BY ORDER OF THE COMMANDER
AIR COMBAT COMMAND

AIR COMBAT COMMAND
INSTRUCTION 11-270

6 NOVEMBER 2024

Flying Operations

OPERATIONS MOBILE DEVICES (OMDS)

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: ACC/A3TV
Certified by: ACC/A3T
Supersedes: ACCI11-270, 9 October 2019
Pages: 31

This instruction implements Air Force Policy Directive (AFPD) 11-2, *Aircrew Operations*. It prescribes procedures for Operations Mobile Device (OMD) program implementation, execution, and sustainment across all Combat Air Forces (CAF) Flying Squadrons and Operations Support Squadrons (OSS) aircrew members only directly involved in flying operations. This instruction applies to all Air Combat Command (ACC) flying units, Air Force Reserve Command (AFRC) and Air National Guard flying units. This publication is applicable to all Combat Air Force Aircrew operators that fly Air Combat Command Mission Design Series' (MDSs) which ACC is the Lead Command as stated in Department of the Air Force Directive (DAFPD) 10-9, *Lead Command/Lead Agent Designation and Responsibilities for the United States Air Force Weapons System, Non-Weapon Systems, and Activities*. Additionally, this instruction has been coordinated with CAF flying units under Pacific Air Forces (PACAF) United States Air Forces Europe-Air Forces Africa (USAFE-AFAFRICA), Air Education and Training Command (AETC), Air Force Material Command (AFMC), and Air Force Special Operations Command (AFSOC). It is not applicable to USAF Civil Air Patrol auxiliary non-profit organizations or the United States Space Force. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (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. Refer recommended changes to this publication to Air Combat Command Standardization and Evaluation (ACC/A3TV) at 205 Dodd Blvd, Suite 234, Joint Base Langley-Eustis, VA, 23665, DSN 574-8170 using Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*, in accordance with (IAW) Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures*; route DAF Forms 847 from the field through the appropriate Standardization and

Evaluation (Stan/Eval) chain of command. This publication may be supplemented at any level, but all direct supplements must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination prior to certification and approval. The authorities to waive wing (WG) or unit level requirements in this publication are identified with a Tier ("T-2 or T-3") number following the compliance statement IAW DAFMAN 90-161. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the publication OPR for non-tiered compliance items. See **paragraph 1.3** through **paragraph 1.3.4** for waiver guidance. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the DAF.

SUMMARY OF CHANGES

This document has been revised and should be completely reviewed. Changes include: redefining Electronic Flight Bag (EFB) and Electronic Kneeboard (EKB) as Operations Mobile Devices (OMD), added new roles and responsibilities process in **paragraph 1.2**, updated content to **paragraph 1.3**, waivers, and Product Improvement Program (PIP) indicates newly revised material.

Chapter 1

GENERAL INFORMATION

1.1. Purpose.

1.1.1. This instruction provides directive guidance on the CAF OMD program, to include its development, processes, operation, and employment.

1.1.2. The CAF OMD program office will provide guidance on additional OMD capabilities as they become available in the future via Flight Crew Information Files (FCIF), publishing announcements on the CAF OMD program SharePoint® via the CAF OMD Baseline Configuration, or via direct emails and Higher Headquarters (HHQ) messages.

1.2. Roles and Responsibilities.

1.2.1. ACC Director of Operations (ACC/A3): Provides overall guidance for the operational aspects and requirements of the CAF OMD program.

1.2.1.1. ACC/A3TV: Serves as the overall program OPR for the CAF OMD program. ACC/A3TV will be responsible for the following:

1.2.1.1.1. Designates a CAF OMD Program Manager (PM) and a CAF OMD Section Lead. The CAF OMD PM will maintain overall responsibility for the CAF OMD program, including all CAF OMD Baseline Configurations, which are all living documents.

1.2.1.1.2. Maintains a CAF OMD SharePoint®, which serves as the focal point for the latest information, policy, and guidance affecting the CAF OMD program at **https://usaf.dps.mil/sites/ACC-A3/A3T/A3TV/OMD**

1.2.1.1.3. Issues FCIF messages, when necessary, as indicated by ACC/A3TV. ACC/A3TV, in conjunction with their Stan/Eval augmentees, will evaluate WG level OMD programs as part of Department of the Air Force Instruction (DAFI) 90-302, *The Inspection System of the Department of the Air Force.* They will also be responsible for verifying the accuracy of available publications.

