BY ORDER OF THE COMMANDER
MACDILL AIR FORCE BASE (AMC)

AIR FORCE INSTRUCTION 17-130_MACDILL AIR FORCE BASE SUPPLEMENT

MACDILL AIR FORCE BASE
Supplement

25 January 2024

Cyberspace

CYBERSECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 6 CS/SCXS

Certified by: 6 CS/CC
(Lt Col Ellis J. Robert III)

Pages: 8

This publication supplements Air Force Instruction (AFI) 17-130, *Cybersecurity Program Management*. It applies to all military, civilian, and contract personnel operating, managing, maintaining, or controlling any information system (IS) programs managed by the 6th Communication Squadron, Commander (6 CS/CC). Refer recommended changes and questions about this publication to the Office of Primary responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication,* from the field through the appropriate functional chain of command. 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 (IAW) the Air Force Records Disposition Schedule (RDS), 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 AF Form 847, Recommendation for Change of Publication; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may not be supplemented or implemented any further. Compliance with the attachments in this publication is mandatory. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items.

1.3. As of the 12 February 2020 rewrite of Air Force Manual (AFMAN) 17-1301, *Computer Security (COMPUSEC)*, no mandate of a Cybersecurity Liaison (CL) program exists. The supplement has been created to setup and designate the roles and responsibilities of the MacDill Air Force Base (AFB) CL program in order to provide expeditious and accurate service to its base of over 5,000 users. This supplement also includes existing instructions and organizational positions that will appoint, oversee, and coordinate with all CLs for effortless understanding of the MacDill AFB operations, procedures, and scope of responsibility for each CL.

2.8.1. **(Added)** Appoint one CL and one alternate (recommend additional alternates if manpower exceeds 120 people) to execute cybersecurity responsibilities protecting and defending information Systems (ISs) by ensuring the availability, integrity, confidentiality, authentication, and non-repudiation of data through the application of cybersecurity measures outlined herein.

2.8.2. **(Added)** Maintain the COMPUSEC Program IAW AFMAN 17-1301.

2.8.3. **(Added)** Maintain the TEMPEST Program, previously known as EMSEC, program IAW Air Force Special System Instruction (AFSSI) 7700, *Emissions Security (EMSEC)*. TEMPEST: A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated ISs equipment.

2.8.4. **(Added)** Suspend access to unclassified and classified ISs when actions threaten or damage AF ISs.

2.8.5. **(Added)** Ensure proper procedures are followed in response to classified information spillages affecting AF ISs.

2.8.6. **(Added)** Review all approved removable media waivers semi-annually to ensure continuous validation of mission requirements.

2.8.7. **(Added)** Endorse follow-up COMPUSEC assessment reports validating the status of open findings.

2.10.4.1. **(Added)** Ensure the integration of cybersecurity into and throughout the lifecycle of the Information Technology (IT) on behalf of the AO.

2.10.4.2. **(Added)** Perform risk identification and assessment activities supporting the change management activities for the system/enclave.

2.10.5. **(Added)** Serve as the cybersecurity technical advisor to the Authorization Official (AO), Program Manager (PM), and Information System Owner (ISO).

2.10.6. **(Added)** Support the PM or ISO in implementing corrective actions identified in the Plan of Actions and Milestones (POA&M).

2.10.7. **(Added)** Appoint Information System Security Officers (ISSOs) and provide oversight to

ensure ISSOs follow established cybersecurity policies and procedures.

2.10.8. **(Added)** Ensure the Air Force IT is acquired, documented, operated, used, maintained, and disposed of properly.

2.10.9. **(Added)** Ensure units conduct AFMAN 17-1301 COMPUSEC MICT SAC and assist with all review and remediation activities.

2.10.10. **(Added)** Conduct annual unit/organization COMPUSEC Staff Assistance Visits (SAVs) using the AFMAN 17-1301 Self-Assessment Checklist (SAC) located in the AF Inspector General (IG) Management Internal Control Toolset (MICT).

2.11.1. Establish COMPUSEC and TEMPEST procedures in the host Wing Cybersecurity Office (WCO). The cybersecurity office addresses all COMPUSEC requirements on the base, including those of tenant units (e.g., Field Operating Agencies, Direct Reporting Units, and other Major Commands) unless formal agreements exist.

2.11.1.1. **(Added)** Assist all base organizations and tenants in the development and management of their cybersecurity program.

