** (STIGs and SRGs can be found on the DISA website).

3.4.1. Enterprise Architecture, IAW AFI 17-100, *Air Force Information Technology (IT) Service Management*, the Target, Implementation, and Operational Baselines (TB, IB, and OB) address the technical standards, protocols and guidance to establish a consistent environment for IT capability engineering, development, deployment and support. The Baselines are prescriptive and include the items required for a repeatable process to develop and deploy IT capabilities.

3.4.2. Place Contract Data Requirements List (CDRL) items for architecture, design, integration, and verification artifacts on contract to receive the implementation detail for security controls to support risk assessment. Document the implementation in the security plan.

3.5. RMF Step 4, ASSESS Security Controls. References DoDI 8510.01, NIST SP 800-30, NIST 800-53Ar4, applicable STIGs, SRGs, and the DoD's RMF KS. Use DoDI 8510.01, enclosure 6 instructions for details for assessing security controls.

3.6. RMF Step 5, AUTHORIZE System. After reviewing the security authorization documentation, the AO formally accepts or rejects risk by authorizing the IT through an IATT, ATO, ATO with conditions, or a DATO. References DoDI 8510.01, enclosure 6.

3.6.1. AOs may issue an IATT, ATO, or an ATO with conditions for any risk determined not to be "Very High" or "High". **(T-0)**

3.6.2. ATO with conditions for unmitigated "Very High" or "High" risk.

3.6.2.1. The SAF/CIO A6 is the only Air Force member who may grant IT to operate (receive an ATO with conditions) 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. Delegation below the AF CIO is not authorized. IT with "Very High" or "High" risk, which are authorized by other DoD Components connecting to the AFIN require their Component CIO approval, and joint systems require DoD CIO approval.

3.6.2.2. IT with unmitigated "Very High" or "High" risk non-compliant security controls must follow the Very High/High Package Submission Guide and submit completed packages to the SAF/CIO A6 for approval prior to making an authorization decision. **(T-0)**

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

3.6.2.4. 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)**

3.7. Denial of Authorization to Operate (DATO).

3.7.1. If risk is determined to be unacceptable when compared to the mission assurance requirement, then the AO, in collaboration with all program stakeholders, will issue the authorization decision in the form of 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.

3.7.2. Upon issuing the DATO, the AO will provide a copy of the issued document to SAF/CIO A6 via **usaf.pentagon.saf-cio-a6.mbx.a6sc-workflow@mail.mil**.

3.8. RMF Step 6, MONITOR Security Controls. References DoDI 8510.01 and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM)*.

3.8.1. 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.

3.8.2. If a system-level ISCM strategy is not yet developed or executed, as a minimum, periodically assess a subset of the selected controls using a team (e.g., ISSM, sys admin, CSSP, PM, ISO) to ensure any changes are immediately addressed the impact to the system, mission, and capabilities are determined. The periodic assessment is documented in the security assessment report (SAR). The PM updates the POA&M and security plan documents with the new vulnerabilities.

3.8.3. Following the issuance of the authorization decision and establishment of a security baseline (i.e., ATO or ATO with conditions), any changes to the system must be assessed by the system's ISSM to ascertain if the change has a security impact. The ISSM is critical in the initiation of the change review process. The ISSM must consult the SCA for an assessment of any change to the system to determine if re-authorization is required. The rule of thumb is that if the implementation of a security control is affected by the change (especially for IA or IA-enabled products), there must be a validation of the security control implementation, as in the initial assessment effort. Therefore, the authorization is at jeopardy, and the SCA must assess the implementation and assessment of the security control/s and determine if the risk level remains consistent with the current authorization.

3.8.4. If the ISSM determines the system change does not adversely affect the security baseline of the system (i.e., no security impact (NSI)), the system may continue to operate under its current authorization decision. Changes are documented and included with the system security documentation and RMF documentation. The ISSM must provide a synopsis of the NSI to the SCA for concurrence. If the SCA concurs with the NSI, a new authorization decision and connection approval is not required.

3.8.5. If the ISSM determines a change impacts the security baseline of the system, the SCA must evaluate the change and determine the appropriate course of action; that is, the SCA could direct use of an independent validator (i.e., an ASCA) for hands-on evaluation of the system. If the SCA concurs the change impacts the security baseline of the system, and/or a weakness cannot be mitigated in a timely manner to bring the risk back to the level the AO accepted in the current authorization, a new authorization decision and connection approval is required. 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.

3.9. Resources and Tools.

3.9.1. 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. **(T-0)**

3.9.2. PIT Cybersecurity Guidebook**.** *The Platform Information Technology (PIT) Cybersecurity 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.

3.9.3. ASCA Licensing Guide**.** The number and complexity of AF IT may require the AF SCA to designate qualified entities as ASCA 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.

3.9.4. Plan of Actions and Milestones (POA&M).

3.9.4.1. The IT security POA&M is a tool that identifies tasks that need to be accomplished to mitigate systems weaknesses and reduce risk. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in IT. For further POA&M information, refer to the Air Force POA&M Guidebook.

3.9.4.2. SAF/CIO A6ZC will monitor and track the overall execution of system-level IT security POA&Ms (on behalf of the AF CIO and CISO) until identified security weaknesses are closed and the RMF documentation appropriately adjusted. **(T-0)**

3.9.4.3. The PM or ISO is responsible for implementing the corrective actions identified in the IT security POA&M and, with the support and assistance of the ISSM, will provide visibility and status to the ISO, AO, and the AF CIO. **(T-0)**

Chapter 4

APPROVAL TO CONNECT (ATC) PROCESS

4.1. Overview. The 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.

NOTE: Although this Instruction specifies the requirements for connections to the AFIN, other AOs are encouraged to utilize this process to authorize connections to enclaves within their authorization (formerly accreditation) boundary.