1.2.1.1.4. Is responsible for maintaining the Authority to Operate (ATO) and any other necessary approvals or waivers as it relates to the CAF OMD program.

1.2.1.1.5. Develops and fields aircrew training material hosted on the OMD device. This training material will be located on the CAF OMD program SharePoint®.

1.2.1.2. ACC/A3 MDS Functional Area Managers (FAMs): FAMs retain primary responsibility to submit requests, coordinate with the System Program Office (SPO) via ACC Directorate of Requirements (ACC/A5), and otherwise manage initial approval processes for their MDS for future capabilities. ACC/A3TV will assist the FAMs on all aspects of MDS OMD program development.

1.2.1.3. ACC Flight Operations Division (ACC/A3T): ACC/A3T will provide the estimated OMD cost that ACC/A3TV compiled to ACC Resource and Budget Division (ACC/A3R) for funding on an annual basis.

1.2.1.4. ACC Flight Operations and Training Branch (ACC/A3TO): ACC/A3TO will be responsible for ensuring that any mobile devices under their purview (e.g., Aircrew Flight Equipment (AFE) mobile devices) have current publications loaded, ensure that units have proper equipment, and that the resources for those tools are properly funded and managed.

1.2.1.5. ACC/A3R: ACC/A3R advocates for funds in the Execution and Budget Year through ACC Comptroller (ACC/FM). This includes the items that will be required to support the OMD program as listed below in paragraphs **1.2.9**, **2.2.2**, and the sub-paragraphs of those sections.

1.2.1.6. ACC Future Operations Division (ACC/A35): ACC/A35 will be responsible for exploring future technology and advanced use-cases of the OMD program. New OMD use cases also extends to wearable technology that augments OMDs.

1.2.2. Directorate of Plans, Programs and Requirement (ACC/A5/8/9): Responsible for developing and managing OMD program requirements, including MAJCOM OMD applications, and serve as the primary MAJCOM liaison to MDS SPOs. The A5 Weapons System Teams (WSTs) will work with their respective FAMs to develop OMD requirements. ACC/A5 advocates for funding for MDS specific applications with appropriate Air Force Life Cycle Management Center (AFLCMC) program offices as the requirements are generated. ACC/A5 will not purchase unit-specific applications. Such applications will be purchased at unit expense as specified in **paragraph 2.2.2**.

1.2.3. CAF SAPMO Security & Policy Division (ACC/A5/8Z): Inform ACC/A3 on equipment (hardware and software) configuration restrictions/requirements to ensure advanced program considerations are effectively managed by the CAF OMD PM.

1.2.4. ACC Communications Directorate (ACC/A6): ACC/A6 will support and advise on all aspects of the Enterprise Mobile Management (EMM) solution, including, but not limited to policy, cybersecurity, assessment and accreditation, equipment spectrum supportability, frequency assignments, and mobile capabilities. Furthermore, ACC/A6 will coordinate on any ACC/A3 correspondences outside of ACC related to EMM.

1.2.5. ACC Acquisition Management and Integration Center (ACC/AMIC): ACC/A3 will coordinate with ACC units and their local contracting squadrons to facilitate any OMD contract requirements, as necessary.

1.2.6. ACC Judge Advocate (ACC/JA): Advise ACC/A3 on legal matters relevant to the OMD program, and serve as the MAJCOM liaison on OMD issues to legal agencies outside of ACC.

1.2.7. ACC Public Affairs (ACC/PA): Collaborate with ACC/A3 on any required or desired internal/external messaging related to the CAF OMD program and assist ACC/A3 and subordinate agencies with media issues related to the OMD program.

1.2.8. ACC Chief of Safety (ACC/SE): Advises ACC/A3 on safety issues related to the OMD program and serve as the MAJCOM liaison on OMD issues to safety agencies outside of ACC.

