BY ORDER OF THE COMMANDER
RAMSTEIN AIR BASE (USAFE)

RAMSTEIN AIR BASE INSTRUCTION
17-130

17 NOVEMBER 2023

Cyberspace

UNIT CYBERSECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is 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: 86 CS/SCXS

Certified by: 86 CS/CC
(Lt. Col Eddy G. Gutierrez)
Pages: 10

This publication implements portions of Air Force Instruction (AFI) 17-101, Risk Management Framework (RMF) For Air Force Information Technology (IT), AFI 10-701, Operations Security (OPSEC), AFI 17-130, Cybersecurity Program Management, Air Force Manual (AFMAN), 17-1301, Computer Security (COMPUSEC), AFMAN 17-1302-O, Communications Security (COMSEC), AFMAN 17-1303, Air Force Cybersecurity Workforce Improvement Program, DAFMAN 17-1304, Identity, Credential and Access Management Program (ICAM), and Air Force Systems Security Instruction (AFSSI) 7700, Emissions Security (EMSEC). It applies to all military, civilian, and contract personnel operating, managing, maintaining, or controlling any information systems (IS) program managed by the 86 Communications Squadron (CS) Commander. Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, Records Management and Information Governance Program, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System (AFRIMS). Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using the DAF Form 847, Recommendation for Change of Publication; route DAF Forms 847 from the field through the appropriate functional chain of command.

Chapter 1

PROGRAM OVERVIEW

1.1. Overview.

1.1.1. As of the 17 January 2023 rewrite of DAFMAN 17-1301, no mandate of a Unit Cybersecurity Representative (UCR) program exists. Each unit on Ramstein Air Base (AB) is required to establish a primary and alternate UCR to facilitate Wing Cybersecurity Office support for 56 thousand personnel and 11 Geographically Separated Units (GSU). Additionally, all hosted systems are required to maintain valid Authorizations to Operate (ATOs) with appointed Information System Security Managers (ISSMs) to properly implement cybersecurity and RMF activities for system hosted within the Ramstein circuit enclave. The following instruction has been created to establish and designate the roles and responsibilities of the Ramstein cybersecurity program to provide expeditious and accurate service to its base of over 10,000 users as well as enhance the overall cybersecurity posture of the 86 Airlift Wing (AW). This also includes existing instructions and organizational positions that will appoint, oversee, and coordinate cybersecurity activities for effortless understanding of the Ramstein AB operations, procedures, and scope of responsibility for each position.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. The Wing Cybersecurity Office (WCO). Develops and maintains the Wing Cybersecurity program as well as enforces all guidelines outlined in DAFMAN 17-1301 and AFI 17-101 with the below Ramstein specific additions. Personnel assigned to the WCO will:

2.1.1. Maintain oversite of all COMPUSEC and TEMPEST (terminality referring to the investigation, study, and control of compromising emanations from telecommunications and automated system equipment.) requirements for Ramstein Air Base and Kaiserslautern Military Community (KMC) area of operation or IT under the control of the 86CS, including IT of tenant units (i.e., Field Operating Agencies [FOA], Direct Reporting Unit [DRU], and other mission partners) unless formal agreements exist.

2.1.2. Provide Identity, Credential, and Access Management (ICAM) policy and technical subject matter expertise for IT under the control of the 86 CS, including IT for tenant units.

2.1.3. Develop and coordinates recommendations on implementation of ICAM doctrine, policy, and procedures as well as annual Local Registration Authority (LRA) program audits.

2.1.4. Provide oversight and direction to UCRs (for organizational level programs) according to this instruction and specialized cybersecurity publications.

2.1.5. Ensure UCRs receive cybersecurity training on a minimum annual basis and refresher training as required.

2.1.6. Ensure UCRs attend quarterly working groups as identified by the WCO.

2.1.7. Ensure UCRs are aware of program changes and implement effective cybersecurity policy and procedures.

2.1.8. Ensure UCRs receive quarterly alerts, bulletins, and advisories impacting the security of an organization’s cybersecurity program.

2.1.9. Ensure cybersecurity guidance, and standard operating procedures (SOP) are prepared, maintained, and properly implemented by each unit.

2.1.10. Monitor implementation of cybersecurity guidance and ensure appropriate actions are taken to remedy cybersecurity deficiencies.

2.1.11. Ensure cybersecurity inspections, tests, and reviews are coordinated.

2.1.12. Ensure all cybersecurity management review items are tracked and reported to the WCO.

2.1.13. Ensure software management procedures are developed and implemented according to configuration management (CM) policies and practices for authorizing use of software on Information Systems (ISs).