4.2. 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 ATD 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.

4.3. Connection to the DoDIN. For enclaves requiring a circuit connection from DISA, ISSMs must follow the DISN Connection Process Guide to ensure all required artifacts are provided on initial submission. Connection requests will be coordinated through the AF Enterprise AO.

4.4. Connection to the Air Force Information Networks (AFIN). The AF Enterprise AO is the only authority permitted to grant an ATC to the AFIN. The Enterprise AO may delegate this authority to appropriate representatives with concurrence of the SAF/CIO A6.

4.4.1. 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.

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

4.4.3. Non-AF owned systems with approved authorizations (i.e., "Guest System", see para 4.5) are required to have an ATC request initiated in eMASS by the AF sponsor, the PM, or ISO before the IT connects to the AFIN.

4.4.4. The AF Enterprise SCA will identify and maintain a listing of the Tier I/II (common) security controls on the RMF KS, Air Force Component Workspace. Furthermore, the AF Enterprise SCA will specify continuous monitoring requirements for each of the identified common controls. **(T-0)**

4.4.5. 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 1/II Common security controls. Required controls may not be tailored out during the security control selection or tailoring steps. Regardless of the source (i.e., Tier I/II 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.

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

4.5. 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.

4.5.1. IT identified as a Guest System must the name of the AF sponsor to **usaf.pentagon.saf-cio-a6.mbx.a6sc-workflow@mail.mil**.

4.5.2. Provide the following information in your request: System acronym, system name, brief system description, ATD, and organization that granted the authorization. If possible, identify the AF community which will use the system and a recommended sponsor.

4.5.3. The appointed sponsor is documented in a sponsorship memo prepared by SAF/CIO A6. 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 for the system being connected. Additionally, the following RMF artifacts or other equivalent are required: Sponsor memo; authorization decision; port, protocol, and services (PPS) listing; hardware/software list; SAR; and POA&M. Additionally, space systems identified as AF IT investments must register in EITDR/ITIPS. **(T-1)**

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

4.6.1. AF functional/mission systems (e.g., A4, SAF/FM, PMOs) systems with an AF Authorization to Operate (ATO), Interim Authorization to Test (IATT), or Authorization to Operate (ATO) with conditions signed by an AF AO (other than the AF Enterprise AO) require an ATC to the AFIN.

4.6.2. The Functional/Mission System PM 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 "Manage ATC" function in eMASS. Contact the AF Enterprise AO staff for other connection (contractor, commercial Internet service provider, direct) AO's POC for information and guidance.

4.7. 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 evaluated and approved by the receiving AO. **(T-0)** If the system fails to meet the continuous monitoring requirements, a Denial of Approval to Connect **(**DATC) may be issued.

4.8. Denial of Approval to Connect (DATC). A DATC may be issued for any IT (connected to the AFIN or other AF enclave) at any time, if the AO determines the risk to the receiving enclave is too high. The PM or ISO is notified immediately of the DATC.

4.8.1. If the system is already connected, the connection must be terminated upon signature of the DATC.

4.8.2. All denial decisions must be signed by the hosting enclave AO, and cannot be delegated further.

Chapter 5

SECURITY CONTROL OVERLAYS

5.1. 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.

5.2. Policy. The DoD may vet all AF overlays for consideration as a DoD or CNSS overlay. The cognizant authorities over 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.

5.3. Development and Approval Process. Follow the process outlined in the AF Approved Overlay Process to develop and approve overlays for use on AF IT.

5.3.1. Send topic to AF Cybersecurity 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.a6sc-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.

5.3.2. 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.

5.3.3. Follow AF Overlay Development and Approval Process. (OPR: Overlay Proposer) If approved, the Overlay Development Team will follow the approved AF Overlay Development and Approval Process. The overlay development team should coordinate with SAF/CIO A6ZC, Cybersecurity Division, throughout the development process.

5.3.4. Support Overlay Development. (OPR: Overlay Proposer/ Overlay Development Team; OCR: SAF/CIO A6, Cybersecurity) The Overlay Proposer is responsible for identifying an Overlay Development Team to build the overlay and supporting documentation. SAF/CIO A6ZC, Cybersecurity Division, can assist with the policy requirements for the overlay.

5.3.5. 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. 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.

5.4. Review and Coordinate Finalized Overlay.

5.4.1. **(OPR: SAF/CIO A6ZC, Cybersecurity Division)** When the Overlay Development Team is completed required actions, the overlay and overlay approval memorandum is provided to SAF/CIO A6ZC for review and posting, as applicable (mission system use, AF or other use, and dissemination). SAF/CIO A6ZC 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.

5.4.2. **(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.

5.5. Coordinate with DISA to Implement Overlay in eMASS. (OPR: SAF/CIO A6, Cybersecurity) SAF/CIO A6ZC, Cybersecurity Division, will coordinate with DISA to implement the approved overlay in the NIPRNet and SIPRNet instances of eMASS. Restrictions on use approved by the Mission Area Owner will be communicated to DISA.

Chapter 6

TRANSFER OF IT BETWEEN AUTHORIZING OFFICIALS

6.1. Overview. Every IT system must be 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 KS) 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.

