BY ORDER OF THE COMMANDER
AIR FORCE RESEARCH LABORATORY (AFRL)

DEPARTMENT OF THE AIR FORCE INSTRUCTION 17-101

AIR FORCE RESEARCH LABORATORY Supplement

28 AUGUST 2025

Cyberspace

RISK MANAGEMENT FRAMEWORK (RMF) FOR DEPARTMENT OF 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: AFRL/IZC

Certified by: AFRL/DC
(Mr. Steven B. Mahurin)

Supersedes: AFRLI17-130, 12 April 2018

Pages: 11

This Air Force (AF) Research Laboratory (AFRL) supplement expands on Department of the Air Force Instruction (DAFI) 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)* by providing AFRL-specific guidance on responsibilities, policies, and procedures. This supplement applies to all AFRL military, civilian and contractor support personnel in accordance with (IAW) appropriate provisions contained in binding support agreements and AFRL contracts. Ensure all records generated as a result of processes prescribed in this publication adhere to *Air Force Instruction 33-322, Records Management and Information Governance Program*, and are disposed of IAW Air Force Records Disposition Schedule, which is located in the Air Force Records Information System. This publication may not be supplemented. Refer recommended changes and questions about this publication to the OPR using DAF Form 847, *Recommendation for Change of Publication;* route DAF Form 847 from the field through the appropriate functional chain of command. Submit requests for waivers through the chain of command to the publication OPR IAW AFRL Delegation of Waiver Approval Authority of Tier Compliance Items Memorandum.

SUMMARY OF CHANGES

(AFRL) This document was substantially revised and converted to a supplement that must be reviewed in its entirety.

1.1. (AFRL) Purpose. This AFRL supplement expands on DAFI 17-101, *Risk Management Framework (RMF) for Department of Air Force Information Technology (IT)* by providing AFRL-specific guidance on responsibilities, policies, and procedures.

1.2. (AFRL) Applicability.

1.2.1. **(ARFL)** This supplement applies to any IT System or IT product, or service procured for use within AFRL facilities or by AFRL organizations for use at any location. These products or services include science and technology demonstrations, experimentation, or related support activities in the various environments the apparatuses are functioning, to include Partnership Intermediary Agreement (PIA) locations, laboratory, or field (ground, air, space, etc.).

3.3. (AFRL) Authorizing Official (AO). The DAF Science &Technology (S&T) AO is the Official with the authority to make authorization decision(s) (e.g., Authorization to Operate (ATO), Denial of Authorization to Operate (DATO), Interim Authorization to Test (IATT)) within the DAF S&T AO Boundary.

3.3.17. **(AFRL)** Be the Official with the authority to approve AFRL use of an existing Federal Risk and Authorization Management Program (FedRAMP) Provisional Authorization to Operate (PATO) or Defense Information Systems Agency (DISA) DoD Cloud Authorization Catalog Provisional Authorization (PA) issuing an ATO or IATT as appropriate.

3.6. (AFRL) DAF S&T Security Control Assessor (SCA).

3.6.6. **(AFRL)** Be responsible for AFRL software certification within the DAF S&T AO's boundary.

3.9. (AFRL) Information System Owners (ISO). AFRL Mission Organization (Msn Org) must officially appoint, in writing, a government official to serve as the Information System Owner (ISO) IAW DAFI 17-101 and Portfolio Manager IAW DAFI 17-110 for all AFRL owned IS to include AFRL owned IS residing in another AO's boundary. DAF S&T AO memos shall state that authorizations are only valid when signed by the Msn Org ISO recognizing responsibility IAW DAFI 17-101 and DAFI 17-110.

3.12. (AFRL) Information System Security Manager (ISSM).

3.12.11. **(ARFL)** Ensure Msn Org level Cybersecurity Representative (e.g. ISSM, Alt. ISSM) attends AFRL Operations Directorate (AFRL/DO) coordinated Flight Test Plan Meetings (FTPMs) for Information Systems (IS) within their purview.

3.18. (AFRL) Cybersecurity Forums.