1.2.9. Wing Commanders (WG/CCs) or Equivalent Directorates: Ensure Organizational or WG-level advocacy and support for the OMD program as follows:

1.2.9.1. Designate and provide, in writing, primary, and alternate WG OMD PM to the CAF OMD PM Email appointment letters to ACC/A3TV CAF Operations Mobile Devices **ACC.A5A3.EFB@us.af.mil**. **(T-3)**

1.2.9.2. Ensure subordinate WG-level agencies and personnel support the OMD program as specified in this instruction. **(T-3)**

1.2.9.3. Account for OMD sustainment costs in annual Wing budgetary processes IAW **paragraph 2.2.2**. **(T-3)**

1.2.9.4. Operations Group (OG) Commanders (OG/CCs) for geographically separated units (GSU) may appoint Group OMD PM that fulfill the functions of the WG OMD PM for their unit. **(T-3)**

1.2.9.5. Commander/Director Equivalent/Designated Representatives may appoint Group OMD PM for units not belonging to WGs (e.g., Detachments, Operating Locations, or Air Force Elements, Direct Reporting Unit, or Field Operating Agency.) **(T-3)**

1.2.10. Flying Squadron Commanders (SQ/CCs) and OSS/CCs: Designate and provide, in writing, primary and alternate Squadron OMD PM to the Wing OMD PM and the CAF OMD PM via email to ACC/A3TV CAF Operations Mobile Devices (**ACC.A5A3.EFB@us.af.mil**). Appointment letters may be combined with the WG appointment letter as discussed above. For locations where all OMD program management has been consolidated at the Group or WG level, this is not required.

1.2.11. Communications SQ/CCs: Provide communications, cybersecurity, and information technology support to WG-level OMD programs as follows:

1.2.11.1. Ensure OMD hardware is managed IAW DAFMAN 17-1203, *Information Technology Asset Management (ITAM) and Accountability.*

1.2.11.2. Coordinate with WG OMD PM to support procurement of commercial internet access on government installations such as utilizing base infrastructure currently in place or new fiber optic cable installs that require work orders or access to communications closets.

1.2.11.3. Coordinate WG-level guidance and procedures, IAW applicable MAJCOM guidance, Air Force, and DoD policy, to permit the introduction of OMD devices into Classified Processing Areas (CPAs) under their purview and identified as mission essential by the WG OMD PM and as authorized by HQ ACC.

1.2.12. Wing OMD PMs. Maintain overall responsibility for the WG OMD program as follows:

1.2.12.1. Identify, address, and elevate, as necessary, OMD requirements and concerns to WG leadership and the CAF OMD PM.

1.2.12.1.1. Will coordinate issues to the CAF OMD Program office on behalf of their Squadron OMD PM.

1.2.12.1.2. Will follow CAF OMD ROE to contact the CAF OMD office during designated hours identified on the CAF OMD SharePoint®.

1.2.12.2. Ensure devices are configured, issued, tracked, updated, and maintained as required by this instruction.

1.2.12.3. Coordinate with Technical Order Distribution Officers (TODOs) to provide OMD users with current electronic flight and ground publications and guidance on

approved methods to keep all required publications up to date on the OMD in accordance with this instruction.

1.2.12.4. Provide the CAF OMD PM with feedback on operational assessments and development of OMD solutions.

1.2.12.5. WG OMD PM will establish a WG OMD PM organizational email box which will be annotated on the WG OMD PM appointment letter. **(T-2)** All CAF OMD related messages and issues will be sent to this organizational box.

1.2.13. Roles and responsibilities of WG OMD PM.

1.2.13.1. Perform all setup, maintenance, and restoration functions on OMD devices to include:

1.2.13.1.1. Device/App unlock.

1.2.13.1.2. Device/App password resets.

1.2.13.1.3. Device wipes.

1.2.13.1.4. Device activations.

1.2.13.1.5. Notify CAF OMD office to initiate lost mode.

1.2.13.2. Perform all setup, maintenance, and restoration functions on Mobile Device Management System (MDMS) to include:

1.2.13.2.1. Facilitating the MDMS setup (based on the Mobile Device Management (MDM) provider or configuration profile provided by the CAF OMD Program Office).

1.2.13.2.2. Initiating MDMS operating system updates as approved by Defense Information Systems Agency (DISA) and CAF OMD Program Office.