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

6.2.1. 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.

6.2.2. As the AO staff identifies IT for transfer, it is important to include the MAJCOM Portfolio Manager (PfM) of the IT in this identification process, as the PfM has an integral role in all IT transfer actions.

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

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

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

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

6.2.7. The owning AO and receiving AO agree to the transfer (skip to 6.2.9).

6.2.8. 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-CIO A6ZC workflow at **usaf.pentagon.saf-cio-a6.mbx.a6sc-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.

6.2.9. Once the IT transfer is agreed to by both AOs, the owning AO and receiving AO sign the Request Transfer of Information Technology to Another Authorizing Official Form.

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

6.3. 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 IT Categorization and Selection Checklist identifies the IT should be assigned in the "other" AO Authorization Boundary, then SAF/CIO A6ZC, 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 IT Categorization and Selection Checklist is returned to the PM/ISO for staffing to and approval by the determined AO.

Chapter 7

RMF TRANSITION

7.1. Overview. All IT will transition to the RMF IAW DoDI 8510.01. In addition, the PM or ISO will ensure all IT is in compliance with the timelines specified below. These timelines provide the latest date a DIACAP package may be submitted for C&A and provide RMF submission guidance. The RMF timeline does not prevent a PM or ISO from moving to the RMF sooner than the times specified below. New and existing systems utilizing a contract shall include contract language ensuring the IT complies with the RMF, which may require modification to the contract language. Acquisition requirement officials shall ensure new requirements/systems are compliant with this Instruction and existing systems must be modified to utilize the RMF by the dates below.

7.2. Transition Timeline.

7.2.1. AOs will establish transition timelines for all AF IT (new and existing) within their purview.

7.2.2. PMs or ISOs may submit completed DIACAP packages to the AO for signature until 1 March 2017 (AF specific deadline), and the ATD is determined by the AO signature date, but no DIACAP authorization may exceed 31 March 2018 without an approved RMF Deviation Request.

7.2.3. All packages submitted after 1 March 2017 (AF specific deadline) must comply with RMF policy and guidance (i.e., be in the format of the RMF security authorization package).

7.3. RMF Deviation Requests.

7.3.1. In the case of a significant financial or operational impact due to transitioning to the RMF, an AO may submit a request for deviation to the SAF/CIO A6 for approval.

7.3.2. Requests for deviation must include an RMF transition plan and a POA&M.

7.3.3. Requests are submitted to SAF/CIO A6ZC Cybersecurity, **usaf.pentagon.saf-cio-a6.mbx.a6sc-workflow@mail.mil**, for coordination by the CISO and approval by the SAF/CIO A6.

7.3.4. An approved deviation request does not relieve the IT from maintaining an acceptable risk posture.

WILLIAM J. BENDER, Lt Gen, USAF
Chief of Information Dominance and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 10-1701, *Command and Control (C2) for Cyberspace Operations*, March 5, 2014

AFI 16-701, *Management, Administration and Oversite of Special Access Programs,* 18 February, 2014

AFI 33-115, *Air Force Information Technology (IT) Service Management*, September 16, 2014

AFI 33-141, *Air Force Information Technology Portfolio Management and IT Investment Review*, December 23, 2008

AFI 17-130, *Air Force Cybersecurity Program Management*

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

AFI 33-401, *Air Force Architecting*, May 17, 2011

AFI 63-101/20-101, *Integrated Life Cycle Management,* March 7, 2013

AFMAN 33-153, *Information Technology (IT) Asset Management (ITAM),* March 19, 2014

AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*

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

AFMAN 33-407, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, October 24, 2012

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

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

CJCSI 6211.02D, *Defense Information System Network (DISN) Responsibilities*, January 24, 2012

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

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

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

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

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

Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, October 2016

DoD Comptroller, *Financial Improvement and Audit Readiness* (FIAR) *Guidance,* April 2015

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

DoDD 8000.01, *Management of the Department of Defense Information Enterprise (DoD IE),* March 16, 2016

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

DoDI 5200.02, *DoD Personnel Security Program (PSP),* March 21, 2014

DoDI 5200.08, *Security of DoD Installations and resources and the DoD Physical Security Review Board (PSRB),* December 10, 2005

DoDI 5205.13, *Defense Industrial Base* (DIB) *Cybersecurity/ Information Assurance* (CS/IA) *Activities*, January 29, 2010

DoDI 8500.01, *Cybersecurity*, March 14, 2014

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

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

DoDI 8580.1, *Information Assurance in the Defense Acquisition System*, July 9, 2004

DoDM 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, February 24, 2012

DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Classified Information*, February 24, 2012

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, February 24, 2012

DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, February 24, 2012

Federal Information Security Modernization Act of 2014

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

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, January 15, 2016

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

NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,* June 2015

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, February 2006

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

NIST SP 800-37r1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010

NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, Dec 2014.