3.18.4. **(AFRL)** AFRL Cybersecurity Working Group. Official Sub-Working Group under the Digital Information Officer (DIO) Group following the AFRL Group/Board/Council structure. This sub-working group is chartered to address Cybersecurity and related IT issues. Each Msn Org must appoint a primary and alternate representative in writing using the "AFRL Cybersecurity WG Appointment Memo" template located at the AFRL Cybersecurity WG SharePoint site. The completed and signed memo must be provided to the AFRL Cybersecurity Office <**afrl.cybersecurity@us.af.mil**>. Each Msn Org must update their existing memo when personnel changes occur. The distribution list, AFRL Cybersecurity WG SharePoint site and associated collaborative tools will have access granted based on the AFRL Cybersecurity WG Appointment Memos on file. Lastly, Msn Org must ensure an appointee attends each AFRL Cybersecurity Working Group meeting.

4.1. (AFRL) Overview. Managing cybersecurity risks is a complex, multifaceted undertaking requiring the involvement of the entire organization, from senior leaders planning and managing AFRL operations, to individuals developing, implementing, and operating the IT supporting the Science and Technology (S&T). The AFRL implementation of RMF provides an enterprise-wide decision structure for cybersecurity risk management. This provides AFRL organizations with a true picture of vulnerabilities caused by noncompliant security implementations as they relate to other risk factors (likelihood, threat, and impact) and enables better-informed system authorization decisions.

4.1.1. **(AFRL)** The AFRL Cybersecurity Guidebook, located on the AFRL Cybersecurity SharePoint site, is the authoritative source for detailed AFRL-specific guidance for RMF implementation, planning, and execution.

4.1.3. **(AFRL)** AFRL's RMF implementation and associated processes are executed using the AFRL Cybersecurity application and/or DAF Enterprise Mission Assurance Support Service (eMASS). The applications provide capabilities that enable users to input data for AFRL systems, products, and services to aid in enterprise-level system tracking; obtain Software Certifications, Assessments, and Authorization decisions; maintain PPS, Plans of Actions and Milestones (POA&M) and other associated data related to an authorized system.

4.1.4. **(AFRL)** AFRL is transitioning from the AFRL Cybersecurity application to DAF eMASS consistent with the AFRL eMASS Transition Timeline and related guidance in the AFRL Cybersecurity Guidebook. System authorization and change packages must be submitted via eMASS for all new systems and all classified systems. Once an existing system has transitioned to DAF eMASS to be assessed or assessed and authorized via DAF eMASS, associated workflows, and automation, Msn Org ISSMs must submit a new change request via the AFRL Cybersecurity Application to enable the package to be removed from the AFRL Cybersecurity Portfolio based on the updated status that reflects the transition to DAF eMASS. Once this final status change is submitted all RMF activity must be completed in DAF eMASS.

4.6. (AFRL) ASSESS Security Controls. RMF is a framework that focuses on risk, and the security controls implemented to mitigate the risk to an appropriate level. AFRL’s RMF implementation is a dynamic approach to risk management that effectively manages mission and cybersecurity risks in the diverse environments of AFRL systems. The RMF Workflows provide questions and guidance for required documentation and data. Additional information may be requested within the workflow by the DAF S&T AO assessment team at any point during the assessment. Additional information must be provided to ensure a more comprehensive representation of the cybersecurity posture to the submitted system and to ensure a well-informed authorization decision.

4.6.1. **(AFRL)** A sampling of AFRL systems, at the DAF S&T AODR’s/AO’s discretion, will have remote assessments or on-site, eyes-on technical and physical assessments performed.

4.6.2. **(AFRL)** Regardless of assessment type, Msn Org ISSM(s), PMs and Subject Matter Experts (SMEs) (for example: Alternate ISSMs, Information System Security Officers (ISSOs) and System SMEs) must be present and active participants during the assessments.

4.6.3. **(AFRL)** Msn Org and their IT and facility support staff are required to grant full access to systems and facilities for on-site, eyes-on technical and physical assessments to be performed by the AFRL Cybersecurity Assessment team. Remote and on-site assessments will be coordinated via the Msn Org ISSM or Msn Org Alternate ISSMs to ensure proper procedures are followed for access.