2.1.14. Serve as member of the base-level CM board or delegate this responsibility to an appropriate Action Officer.

2.1.15. Evaluate modifications, exceptions, and deviations to ISs for accuracy and completeness before forwarding to the appropriate agency.

2.1.16. Consult with host or United States Air Forces in Europe (USAFE) Foreign Disclosure Office (FDO) before authorizing Foreign National/Local National (FN/LN) access to ISs.

2.1.17. Conduct annual COMPUSEC and RMF assessments as well as support any 86 Airlift Wing Inspector General vertical inspections upon notification.

2.1.18. Assist with assessment or analysis supporting Vulnerability Management activities.

2.2. Ramstein Circuit Enclave Information System Security Manager (ISSM). Serves as the primary cybersecurity technical advisor to the Authorization Official (AO), Program Manager (PM), and Information System Owner (ISO) for the Ramstein Unclassified and Classified network circuit enclaves and established procedures for hosted systems to maintain minimum RMF compliance standards. While fulfilling requirements of the role outlined in AFI 17-101 and DAFMAN 17-1301, they will also enforce the below Ramstein specific additions. Personnel assigned to this role will:

2.2.1. Ensure that connecting systems follow proper procedures for acquisition and cybersecurity through the 86 CS Cyberspace Infrastructure Planning System (CIPS) process prior to operational use.

2.2.2. Ensure that systems posing significant risk to the network are identified and mitigated to an acceptable risk level or disconnected if determined to negatively impact the 86 AW mission.

2.2.3. Assist 86 AW Hosted ISSMs with compliance activities to include relaying current AF Enterprise AO RMF requirements and DoD cybersecurity policy guidelines.

2.2.4. Conduct annual unit/organization self-assessments using the AFI 17-101 Risk Management Framework self-assessment checklist (SAC) located in the AF Inspector General (IG) Management Internal Control Toolset (MICT).

2.3. Hosted Information System Security Manager. An ISSM is required for all Ramstein hosted systems, including those not managed under the Ramstein circuit enclave Authorizations to Operate (ATOs) for Secret Internet Protocol Router network (SIPRNet) and Non-Classified Internet Protocol Router Network (NIPRNet) and are required to maintain valid ATOs whether connected to the network or not. Personnel assigned in this role will:

2.3.1. Provide the Ramstein circuit enclave ISSM system identification information within the Enterprise Mission Assurance Support Service (eMASS) or other applicable program of record for Authority to Connect (ATC) and ATO compliance tracking purposes.

2.3.2. Support the 86 CS in implementing corrective actions identified in Plan of Action & Milestones (POA&M), Vulnerability scans, or downward directed cybersecurity taskings.

2.3.3. Ensure new systems are properly vetted through the 86 CS Cyberspace Infrastructure Planning System (CIPS) and fully account for the full RMF lifecycle outlined within AFI 17-101 and DAFMAN 17-1203 prior to operational use.

2.3.4. Perform risk identification and assessment activities supporting change management activities for the system.

2.3.5. Conduct internal unit self-assessments using the AFI 17-101 Risk Management Framework SAC located in the AF/IG MICT.

2.3.6. Assist with all DAFMAN 17-1301 COMPUSEC SAC review and remediation activities.

2.3.7. Provide technical vulnerability data to the 86 CS on a minimum monthly basis or as required.

2.4. Hosted Information System Security Officer (ISSO). An Information System Security Officer is responsible for the technical implementation of a cybersecurity program. When circumstances warrant, a single individual may fulfill both the Information System Security Manager and the Information System Security Officer roles. Department of Defense Instruction (DoDI) 8500.01, AFI 17-101, and AFMAN17-1303 outline the duties of the Information System Security Officer. Ramstein specific ISSO requirements are below. Personnel assigned to this role will:

2.4.1. Be responsible for ensuring the appropriate operational security posture is maintained for assigned IT.

2.4.2. Implement and enforce all AF cybersecurity policies, procedures, and countermeasures.

2.4.3. Ensure software, hardware, and firmware complies with appropriate security configuration guidelines (e.g., Security Technical Implementation Guides (STIGs), Security Requirement Guides (SRG)).

2.4.4. Report security incidents or vulnerabilities to the ISSM.

2.4.5. Participate in Remission Security (REMSEC) risk management processes.

2.4.6. Execute procedures that identify the residual risk and risk tolerance.

2.4.7. Conduct annual COMPUSEC and RMF self-assessments using the AFI 17-101 RMF and DAFMAN 17-1301 COMPUSEC SAC located in the IG MICT.