NIST SP 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013

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

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

NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)*, May 2015

OMB Circular A-123 as revised, *Management's Responsibility for Internal Control*, 21 December 2004

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016

Title 10 USC § 2224, *Defense Information Assurance Program*, January 7, 2011

Title 44 USC § 3541, *Information Security*

Title 44 USC § 3602, *Office of Electronic Government*, December 17, 2002

Title 5 United States Code (USC) § 552a, *The Privacy Act of 1974, as amended* January 7, 2011

Abbreviations and Acronyms

AF—Air Force

AFCTA—Air Force Cybersecurity Technical Advisory Group

AF EPL—AF Evaluated Products List

AF SACA—Air Force Software and Application Certification Assessment

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 Net (NIPRNet)

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

AFNIC—Air Force Network Integration Center

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AFRMC—Air Force Risk Management Council

AFSPC—Air Force Space Command

AO—Authorizing Official

AODR—Authorizing Official Designated Representative

ARW—Application Request Worksheet

BMA—Business Mission Area

C2—Command and Control

CAL—Category Assurance List

CIO—Chief Information Officer

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CND—Computer Network Defense

CNSSI—Committee on National Security Systems Instruction

CNSSP—Committee on National Security Systems Policy

COCOM—Combatant Command

COMSEC—Communications Security

COTS—Commercial Off-The-Shelf

CTO—Cyber Tasking Order

DATC—Denial of Approval to Connect

DATO—Denial of Authorization to Operate

DSCC—DoD Server Core Configuration

DFARS—Defense Federal Acquisition Regulation Supplement

DIB—Defense Industrial Base

DIMA—DoD Portion of the Intelligence Mission Area

DISA—Defense Information Systems Agency

DNI—Director of National Intelligence

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDIN—Department of Defense Information Network

DSAWG—Defense Information Assurance Security Accreditation Working Group

EITDR—Enterprise Information Technology Data Repository

eMASS—Enterprise Mission Assurance Support Service

FAR—Federal Acquisition Regulation

FIPS—Federal Information Processing Standard

FISMA—Federal Information Security Modernization Act

HAF—Headquarters Air Force

HBSS—Host Based Security System

HQ AFSPC—Headquarters Air Force Space Command

IAW—In Accordance With

IC—Intelligence Community

ICD—Intelligence Community Directive

IEMA—Information Environment Mission Area

IP—Information Protection

IPO—Information Protection Office

IS—Information System

ISCM—Information Security Continuous Monitoring

ISSM—Information System Security Manager

ISSO—Information System Security Officer

ISO—Information System Owners

ISSE—Information System Security Engineering

ISSO—Information System Security Officer

IT—Information Technology

ITIPS—Information Technology Investment Portfolio System

JP—Joint Publication

MAO—Mission Area Owner

MAJCOM—Major Command

NC3—Nuclear Command Control and Communications

NIPRNet—Non-Secure Internet Protocol Router Network

NIST—National Institute of Standards and Technology

NSS—National Security System

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

OSS—Open Source Software

PII—Personally Identifiable Information

PIT—Platform Information Technology

PKI—Public Key Infrastructure

PM—Program Manager

PMO—Program Management Office

POA&M—Plan of Actions and Milestones

PPS—Ports, Protocol, and Services

PPSM—Ports, Protocol, and Services Management

RDS—Records Disposition Schedule

SAF—Secretary of the Air Force

SAP/SAR—Special-Access Program/Special Access Required

SCA—Security Control Assessor

SCI—Sensitive Compartmented Information

SDC—Standard Desktop Configuration

SECAF—Secretary of the Air Force

SIPRNet—Secret Internet Protocol Router Network

SP—Special Publication

SRG—Security Requirements Guides

STIG—Security Technical Implementation Guide

TAG—Technical Advisory Group

UR—User Representative

US—United States

USC—United States Code

USSTRATCOM—United States Strategic Command

WMA—Warfighting Mission Area

Terms

All terms used in this Instruction are defined in CNSSI No. 4009, DoDI 8500.01, or DoDI 8510.01, which may refer to authoritative NIST issuances. Any exceptions are defined below.

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.

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).

Functional System—A system with a mission-unique function usually authorized by an AO other than the AF Enterprise AO (e.g., Global Command and Control System (GCCS), Global Decisions Support System (GDSS))

Operational Technology (OT)—IT adapted to directly monitor and control physical devices, processes, and events where availability is the primary operational concern.

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

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.

Attachment 2

AF IT ASSESS ONLY REQUIREMENTS

1. PIT Subsystems, PIT Products, IT Services, and IT Products. IT categorized below the system level will not require an authorization decision. These 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.

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 complete 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.

1.2. IT Services. Organizations that use internal IT 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 written agreements describing the roles and responsibilities of both the provider and the recipient are in place. 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. Organizations contracting for external IT services in the form of commercial cloud computing services must comply with DoD and AF cloud computing policy and procedural guidance.

1.3. IT Products. Products will be configured by the system administrator in accordance with applicable STIGs under a cognizant ISSM and SCA. STIGs are product specific and document applicable DoD policies and security requirements, as well as best practices and configuration guidelines. When a STIG is not available for a product, a Security Requirements Guide (SRG) may be used.

1.4. 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. This can be accomplished via the following methods:

1.4.1. Assess and Authorize. ISSM's may incorporate software assessment and evaluation, giving the Software Assessment Report (SwAR) as part of their system enclave's security authorization package. Follow the guidance and use the template on the DoD RMF KS.