1.2.14. Operations Group Stan/Eval (OGV): Enforce Stan/Eval policy applicable to the OMD program, including currency of required flight publications.

1.2.15. Squadron Stan/Eval (CCV) and OSS: Ensure Stan/Eval guidance applicable to the OMD program, including currency of required flight and ground publications for the applicable OMD's they are responsible to maintain.

1.2.16. Squadron OMD PM: Maintain overall responsibility for the Squadron OMD program as follows:

1.2.16.1. Identify, address, and elevate, as necessary, OMD requirements, issues and concerns to Unit leadership and the WG OMD PM Coordinate with TODOs to provide OMD users with current electronic flight publications and guidance on approved methods to keep all required publications up to date on the OMD in accordance with this instruction.

1.2.16.2. Provide the WG OMD PM with feedback on operational assessments and development of OMD solutions.

1.2.16.3. Ensure all applicable forms are completed for each user. This includes the DAF Form 4433, *The Department of the Air Force Mobile Device User Agreement*, DAF Form 1297, *Temporary Issue Receipt*, and any other user agreements that are required.

1.2.16.4. Ensure all Unit OMD user training is completed; to include device setup, device operations, troubleshooting, vault entry/exit procedures (if applicable), simulator operations (if applicable), user account setup, automatic dependent surveillance broadcast-in (ADS-B IN) check in/out procedures, etc.

1.2.16.5. Responsible for identifying and coordinating with WG OMD PM for approval of utilizing OMDs in specific classified areas, such as simulators.

1.3. Waivers and Product Improvement Program (PIP).

1.3.1. Units will coordinate with their chain of command WG OMD PM for any waiver request. WG OMD PMs will submit request to CAF OMD office for processing, coordination, and approval by MAJCOM/A3 or the appropriate agency. CAF MAJCOM/A3s other than ACC/A3 may waive guidance in this instruction for items that do not affect the other CAF MAJCOMs (e.g., items isolated to a single MAJCOM).

1.3.2. Waivers to this publication. Units requesting waivers to the guidance provided in this document will use the DAF Form 679, *Department of the Air Force Publication Compliance Item Waiver Request/Approval*, on the CAF OMD Program SharePoint® and request waivers through the OG or ***WG OMD PM*** (if applicable), to the MAJCOM Stan/Eval OMD PM office (if applicable), to ACC/A3TV. **(T-2)** Upload all waiver requests to the [Waiver] section of the CAF OMD Program SharePoint®. The ***CAF OMD PM*** work with the unit to process the waiver and will publish the results of the waiver request on the CAF OMD SharePoint®.

1.3.3. OMD Configuration Waivers. Configuration waivers, deviations, and change requests will be submitted via the CAF OMD Program SharePoint® site under the [Waiver] section on AF Form 4169, *Request for Waiver from Information Assurance Criteria*, for coordination with the Authorizing Official (AO).

1.3.4. PIP. Submit all PIP ideas (e.g., new Apps, websites, accessories) through the WG OMD PM. For any PIP submission that will result in funding requirements outside of the Unit or manpower outside of the unit, route the PIP form through the OG/CC and WG OMD PM. All PIP ideas will use the AF Form 1768, *Staff Summary Sheet,* and submitted on the CAF OMD Program SharePoint® under the [Waivers] section.

Chapter 2

PROGRAM IMPLEMENTATION

2.1. General.

2.1.1. Units operating under local Concept of Operation (CONOPS). Units will follow the direction of this Air Combat Command Instruction (ACCI) if operating OMDs unless a specific waiver has been granted to operate their own OMD program. Use-cases not discussed in this instruction will be coordinated with the CAF OMD office prior to launching those efforts. Units who possess a waiver to operate their own OMD program from the MAJCOM/A3 and have an approved Interim Authority to Test (IATT) or ATO from the appropriate AO, will supplement this ACCI accordingly and will not have their own standalone CONOPS **(T-2)**

2.1.2. OMD Testing. The CAF OMD office periodically requires testing outside of their office and will coordinate with outside agencies at their earliest opportunity should testing be required. For OMD's, the CAF OMD office will work the various aircraft test units in ACC, the National Guard Burera (NGB), and AFRC to accomplish in-flight or specialized testing if required. For aircraft types where no test organization exists, the CAF OMD office will coordinate directly with line units. For routine testing (e.g., non-flight testing), the CAF OMD office will coordinate with any unit that can evaluate routine items (e.g., setup of devices, functionality testing of new Apps, and publications distribution).