4.6.4.2. **(AFRL)** Firewall Exceptions must be initiated and maintained at the Msn Org ISSM level via the Host Communications Unit. Msn Org ISSM will need to use the appropriate process/tool as required by the host base.

4.7. (AFRL) AUTHORIZE System.

4.7.3. **(AFRL)** AFRL IS, products and services will utilize the AFRL RMF processes to obtain assessment and authorization decisions. AFRL IS, products and services will obtain an assessment or authorization decision prior to the operation of the IS, products, or procurement of services. All IS, products and services will utilize a valid RMF process.

4.8. (AFRL) Denial of Authorization to Operate (DATO).

4.8.3. **(AFRL)** A DATO may be issued for systems that fail to follow AFRL processes and comply with applicable laws, regulations, and policy. DATO are issued by the DAF S&T AO based on recommendations from DAF S&T SCA.

4.9. (AFRL) MONITOR Security Controls.

4.9.1. **(AFRL)** There are multiple parts of Continuous Monitoring in place such as Change Management, Software Certification, and on-site Assessments. Msn Org are responsible for maintaining their approved system security posture and documentation of the system including POA&M updates. Documentation which addresses the administrative and policy aspects of a system is a key component of Continuous Monitoring and will be required and reviewed during the compliance portion of the AFRL Inspector General (IG) inspections. A system can be physically, remotely, technically, and administratively assessed at any time during continuous monitoring (i.e., Facilities, PPS, POA&M, relevant RMF documentation, Configuration, Vulnerabilities, STIG compliance, auditing requirements, etc.).

4.9.1.1. **(AFRL)** The AFRL Cybersecurity Guidebook located on the AFRL Cybersecurity SharePoint site provides AFRL specific guidance to implement continuous monitoring.

4.9.8. **(AFRL) Comprehensive Change Management.** Changes made to an approved information system, product or service will be submitted for review via eMASS to determine the impact on its approved security posture. Changes could include, but are not limited to, classification changes, changes to the types of data being processed, configuration changes, updates to the POA&M, or the addition of hardware or software.

4.9.9. **(AFRL) Decommissioning Process.** This RMF Workflow is available in the AFRL Cybersecurity application and eMASS. If a system requires decommissioning, Msn Org ISSMs must submit workflow via the appropriate application.

4.10. (AFRL) Resources and Tools.

4.10.9. **(AFRL)** The AFRL Cybersecurity Guidebook is a living document that supports RMF implementation, planning, and execution within AFRL as the authoritative source for AFRL RMF procedures and guidance consistent with applicable policy and guidance and is located at **https://usaf.dps.mil/teams/20552/default.aspx**.

5.1. (AFRL) PIT Subsystems, PIT Products, IT Services, and IT Products.

5.1.4. **(AFRL)** FedRAMP and/or DISA approved Contractor provided Cloud Service Offerings (CSOs) that process or store government data require Assessment & Authorization via the DAF S&T AO workflow within eMASS to obtain an ATO or IATT.

5.1.5.1. **(AFRL)** When the requesting organization's DIO approves a mission requirement calling for new hardware not previously approved via the RMF process, and this hardware must be installed before the change management process concludes, the AFRL ISSM is responsible for ensuring proper configuration and assessing it as outlined in the AFRL Cybersecurity Guidebook. If the AFRL ISSM determines the addition of the hardware will not raise the risk profile of the system for the environment in which it resides, the ISSM may immediately allow the use of the hardware on the system with notification to the AFRL Cybersecurity Office <**afrl.cybersecurity@us.af.mil**> and requesting organization’s DIO. If the AFRL ISSM determines the addition of the hardware may raise the risk profile of the system or the environment in which it resides, the hardware must be approved via DAF S&T AO before the hardware can be used. The AO may order the removal of the hardware from systems if further investigation reveals additional risk.

5.1.5.2. **(AFRL)** Hardware allowed IAW this process must be added to the existing authorized AFRL RMF package(s) via the Change Management process IAW this instruction within 30 calendar days of installation.

5.1.6. **(AFRL)** AFRL ISSMs have the responsibility to exercise due diligence for software that resides 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. Software may be used on systems within the DAF S&T AO boundary IAW the following processes.