2.4.8. Assist with AFMAN 17-101 RMF and DAFMAN 17-1301 COMPUSEC SAC review and remediation activities.

2.5. Organizational Commander: Serves as the organizational unit cybersecurity Program Manager and supports cybersecurity requirements through the appointment of representatives to protect and defend ISs enhancing the availability, integrity, confidentiality, authentication, and non-repudiation of data through the application of cybersecurity measures outlined herein. Organizational commanders will:

2.5.1. Assign a minimum of one primary and one alternate UCR to execute cybersecurity responsibilities. These members may be foreign nationals as long as they have a valid local files check, are cleared for access to Unclassified Air Force Network through the USAFE FDO and are in good standing with the Unit Security Manager (USM). Foreign Nationals are limited in their ability to carry out UCR responsibilities for Classified ISs and it is not recommended to appoint these members as primaries.

2.5.2. Ensure that ISs hosted on the Ramstein circuit enclave to support unit missions maintain RMF and cybersecurity baseline compliance.

2.5.3. Ensure that ISs hosted on the Ramstein circuit enclave to support unit missions have appointed ISSMs.

2.5.4. Maintain the organizational COMPUSEC Program IAW DAFMAN 17-1301.

2.5.5. Maintain organizational RMF compliance IAW AFI 17-101 through coordination with appointed organizational Hosted ISSMs and the Circuit Enclave ISSM.

2.5.6. Maintain organizational TEMPEST (EMSEC) program IAW AFSSI 7700.

2.5.7. Suspend access to unclassified and classified ISs when actions threaten or damage AF ISs.

2.5.8. Ensure proper procedures are followed in response to classified information spillages affecting AF ISs.

2.5.9. Review all approved removable media wavers semi-annually to ensure continuous validation of mission requirements.

2.5.10. Endorse follow-up COMPUSEC or RMF assessment reports validating the status of open findings.

2.5.11. Implement and enforce AFNET account management administrative processes and procedures using the guidance within this instruction, in accordance with AFI 17-130.

2.6. Unit Cybersecurity Representative. Members appointed by organizational command or other cognizant authority (i.e., Group Commander) as a primary UCR and at least one alternate UCR should be appointed when cybersecurity functions are consolidated at a central location or activity. Units that are not manned to support UCRs will consolidate the role to the next organizational tier. Personnel assigned to this role will:

2.6.1. Develop, implement, oversee, and maintain an organization cybersecurity program that identifies requirements, personnel, processes, and procedures.

2.6.2. Supervise the organization's cybersecurity program and provide commander's program visibility.

2.6.3. Implement and enforce all Air Force cybersecurity policies and procedures using the guidance within this instruction and applicable specialized (COMPUSEC, TEMPEST etc.) cybersecurity publications.

2.6.4. Assist the WCO in assisting organizational users through IAO Express, Remedy, and CIPS and ticketing systems designated by the 86 CS.

2.6.5. Ensure attendance to all quarterly working groups as prescribed by the WCO.

2.6.6. Assist the WCO in meeting duties and responsibilities tasked by 86 AW through MTOs, NOTAMs, and TMT when information is needed from the organizational level.

2.6.7. Ensure all users have the requisite security clearances, supervisory need-to-know authorization, and are aware of their cybersecurity responsibilities. (via cybersecurity training) before being granted access to Air Force IT.

2.6.8. Ensure IT is acquired, documented, operated, used, maintained, and disposed of properly and in accordance with the IT's security A&A documentation as prescribed by AFI 17-101.

2.6.9. Ensure proper Configuration Management (CM) procedures are followed. Prior to implementation and contingent upon necessary approval according to this instruction and AFI

17-101, the UCR will coordinate any changes or modifications to hardware, software, or firmware with the WCO and system-level ISSM or ISSO.

2.6.10. Ensure all owners of Project Management Office (PMO) systems provide scans for their respective systems as requested by the WCO.

2.6.11. Report cybersecurity incidents or vulnerabilities to the Unit Security Manager, Comm Focal Point, and Wing Information Protection Office.

2.6.12. In coordination with the Unit Security Manager and Comm Focal Point, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered.

2.6.13. Implement and maintain required cybersecurity (COMSEC, COMPUSEC and TEMPEST) countermeasures and compliance measures as directed by the WCO and cognizant authorities.