2.2. Funding.

2.2.1. MAJCOM Funding.

2.2.1.1. Each MAJCOM will budget for and fund the initial procurement of OMD hardware, including the device, charging cord, protective case, licenses for the MDM/Mobile Content Management (MCM) enrollment, and pubs reader software for each CAF flying unit. Each MAJCOM may help augment unit sustainment funding of the OMD program if funding is available, but the primary source of funding is the unit until an Air Force program of record is established, at which time funding will transition to that office.

2.2.1.2. ACC/A3 FAMs will work with the ACC/A5 MDS WST and SPO to program for sufficient funding on an annual basis to support requirements identified by ACC/A3.

2.2.2. WG/unit Funding Requirements. WGs and units will budget for and fund the following OMD related requirements:

2.2.2.1. Hardware Refresh: WGs, in coordination with the CAF OMD office, to ensure program integrity, will budget for updated OMD hardware at intervals driven by device usable service-life and current OMD program requirements. **(T-2)**

2.2.2.2. Procurement of additional OMD devices (e.g., replacements for broken or missing devices), as required, not covered by the initial MAJCOM-funded equipment procurement. **(T-2)**

2.2.2.3. OMD compatible flight gloves. The AFLCMC Air Force Uniform Office (Human Systems Division) (AFLCMC/WNU) maintains the current list. Should the gloves on that list be found to be poor choices for certain mission needs, OG/CCs may approve gloves not on the list but must maintain a risk assumption memorandum on file that discusses their

rationale for choosing the alternate gloves and how they are mitigating the risk by not using approved gloves. **(T-2)**

2.2.2.4. Procurement of OMD Anti-Glare and Night Vision Device (NVD) compatible filters.

2.2.2.5. Procurement of OMD ADS-B IN Devices.

2.2.2.6. Procurement of approved OMD battery life extenders.

2.2.2.7. Procurement of standalone OMD management laptops and docking stations.

2.2.2.8. Procurement of authorized OMD mounting solutions, if desired. Base or Commercial internet access and sufficient quantities of wireless routers, as specified in **paragraph 3.1.1.3**, to support unit OMD requirements.

2.2.2.9. Unit-specific OMD applications. Units may only purchase CAF OMD approved applications, as specified on the OMD Baseline Configuration, located on the CAF OMD SharePoint®. Units will submit a request to the CAF OMD Program Office for any applications not listed on the OMD Baseline Configuration. Upon approval, units will be authorized to procure the requested application(s) at unit expense after coordinating with the CAF OMD office.

2.2.2.10. If units choose to upgrade to cellular data capable devices, they will be responsible for the cellular data plan cost. Cellular capable devices are approved IAW current CAF Special Security Office (SSO) and Special Access Program Management Office (SAPMO) guidance and policies to include devices, potential data plans, GPS functionality, etc. Future approval of cellular capable devices for TS/SCI or Special Access Program (SAP) capable aircraft will be published by the applicable security office and posted on the CAF OMD SharePoint® as a waiver to this paragraph. **(T-2)**

2.2.2.11. TDY expenses related to initial/recurring WG OMD PM and/or MDM/MCM training, and any other TDY required to properly execute the unit-level OMD program.

2.3. Operations Mobile Device (OMD) Approval Requirements.

2.3.1. General. The list below outlines the various documents required for OMD operations. The list of documents can be found at the CAF OMD Program SharePoint®. If new document requirements are generated, the CAF OMD Program Office will identify the requirement and place guidance on the CAF OMD SharePoint until such time that this instruction is re-written.

2.3.2. All OMDs:

2.3.2.1. This ACCI covering OMDs or equivalent for other CAF MAJCOMs (OPR: ACC/A3TV).

2.3.2.2. Unit supplement to this instruction if operating under a MAJCOM/A3 waiver to operate their own OMD program (OPR: ACC/A3TV).

2.3.2.3. [If applicable] AO or Designated Approval Authority (DAA) approved ATO (OPR: ACC/A3TV).