5.1.6.1. **(AFRL)** If the AFRL ISSM determines the addition of the software will not raise the risk profile of the system with all mitigations in place, and after reviewing the test results and related data, the ISSM may immediately approve the use of the software on the system.

5.1.6.1.1. **(AFRL)** All software used on systems must be added to the existing AFRL RMF package(s) via the Change Management process IAW this instruction within thirty calendar days of installation. If automated workflow restricts the ability to complete the change via the formal workflow, update(s) must be provided to the AFRL Cybersecurity Office **afrl.cybersecurity@us.af.mil**. If software is permanently removed from the IS before the thirty calendar days have passed, an update to the RMF package will not be required (for example if it is determined that software does not meet mission requirements after initial use and evaluation). If the ISSM determines the addition of the software may raise the risk profile of the system, the software must be approved via DAF S&T AO before the software can be used. The AO may order the removal of the software from systems if further investigation reveals additional risk.

5.1.6.2. **(AFRL)** Assessed software submitted via RMF may be further reviewed for addition to the AFRL Software Evaluated Products List (EPL) to allow reciprocal use of software across and beyond AFRL. Testing is performed by the organization sponsoring the software product. Instructions, templates, and the testing methodology are located on the Software Tracker subsite of the AFRL Cybersecurity SharePoint site.

5.1.6.2.3. **(AFRL)** If the software presents an acceptable risk (e.g., moderate or below) to AFRL, the major version of the product will be certified for up to 3 years by the AFRL SCA and placed on the AFRL EPL.

5.2. (AFRL) Reciprocity. Software may be added to a system leveraging reciprocity from other sources. If the ISSM determines the reciprocal software will not raise the risk profile of the system, they may immediately approve the use of the software on the system. When using reciprocity, the ISSM must be cognizant of expiration date when one exists and must reevaluate prior to expiration. In addition, ISSM must ensure software is added to the existing AFRL RMF package(s) and that the security baseline is not negatively impacted by checking for supply chain risks and applying all applicable mitigation(s) to include mitigations for vulnerabilities found in National Vulnerability Database (NVD). Reciprocally certified products are not added to the AFRL Software EPL. Cybersecurity reciprocity is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the AFRL, DAF and DoD Enterprise. When applied appropriately, reciprocity reduces redundant testing, assessing and documentation as well as the associated costs in time and resources. For that reason, to promote transparency and interoperability with our DoD and DAF mission partners as well as continue our efforts in achieving efficient and effective mission processes, AFRL will leverage reciprocity to the maximum extent possible. AFRL will accept other DoD Agencies and organizations RMF documentation for software and hardware for review and rapid deployment of capabilities. AFRL will provide AFRL RMF documentation to authorized requestors.

6.1. (AFRL) Overview. All systems connecting to NIPRNet, SIPRNet, DREN, SDREN or any other networks used to support AFRL will require coordination through the appropriate AOs and network owners.

JASON E. BARTOLOMEI,
Brigadier General, USAF
Commander, Air Force Research Laboratory

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DAFI 17-101, *Risk Management Framework (RMF) for Department of Air Force Information Technology (IT)*, 6 February 2020

AFRL Cybersecurity Application, **https://bpms.ebs.afrl.af.mil/prweb/PRWebLDAP1/app/AFRLFW/cRqYMHGdWBOvAFzSBJHFPA*/!STANDARD**.

AFRL Cybersecurity SharePoint, **https://usaf.dps.mil/teams/20552/default.aspx**.

AFRL Cybersecurity WG Appointment Memo, **https://usaf.dps.mil/teams/20552/acwg/shared%20documents/organizational**.