1.4.2. Air Force Software and Application Certification Assessment (AF SACA). Software products may be assessed through the AF SACA process managed by the Air Force Network Integration Center (AFNIC). The Enterprise SCA then certifies software products for inclusion on the AF Evaluated Products List (AF EPL). Testing may be accomplished by AFNIC 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.
1.4.2.1. All assessments must be initiated and documented using an Application Request Worksheet (ARW). The ARW will be submitted and endorsed by the Wing ISSM or MAJCOM functional directorate.
1.4.2.2. Once the ARW is accepted by AFNIC, testing is accomplished by either the sponsor or AFNIC. The software assessment must be conducted on an environment external to the operational network.
1.4.2.3. If the software product presents an acceptable risk (e.g., low or very low) to the enclave, the major version of the product will be certified for up to 3 years by the AF Enterprise SCA and placed on the AF EPL. 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. This update will be considered a "no security impact" modification to the system authorization.
2. Reciprocity. For products not already assessed via the RMF or the AF SACA process, the Enterprise AO allows ISSMs to use software products that are certified by another DoD AO or SCA. A list of recognized sources can be found at http://go.usa.gov/3vPDS. 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. Compliance with this decision is contingent upon the following conditions:
2.1. The software product and major version is verified on one of the recognized sources.
2.2. Prior to implementation, the system/enclave ISSM must implement any required mitigations to reduce the security risk.
2.3. 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.
3. Software Products Excluded from AF SACA. The following software products must be submitted through the AF Enterprise AO processes:
3.1. Products whose main function is encryption, but does not have Federal Information Processing Standard 140-2 certification.
3.2. Software that does not have a vendor or sponsor responsible for developing security patches.
3.3. Software with immitigable Moderate (CAT II) or higher vulnerabilities.
3.4. Software that uses ports, protocols, or services not listed in the DoD Category Assurance List (CAL).
3.5. Unsupported freeware and shareware.
3.6. Open Source Software (OSS) with no configuration/software support plan.
3.7. IA or IA-enabled products/software (IAW CNSSP No. 11, *National Policy Governing the Acquisition of Information Assurance* (IA) *and IA-Enabled Information Technology Products*).

Attachment 3

FINANCIAL IMPROVEMENT AND AUDIT READINESS (FIAR) IT CONTROLS GUIDANCE (OPR: AF/FM)

1. PURPOSE.
The purpose of this publication is to articulate mandatory guidance necessary to help ensure AF FIAR systems (described below) are authorized in a manner that promotes AF audit readiness under the terms of DoD Comptroller [OUSD(C)] *Financial Improvement and Audit Readiness (FIAR) Guidance*.

2. SCOPE.
2.1. The scope of this attachment encompasses AF system authorization processes relating to all AF systems designated by SAF/FM as AF FIAR systems.
2.2. 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). They 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:
• Controls within the system are identified as key controls in the internal controls assessment;
• Systems are used to generate or store original key supporting documentation;
• Reports generated by the system are utilized in the execution of key controls; or
• Systems are relied upon to perform material calculations (i.e., to compute payroll).
2.3. This attachment's scope does not encompass system authorization processes relating to non-FIAR systems, nor does it include the full range of cybersecurity controls required to protect the confidentiality, integrity and availability of AF systems and applications.

3. APPLICABILITY.
This publication applies to:
3.1. All AF FIAR systems. AF FIAR systems may include but are not limited to: information systems (enclaves, major applications), IT services (internal & external), and IT products (software, hardware, applications).
3.2. All financial or financially-related information that is processed, stored, displayed, and/or transmitted by AF FIAR systems.
3.3. All service level agreements that manage service provider audit readiness requirements.

4. RESPONSIBILITIES.
The following assignment of responsibility and delegation of authority are to be understood as *additions* to the Responsibilities outlined in Chapter 2, rather than *substitutions.*
4.1. SAF/FM CIO. The SAF/FM CIO will oversee:
4.1.1. Adherence of Internal Control over Financial System (ICOFS) risk assessments and continuous monitoring of all AF FIAR systems;
4.1.2. The design of FIAR-related key controls over all AF FIAR systems, as well as tests to ensure their continuous effectiveness.
4.1.3. Development of standard contract language for use in contracts to develop, modify, or support AF FIAR systems to ensure that financial reporting and financial information integrity requirements are properly reflected to meet statutory and regulatory requirements.

4.2. Program Manager (PM). PMs of AF FIAR systems will:
4.2.1. Ensure AF system development lifecycle (SDLC) requirements, relevant FIAR requirements, and required FIAR IT controls are explicitly addressed in contracts with vendors for developing, modifying, or supporting AF FIAR systems.
4.2.3.Manage the design, test, and effective implementation of FIAR-related controls over their respective AF systems.
4.2.4.Oversee the documentation of all controls that are relevant to their system or application in a form suitable for presentation to IT auditors.
4.2.5.Manage the continuous monitoring regimen of AF FIAR systems for which they have program management responsibility.
4.2.6.Manage the process through which the design and tests of effectiveness for programs they manage are properly executed and memorialized in eMASS, to include the collection and storage of evidentiary documents.
4.5.3.Coordinate their activities as required with financial and IT auditors.
4.3. Information Owner (IO). Owners of AF financial and financially-related information pertinent to the AF's consolidated financial audit will:
4.3.1. Establish standards, policies, and procedures for proper handling of their financial information consistent with FIAR guidance.
4.3.2. Coordinate with AF FIAR system owners; identify confidentiality, integrity and availability requirements to help ensure AF FIAR systems are properly categorized.
4.3.3. Coordinate on controls selection and implementation with FIAR system PMs, ISOs, and ISSMs.
4.3.4. Coordinate with AO, SCAs, ISSMs, and ISSOs in the authorization and continuous monitoring processes related to financial information.
4.4. Information System Owner (ISO). Owners of AF FIAR systems will:
4.4.1. Ensure AF FIAR systems under their purview are appropriately categorized.
4.4.2. Coordinate with owners of financial and financially-related information to ensure all financial information handling requirements are appropriately addressed.
4.4.3. Coordinate with all RMF representatives for the AF FIAR system to ensure finance and financially-related controls are properly designed and effectively implemented.
4.4.4. Coordinate with SAF/FM CIO or designee to ensure AF FIAR systems and controls are properly configured to support relevant financial processes.
4.5. Information Systems Security Engineer (ISSE). ISSEs associated with AF FIAR systems will:
4.5.1. Capture and refine FIAR IT control and financial business process requirements, and ensure such requirements are effectively integrated into IT through purposeful architecting, design, development, configuration, and test.
4.5.2.Employ generally accepted best practices when implementing financial and finance-related controls and processes within AF FIAR systems, including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques.
4.6. AO. AOs assigned to AF FIAR systems will:
4.6.1. Assess and accept the risk of any FIAR-related controls not properly designed and not operating effectively before authorizing such systems to process, store, display, or transmit financial or financially-related information.