2.11.1.2. **(Added)** Provide oversight and direction to CLs (for organizational level programs) according to this instruction and specialized cybersecurity publications.

2.11.1.3. **(Added)** Ensure CLs receive effective cybersecurity training.

2.11.1.4. **(Added)** Ensure CLs are aware of and follow cybersecurity policy and procedures.

2.11.1.5. **(Added)** Ensure CLs receive quarterly alerts, bulletins, and advisories impacting the security of an organization's cybersecurity program.

2.11.1.6. **(Added)** Ensure cybersecurity guidance, and standard operating procedures (SOP) are prepared, maintained, and implemented by each unit.

2.11.1.7. **(Added)** Monitor implementation of cybersecurity guidance and ensure appropriate actions are taken to remedy cybersecurity deficiencies.

2.11.1.8. **(Added)** Ensure cybersecurity inspections, tests, and reviews are coordinated.

2.11.1.9. **(Added)** Ensure all cybersecurity management review items are tracked and reported to the WCO.

2.11.4. **(Added)** Ensure software management procedures are developed and implemented according to configuration management (CM) policies and practices for authorizing use of software on ISs.

2.11.5. **(Added)** Serve as member of the base-level CM board or delegate this responsibility to an

appropriate Action Officer.

2.11.5.1. **(Added)** Evaluate modifications, exceptions, and deviations to Information Systems (IS) for accuracy and completeness before forwarding to the appropriate agency.

2.11.5.2. **(Added)** Assist with assessment or analysis supporting Vulnerability Management.

2.11.6. **(Added)** Consult with host or MAJCOM Foreign Disclosure Office (FDO) before authorizing Foreign National/Local National (FN/LN) access to ISs.

2.11.7. **(Added)** Conduct annual COMPUSEC assessments.

2.16. (Added) The Information System Security Officer (ISSO) shall:

2.16.1. **(Added)** Be responsible for ensuring the appropriate operational security posture is maintained for assigned IT.

2.16.2. **(Added)** Implement and enforces all AF cybersecurity policies, procedures, and countermeasures.

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

2.16.4. **(Added)** Report security incidents or vulnerabilities to the ISSM.

2.16.5. **(Added)** Participate in Remanence Security (REMSEC) risk management processes.

2.16.6. **(Added)** Execute procedures that identify the residual risk and risk tolerance.

2.16.7. **(Added)** Conduct annual COMPUSEC SAVs using the AFMAN 17-1301 COMPUSEC SAC located in the IG MICT.

2.16.8. **(Added)** Assist with AFMAN 17-1301 COMPUSEC SAC review and remediation activities.

2.17. (Added) The Cybersecurity Liaison (CL) shall:

2.17.1. **(Added)** Be appointed by each organizational command or other cognizant authority (i.e., Group Commander, WCO) as a Primary CL and at least one alternate CL should be appointed when cybersecurity functions are consolidated at a central location or activity.

2.17.2. **(Added)** Develop, implement, oversee, and maintain an organization cybersecurity program that identifies cybersecurity requirements, personnel, processes, and procedures.

2.17.3. **(Added)** Supervise the organization’s cybersecurity program.

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

2.17.5. **(Added)** Assist the WCO in assisting organizational users via tools and ticketing systems designated by the WCO.

2.17.6. **(Added)** Assist the WCO in meeting duties and responsibilities tasked by 6th Air Refueling Wing when information is needed from the organizational level.

2.17.7. **(Added)** 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.

2.17.8. **(Added)** Ensure all users receive cybersecurity refresher training on an annual basis to be authorized and maintain access to the base NIPR and SIPR network.

2.17.9. **(Added)** 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.

2.17.10. **(Added)** 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 CL will coordinate any changes or modifications to hardware, software, or firmware with the WCO and system-level ISSM or ISSO.

2.17.11. **(Added)** Report cybersecurity incidents or vulnerabilities to the WCO.

2.17.12. **(Added)** In coordination with the WCO, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered.

2.17.13. **(Added)** Implement and maintain required cybersecurity (COMSEC, COMPUSEC and TEMPEST) countermeasures and compliance measures IAW AFI 10-701.

2.17.14. **(Added)** Initiate requests for temporary and permanent exceptions, deviations, or waivers to cybersecurity requirements or criteria according to this instruction and applicable specialized cybersecurity publications.