Air Force RMF Knowledge Service (KS), **https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspxCertified** & Authorized Cybersecurity Service Provider (CSSP), **https://intelshare.intelink.gov/sites/jfhq-dodin/JD/CSSP/Pages/Authorized-CSSP-Listing.aspx**

CNSSI-4009, *Committee on National Security Systems (CNSS) Glossary, Committee on National Security Systems Instruction (CNSSI) No. 4009*, 7 March 2022

Department of Defense Cloud Computing Security Requirements Guide, Version 1, Release 4, 20 January 2022, **https://public.cyber.mil/dccs/dccs-documents/**

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

eMASS, NIPRNet, **https://airforce.emass.apps.mil/Public/SiteAgreement**

EMASS, SIPRNet, **https://airforce.emass.csd.disa.smil.mil/**

FedRAMP, **https://marketplace.fedramp.gov**

STIGs Document Library, **https://cyber.mil/stigs/downloads/**

STIG Viewing Tools, **https://cyber.mil/stigs/srg-stig-tools/**

NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, 10 December 2020

Adopted Forms

DAF Form 847, Recommendation for Change of Publication, 22 September 2009

Abbreviations and Acronyms

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFRIMS—Air Force Records Information Management System

AFRL—Air Force Research Laboratory

AFRLI—Air Force Research Laboratory Instruction

AO—Authorizing Official

ATC—Approval to Connect

ATD—Authorization Termination Date

ATO—Authorization to Operate

CCB—Configuration Control Board

CSSP—Cybersecurity Service Provider

DAF—Department of Air Force

DAFI—Department of Air Force Instruction

DATO—Denial of Authorization to Operate

DISA—Defense Information Systems Agency

DIO—Digital Information Officer

DoD—Department of Defense

DoDI—Department of Defense Instruction

DREN—Defense Research and Engineering Network

eMASS—Enterprise Mission Assurance Support Service

EPL—Evaluated Products List

FedRAMP—Federal Risk and Authorization Management Program

FTPM—Flight Test Plan Meeting

GM—Guidance Memorandum

HPW—Human Performance Wing

IA—Information Assurance

IATT—Interim Authorization to Test

IAW—In Accordance With

IG—Inspector General

IS—Information System

ISSM—Information System Security Manager

ISSO—Information System Security Officer

IT—Information Technology

ITN—Integrated Tactical Network

MSN ORG—Mission Organization

MOA—Memorandums of Agreement

MOU—Memorandums of Understanding

NIPRNet—Non-classified Internet Protocol Router Network

NIST—National Institute of Standards and Technology

OPR—Office of Primary Responsibility

PfM—Portfolio Manager

PM—Program Manager/Project Manager

POA&M—Plan of Action and Milestones

PPS—Ports, Protocols and Services

RDS—Records Disposition Schedule

RMF—Risk Management Framework

S&T—Science and Technology

SCA—Security Control Assessor

SCAR—Security Control Assessor Representative

SDREN—Secret Defense Research and Engineering Network

SIPRNet—Secret Internet Protocol Router Network

SRG—Security Requirement Guide

STIG—Security Technical Implementation Guide

USAF—United States Air Force

Terms

Availability—Ensuring timely and reliable access to and use of information.

Confidentiality—Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control Board (CCB)—A group typically consisting of two or more qualified individuals who represent various perspectives from within the organization and have the collective responsibility to review, evaluate, and verify change requirements for a system. The CCB is a check and balance on configuration change activity, assuring that changes are held to organizationally defined criteria (e.g., scope, cost, impact on security) before requesting AO approval for the system change and implementing the system change.

Connected—A system or collection of systems that have a logical or physical connection to any ISP, Tier I network (NIPR, SIPR, DREN, SDREN, etc.), or Tier I networking equipment at any time.

Cybersecurity—Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Information Assurance—(IA) – Measures that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of IS by incorporating protection, detection, and reaction capabilities.

Information System (IS)—A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (NIST 800-34, Appendix G2, pulled directly from 44 USC 3502, paragraph 8.)

Information Technology Services—Both internal and external to AFRL defined as a department or company specializing in computer related services such as assistance and troubleshooting, repair, installation, integration for clients and other such computer and technology related services.

Integrity—Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

MOA/MOU—Document(s) established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.

POA&M—The POA&M is a tool identifying tasks that need to be accomplished to remediate any identified risk (i.e., deficiencies, vulnerabilities, weaknesses) in a program or system. It specifies resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.

Security Posture—The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

STIG—Based on DoD policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.

Tier-1 Network—e.g., Commercial ISP/Internet, DREN, NIPR, SIPR, other WAN, including Wright-Patt ITN.