4.6.2. Ensure the design and tests of effectiveness are properly executed and documented in eMASS, to include the collection and storage of evidentiary documents in support of audit/ FIAR requirements.
4.6.3. Coordinate with the SAF/FM CIO on authorization decisions that have POA&Ms associated with key FIAR controls as referenced in Appendix 1.
4.7. SCA/ SCAR/ ASCA. SCAs/SCARs/ASCAs of FIAR systems will:
4.7.1. Develop a plan to assess key FIAR controls to ensure controls are properly implemented.
4.7.2. Assess FIAR-related controls to determine if they are properly designed and operating effectively before recommending the AO authorize such systems to process, store, display, or transmit financial or financially-related information.
4.7.3. Advise PMs and system owners on measures that could improve the design and/or effectiveness of FIAR-related controls.
4.8. Information System Security Manager (ISSM). ISSMs for AF FIAR systems will:
4.8.1. Maintain the audit readiness of the system throughout its lifecycle.
4.8.2. Support the ISO and/or PM in implementing the RMF in a manner that satisfies IT audit requirements reflected in GAO-09-232G, *Federal Information System Controls Audit Manual (FISCAM)*.
4.8.3. Ensure all audit evidence and related documentation is current and accessible to financial and IT auditors.
4.8.4. Manage the identification and implementation of controls that are relevant to financial audits performed under the terms of DoD Comptroller [OUSD(C)]; leverage the results of prior inspections and audits, including risk assessments performed under OMB Circular A-123 (as revised), *Management's Responsibility for Internal Control*, to develop an understanding the financial controls applicable to their respective system/application environments.
4.8.5. Support the ISO/PM in implementing corrective actions identified in audit Notice of Finding and Recommendations (NFRs)/Notice of Findings (NOFs) and associated plan of action and milestones (POA&M).
4.8.6. Report and present any additions and/or modifications that significantly impact the audit readiness posture of AF FIAR systems. As necessary, conduct additional risk assessments and/or security testing in coordination with assigned SCAs/SCARs/ASCAs. Notify the ISO, PM, and AO if any significant changes occur that may affect the authorization for the system.
4.8.7. In support of annual reporting requirements associated with Internal Controls Over Financial Systems (ICOFS), develop a strategy for continuously monitoring the AF FIAR system and information environment for events and configuration changes impacting the audit readiness posture, and assess the quality of FIAR controls implementation against performance indicators such as security incidents, feedback from external audit agencies, and financial evaluations.
4.8.8. Document all controls relevant to the system or application in a form suitable for presentation to IT auditors.
4.9. Information System Security Officer (ISSO). ISSOs for AF FIAR systems will:
4.9.1. Implement and enforce all AF FIAR policies, procedures, and countermeasures using the guidance within this instruction and applicable financial controls publications (i.e., Reference DoD Comptroller [OUSD(C)]).
4.9.2. In coordination with the ISSM, implement controls relevant to financial audits performed under the terms of DoD Comptroller [OUSD(C)].
4.9.3. Ensure authorized users are not assigned incompatible duties when granted access to AF FIAR systems.

4.9.4. In coordination with the ISSM, maintain all IS authorized user access control documentation; ensure this documentation is kept current, maintained as audit evidence, and made readily accessible to financial and IT auditors.
4.9.5. In coordination with the ISO, PM, and IO ensure software, hardware, and firmware complies with appropriate financial and business process configuration guidelines.
4.9.6. In coordination with the ISSM, initiate protective or corrective measures when a financial incident or vulnerability is discovered; cooperate with the implementation of the POA&M.

5. PROCESS.

The following process descriptions are intended to augment the systems authorization process described in Chapter 3; this supplemental guidance is applicable as described above.