2.6.14. Initiate requests for temporary and permanent exceptions, deviations, or waivers to cybersecurity requirements or criteria according to this instruction and applicable specialized cybersecurity publications.

2.6.15. When called upon to assist with an assessment conducted by the WCO, provide subject matter experts to analyze the data and provide recommendations for further action.

2.6.16. Maintain all IS authorized user access control documentation IAW the applicable AFRIMS.

2.6.17. Conduct annual unit/organization self-assessments using DAFMAN 17-1301 COMPUSEC SAC located in the IG MICT.

2.6.18. Acts as the focal point for all new IT requirements (printers, computers, network ports, etc).

2.6.19. Assist the WCO with administrative cybersecurity functions to include administrative tasking orders, in/out-processing checklists, and distributing user training materials.

2.6.20. Collects and verifies PKI subscriber requirements to include completion of DD Form 2842 and provides to the WCO.

Chapter 3

COMPUSEC AND RMF ASSESSMENT

3.1. Overview. The COMPUSEC and RMF Assessment is designed to provide Cybersecurity personnel assistance with implementing and maintaining a cybersecurity program within all 86 AW units.

3.2. Objective.

3.2.1. The COMPUSEC and RMF Assessment process is a "find and fix" program review, essentially functioning as a staff assistance visit and therefore, the COMPUSEC and RMF Assessment is not intended to replace, but rather augment, the Air Force Inspection System (AFIS) and strengthen the AF cybersecurity program IAW AFI 17-130 and AFI 17-101.

3.2.2. In instances where local inspection authorities (e.g., Wing Inspection Teams) are already performing inspection activities in partnership with the WCO, conduct a separate annual COMPUSEC or RMF assessment at the discretion of the WCO and organizational commander.

3.2.3. WCO assessments may be combined with MAJCOM IG inspections that assess COMPUSEC or RMF criteria.

3.2.4. Results of these inspections satisfy annual COMPUSEC and RMF assessment reporting requirements in **Paragraph 3.3**.

3.3. Reports. COMPUSEC and RMF Assessment Reports provide a narrative description of the deficiencies and significant trends identified during the assessment period consisting of detailed unit reports, follow-up reports, and annual executive summaries.

OTIS C. JONES, Brig Gen, USAF
Commander, 86th Air Base Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Air Force Instruction (AFI) 17-101*, Risk Management Framework (RMF) For Air Force Information Technology (IT), 23 Feb 2021*

AFI 10-701*, Operations Security (OPSEC), 24 Jul 2019*

AFI 17-130, *Cybersecurity Program Management*, 13 Feb 2020

AFI 33-322, *Records Management and Information Governance Program*, 23 Jul 2021

AFMAN 17-1302-O, *Communications Security (COMSEC)*, 09 Apr 2020

AFMAN 17-1303, *Air Force Cybersecurity Workforce Improvement Program*, 12 May 2020

DAFMAN 17-1203, *Information Technology Asset Management and Accountability*, 13 Sep 2022

DAFMAN 17-1301, *Computer Security (COMPUSEC)*, 17 Jan 2023

DAFMAN 17-1304, *Identity, Credential, and Access Management (ICAM)*, 18 Aug 2021

DAFMAN 90-161, *Publishing Processes and Procedures*, 15 Apr 2022

Air Force Systems Security Instruction (AFSSI) 7700, *Emissions Security (EMSEC)*, 24 October 2007 (IC 14 Apr 09)

Prescribed Forms

DD Form 2842, *Department of Defense (DoD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities*

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AO—Authorizing Official

CM—Configuration Management

COMPUSEC—Computer Security

COMSEC—Communications Security

CSS—Commander Support Staff

DRU—Direct Reporting Units

EMSEC—Emissions Security

FN—Foreign National

FOA—Field Operating Agencies

GSU—Geographically Separated Unit

IG—Inspector General

IS—Information System

ISO—Information System Owner

ISSM—Information System Security Manager

ISSO—Information System Security Officer

IT—Information Technology

LN—Local nation

MAJCOM—Major Command

MICT—Management Internal Control Toolset

OI—Operating Instruction

OPR—Office of Primary Responsibility

OPSEC—Operational Security

PKI—Public Key Infrastructure

PM—Program Manager

POA&M—Plan Of Action & Milestone

RDS—Records Disposition Schedule

REMSEC—Remission Security

RMF—Risk Management Framework

SAC—Self-Assessment Checklists

SOP—Standard Operating Procedures

SRG—Security Relevant Guidance

STIG—Security Technical Implementation Guide

WCO—Wing Cybersecurity Office