2.17.15. **(Added)** 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.

2.17.16. **(Added)** Maintain all IS authorized user access control documentation IAW the applicable Air Force records Information Management System (AFRIMS).

2.17.17. **(Added)** Conduct annual unit/organization self-assessments using AFMAN 17-1301

COMPUSEC SAC located in the Inspector General (IG) Management Internal Control Toolset (MICT).

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

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

Chapter 4 (Added)

COMPUSEC ASSESSMENTS

4.1. (Added) Purpose. The COMPUSEC Assessment is designed to provide Cybersecurity personnel assistance with implementing and maintaining a cybersecurity program.

4.2. (Added) Objective

4.2.1. **(Added)** The COMPUSEC Assessment is a "find and fix" program review, essentially functioning as a Staff Assistance Visit (SAV) and therefore, the COMPUSEC 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.

4.2.2. **(Added)** 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 assessment at the discretion of the WCO and organizational commander.

4.2.3. **(Added)** WCO assessments may be combined with MAJCOM IG inspections that assess COMPUSEC criteria.

4.2.4. **(Added)** Results of these inspections satisfy annual COMPUSEC assessment reporting requirements in paragraph 4.4.

4.3. (Added) Assessment Process

4.3.1. **(Added)** Assessments consist of an interview and site visit with the applicable CL. During the interview, the WCO reviews all responses annotated on the AFMAN 17-1301 COMPUSEC MICT SAC provided by the CL during the last self-assessment. As part of the site visit, the WCO may assess organizational compliance with any COMPUSEC criteria as outlined in this manual. Added areas for review are at the discretion of the WCO.

4.3.2. **(Added)** For geographically separated units (GSUs), remote interviews (i.e., over the phone) are acceptable in lieu of a site visit when travel costs are a concern.

4.3.3. **(Added)** In-brief, out-brief, and other formalization of assessment processes are at the

discretion of the WCO and the assessed unit.

4.3.4. **(Added)** Assessments are not graded but should instead provide organizational commanders an accurate COMPUSEC posture indication by itemizing the deficient COMPUSEC items and summarizing additional observations, recommendations, and best practices.

4.4. (Added) Reports. COMPUSEC Assessment Reports provide a narrative description of the deficiencies and significant trends identified during the annual COMPUSEC Assessment. Reports consist of detailed unit reports, follow-up reports, and annual executive summaries.

ADAM D. BINGHAM, Colonel, USAF
Commander, 6th Air Refueling Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

AFMAN 17-1301, *Computer Security (COMPUSEC),* 12 Feb 2020

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

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

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

AFI 33-322, *Records Management and Information Governance Program,* 23 Mar 2020

AF847, *Recommendation for Change of Publication,* 22 Aug 2019

DAFMAN**,** *Publishing Process and Procedures*, 15 Apr 2022

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AO (Added)—Authorizing Official

CL (Added)—Cybersecurity Liaison

CM (Added)—Configuration Management

COMPUSEC—Computer Security

COMSEC—Communications Security

EMSEC (Added)—Emissions Security

FN (Added)—Foreign National

GSU (Added)—Geographically Separated Unit

IG (Added)—Inspector General

IS (Added)—Information System

ISO—Information System Owner

ISSO (Added)—Information System Security Officer

IT—Information Technology

LN (Added)—Local nation

MAJCOM—Major Command

MICT (Added)—Management Internal Control Toolset

OPR (Added)—Office of Primary Responsibility

OPSEC (Added)—Operational Security

PKI (Added)—Public Key Infrastructure

PM (Added)—Program Manager

POA&M (Added)—Plan of Action & Milestone

RDS (Added)—Records Disposition Schedule

REMSEC (Added)—Remanence Security

RMF—Risk Management Framework

SAC (Added)—Self-Assessment Checklists

SOP (Added)—Standard Operating Procedures

SRG (Added)—Security Requirements Guide

STIG—Security Technical Implementation Guide

WCO (Added)—Wing Cybersecurity Office

Terms

Foreign Nation/Local National (FN/LN) (Added)— Any person other than a US citizen, US permanent or temporary legal resident alien, or person in US custody

Information System Security Officer (ISSO) (Added)— Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

Plan of Action & Milestone (Added)— A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Remanence Security (REMSEC) (Added)— Residual information remaining on data media after clearing. (Committee on National Security Systems Instruction No. 4009).