5.1. FIAR Considerations in RMF Step One, *Categorize System.*

5.1.1. IAW categorization guidance contained in CNSSI No. 1253 (Reference (e)) and NIST Special Publication 800-60, Volume 2 (Reference (f)), the baseline security categorization for AF FIAR systems, exclusive of special factors affecting confidentiality, integrity and availability, is, at a minimum, as follows:
Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}
5.1.2. Special factors affecting confidentiality. Confidentiality impacts are generally associated with the sensitivity of specific AF projects' existence, programs, and/or technologies that might be revealed by unauthorized disclosure of financial information. If an AF FIAR system contains financial information pertaining to sensitive programmatic or technical information, the baseline confidentiality value may be raised to Moderate. If the existence of programs or technologies is classified, the baseline confidentiality value may be raised to High.
5.1.3. Special factors affecting integrity. Fraud and errors can affect the AF's image, and corrective actions are often disruptive to operations. Errors represent the greatest threat; if an AF FIAR system contains financial information, the integrity of which supports or is considered crucial to a key decision-making process, the baseline integrity value may be raised to High.
5.1.4. Special factors affecting availability. Permanent loss/unavailability of financial management information can temporarily cripple AF financial operations. If an AF FIAR system contains financial information, the temporary or permanent loss of which would result in a *serious* adverse effect on AF financial operations or assets, or other DoD or federal financial operations or assets, the baseline availability value may be raised to Moderate; e.g., the unavailability of a given application and/or it's information output could directly or indirectly trigger a potentially material erroneous financial event. If an AF FIAR system contains financial information, the temporary or permanent loss of which would result in *severe or catastrophic* adverse effect on AF financial operations or assets, or other DoD or federal government financial operations or assets, the baseline availability value may be raised to High, e.g., the unavailability of a given application and/or it's information output could directly or indirectly triggers erroneous financial events across multiple systems, and/or in a manner that is like to result in a material impact on financial reporting.

5.2 FIAR Considerations in RMF Step Two, *Select Security Controls.*

5.2.1. Many RMF controls and enhancements are identical, or very similar, to analogous FISCAM controls, but require supplementation. DoD's instantiation of RMF allows for supplementary overlays to be issued addressing such specific needs; these overlays levy requirements that modify the standard RMF control baselines. OSD developed one such overlay, *Supplemental Implementation Instruction for Systems Impacting Financial Statement Audit Readiness,* that is intended to be implemented by all DoD components and financial and

financially-relevant systems. However, OSD's guidance allows for flexibility of implementation, stating:
"If during the audit readiness process it is determined that a FISCAM control technique is not key to addressing the control objectives, then the associated RMF/NIST security control would no longer be required for financial statement audit readiness purposes."
5.2.2. AF FIAR systems must apply the control baseline appropriate to each system's overall security categorization, and tailor the resulting controls as appropriate on a system-by-system basis. Controls may be added to address non-financial concerns (i.e., cybersecurity, operational), or intentionally not implemented to contain costs and allow functionality consistent with risk. Such decisions should be the result of a consultative process between IOs, ISOs, PMs, ISSMs, AOs, with a full appreciation for AF financial control objectives. Appendix 1 to this publication contains a list of controls that must be considered. ISSMs and ISSOs should take into consideration and leverage the results of prior inspections and audits, including risk assessments performed in support of OMB Circular A-123.
5.2.3. AF FIAR system PMs, ISOs, ISSMs, and ISSOs must additionally determine which FIAR controls are common to, and/or inherited by, their respective systems/applications. As noted in NIST SP 800-53 r4, the determination as to whether a security control is common or inherited is context-based, and cannot be characterized as common or inherited simply based on reviewing the language of the control.
Many FIAR systems will benefit from inheriting some of the controls from a common service provider; that is, their system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities internal or external to the system/application's responsible organization.
5.2.4. AF FIAR system PMs and ISSM must document all controls relevant to the system or application in a form suitable for presentation to IT auditors. ISSMs should be able to describe in detail which controls are the responsibility of the program, which are shared between the program and an external service provider, and which are inherited from an external service provider.
5.3. FIAR Considerations in RMF Step Three, *Implement Security Controls.* Effective AF FIAR control implementation requires the controls be properly designed, implemented, and operated.
5.3.1. Security Control Design: Proper control design is demonstrated by an architecture of guidance and documentation that includes:
A specific description of the control as it is applies to the system/application environment, including identification of the responsible person(s)/organization(s);
Identification of governing local, AF, and/or DoD plans and policies;
Identification of relevant technical, operational, or behavioral standards; and
Documented procedures addressing the steps for implementing and monitoring the control.
All design documentation must be in final form; documents in draft form will not be considered authoritative for audit purposes.

5.3.2. Security Control Implementation: Proper control implementation is demonstrated by provision of evidentiary materials that prove the control is in place and operating effectively. Evidentiary matter can include but is not limited to:
Meeting minutes
Organizations emails
Populated decision matrices
Formal (i.e., signed and dated) forms, reports, and decision papers
Configuration management records
System logs
Recent operational system records/dumps
Reconciliation records

5.4. FIAR Considerations in RMF Step Four, *Assess Security Controls.* Generally accepted financial audit methodology provides standard procedures for testing both control design and control effectiveness.

5.4.1. Tests of Design (TOD). TOD procedures are performed first; if TOD tests are not passed, the control may be failed in its entirety at the auditor's discretion.

5.4.2. Tests of Effectiveness (TOE). If TOD tests are passed, auditors will execute TOE procedures to assess whether the control is operating as designed and effective in its operation. Should a control not pass TOE, the control will be failed; auditor discretion will be applied to determine the severity of the failure.

5.4.3. Creating, Maintaining, and Presenting Evidence.

5.4.3.1. Evidentiary matter need only supply sufficient evidence of a given control's effectiveness and management's due diligence in continuous monitoring. It is neither required nor desired that evidence be created for no other purpose, or embellished past the point of management's legitimate needs.

5.4.3.2. Evidence will be maintained in the eMASS system of record. eMASS provides a venue for organizing and storing digital information; however, some evidence does not lend itself to digital storage and may be best preserved in hard copy.

5.4.3.3. Some evidentiary records must be created on an ad hoc basis at the auditor's request. PMs, ISOs, and ISSM's should coordinate with the audit team as early as possible to gain an understanding of such possible requests.

5.4.4. Minimizing the impact of audit investigations on mission operations requires pre-audit and pre-interview coordination between the PM, ISSM, and audit team.

5.4.4.1. PMs should expect to receive a request from the audit team for evidentiary documents in the form of a Document Request List (DRL) or Provided By Client (PBC) request, and be prepared to respond in a timely manner. (*Average allotted time to provide evidence is 2 weeks from date PBC is received by the AF team).*

5.4.4.2. PMs should coordinate with the audit team to help ensure interview objectives are clearly articulated by the auditor in order to limit the need for multiple interviews on the same subject and ensure all relevant/knowledgeable system/application personnel are available during the interview.

5.4.4.3. PMs should coordinate with the audit team to help ensure all DRL/PBC requests are satisfied at least 1 day prior to interviews.

5.5. FIAR Considerations in RMF Step Five, *Authorize the System.*

5.5.1. AF FIAR system AOs must obtain the advice and consent of a designated SAF/FM CIO or designated representative before issuing an authorization decision for an AF FIAR system.

5.5.2 FM ISO's coordination on authorization decisions must be formally signed and retained.

5.6. FIAR Considerations in RMF Step Six, *Monitor Security Controls.* AF FIAR system control monitoring will take place both in-process and periodically through internal reviews and external inspections.

5.6.1. AF FIAR systems will be configured to preserve AF financial information's integrity to the greatest extent practical. AF FIAR system ISSOs must configure their respective systems/applications to automatically identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries. Examples of automated integrity functions include, but are not limited to:

Batch totals

Sequence checking

Reconciliations

Control totals

5.6.2 AF FIAR PMs must develop and implement management procedures to identify and correct errors that occur during data entry and processing. Error handling procedures must provide reasonable assurance that errors and irregularities are detected, reported, and corrected. This audit and monitoring capability should include:

User error logs to provide timely follow-up and correction of unresolved data errors and irregularities,

An established monitoring process to assure the effectiveness of error handling procedures, and

Procedures to periodically review user error logs to determine the extent to which data errors are being made, and the status of uncorrected data errors.

5.6.3.AF FIAR system PMs must initiate prompt action to correct deficiencies identified through internal monitoring or external inspection. This includes maintenance of a formal POA&M, as well as procedures to:

Ensure the accuracy of POA&M information.

Prioritize POA&M items based on cost, level of complexity, risk, and impact on the financial statement.

Determine whether control weaknesses identified through IT audits are included in the POA&Ms, and, if not, determining the cause.

Ensure the timely resolution of identified deficiencies. OMB Circular A-123 recommends audit remediation items be addressed within 6 months.

6. FM Control Implementation Guidance.

The RMF process is similar to the DoD C&A process it replaced, but the scope of 'risk management' is substantially greater. While the former process was sharply focused on IT risk, the RMF encompasses both IT risk and business risk, and tends DoD program managers (PMs) to a more varied view of risk that can be continuously monitored at both program and enterprise levels.

This is a favorable development for DoD's financial managers, as the RMF controls baseline aligns more closely with the controls precepts and baselines that are intended to protect the integrity of financial information and processes as expressed in the Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM). Viewed broadly, RMF controls accord with financial substantially, although not completely; in other words, successfully executing the RMF process is tantamount to satisfying most, but not all of the IT general controls in the FISCAM control baseline.

As the AF transitions to the new system authorization process, the AF decided to leverage the RMF to achieve AF financial audit readiness as directed by DoD Comptroller guidance, Financial Improvement and Audit Readiness (FIAR). To this end, Secretary of the Air Force/ Financial Management (SAF/FM) developed financial management (FM) supplemental guidance to augment and extend the RMF controls baseline to fully address all financial and financially relevant controls. This control guidance is intended to be used in conjunction with the RMF process as it is applied to AF financial and financially-related IT, the goal being to use the RMF process to satisfy cybersecurity and FISCAM controls guidance simultaneously.

The Appendix below presents a list of controls that SAF/FM determined to be mandatory for all AF FIAR systems, as well as a list of controls that SAF/FM determined as candidates for tailoring-out on a system-by-system basis.

As noted above in section 2, the controls presented in the appendix relate to securing financial information, and do not encompass the full range of cybersecurity controls that may be required to attain an unqualified ATO.

Appendix 1 to Attachment 3

AF FIAR SYSTEM MANDATORY AND TAILORABLE AF FINANCIAL CONTROLS

This Appendix presents all controls that are or may be applicable to AF FIAR systems. These include both controls presented in NIST SP 800-60 volume 2, as well as additional controls that SAF/FM determined to be mandatory for implementation in AF FIAR systems. Controls that SAF/FM determined to be of insufficient relevance to the AF Financial statement, or which are likely to prove uneconomic or operationally infeasible, are so indicated as ‘Tailorable’ in the Appendix column titled "Control Ranking", so long as those controls are not specified as mandatory for connection to the AFIN. At the discretion of the pertinent AO, controls so indicated can be tailored out of AF FIAR systems' control baselines for the purposes of financial reporting. However, nothing presented in this Appendix is intended to preclude control implementations that are required for cybersecurity or operational purposes.

The complete list of financial management overlay controls can be found here.