2.3.2.4. [As applicable] CPA, Special Access Program Facility (SAPF), and Sensitive Compartmentalized Information Facility (SCIF) entry approval for OMDs (OPR: MAJCOM SAP office, WG Cybersecurity/IP Office, or DAA).

2.3.2.5. May create a unit level Supplement to this ACCI (OPR: WG OMD PM). **Note:** See **paragraph 2.1.1** for units that are required to supplement this publication and reference opening paragraph for supplement guidance.

2.3.2.6. Final MAJCOM/A3 approval message, FCIF from the MAJCOM/A3, or inclusion on the CAF OMD Baseline Configuration (OPR: ACC/A3TV).

2.3.2.7. Electromagnetic Interference (EMI) Certification (OPR: ACC/A3TV).

2.3.2.8. [If applicable] Any battery life extender EMI Certification (OPR: ACC/A3TV).

2.3.2.9. [If applicable] Hazards of Electromagnetic Radiation to Ordnance (HERO) (OPR: ACC/A3TV).

2.3.2.10. Explosive Decompression / Atmospheric Testing (OPR: ACC/A3TV).

2.3.2.11. New mobile device use-cases must be discussed with the CAF OMD office prior to implementation and documented accordingly as referenced in this ACCI.

2.3.2.12. Coordination must occur to ensure that all paperwork is accomplished, and all approvals are granted.

2.3.3. Approved Devices.

2.3.3.1. The CAF OMD office will announce approved OMD devices via FCIF, announcements on the CAF OMD SharePoint®, or via inclusion on the current OMD Baseline Configuration document. The CAF OMD PM will provide device implementation, funding processes, and associated timelines if applicable.

2.3.3.2. Recommendations for new devices, features, accessories, etc., will be submitted to the CAF OMD office for review IAW this instruction.

2.3.3.3. All devices approved for use are deemed sufficiently secure to view/store/process information identified in this instruction and approved by the data owners.

2.3.3.4. The Air Force Enterprise AO or DAA certified the OMD system via a “System” accreditation ATO. All OMDs and MDMS systems must be configured and secured IAW the ATO (if applicable).

2.3.3.5. OMD systems are approved for use by the MAJCOM/A3 IAW AFMAN 11-202, Volume 3, *Flight Operations*. It is mandatory that all OMDs and MDMS systems used by all CAF flying units are configured and secured IAW the applicable ATO.

2.3.3.6. Only government issued OMD devices may be used to store DoD information for flight operations IAW AFMAN 17-1301, *Computer Security (COMPUSEC),* and this instruction.

Chapter 3

OPERATIONS AND EMPLOYMENT

3.1. Operating Instructions. OIs will address:

3.1.1. Required Equipment.

3.1.1.1. All MDMS computers must be managed/setup IAW **paragraph 3.1.2**. All units operating certain OMD's may require a backup per the program ATO. Approved read only/re-writeable CD/DVD can be used as a back-up method. Deploying units are highly encouraged to maintain an MDMS computer and update prior to deployment.

3.1.1.2. Some programs may require annotation of data transfer via media.

3.1.1.3. Wireless networking equipment required for compliance with the Air Force Commercial Internet Service Provider (CISP) solution for OMD programs IAW the ATO and Secretary of the Air Force, Chief Information Officer (SAF/CN) or DoD Components must submit requests for information security waivers or exceptions to the standards and requirements in this instruction through the chain of command to the Under Secretary of Defense for Intelligence (USD(I)). Units are responsible for coordinating with ACC/A3TV to ensure they acquire approved wireless routers, access points, tech support, software licenses, etc. Units not utilizing the AF CISP solution must attain their own approvals IAW DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*, AFI 17-130, *Cybersecurity Program Management,* and applicable DISA Wireless Security Technical Implementation Guide(s) (STIG(s)), and DoDM 5200.01V1_AFMAN16-1404V1, *Information Security Program: Overview, Classification, and Declassification.*

3.1.1.4. ***Commanders of units utilizing OMDs in-flight, may procure and authorize mounting solutions that are not permanently attached to the aircraft.***

3.1.1.5. Commanders of units utilizing OMD's in-flight may procure and authorize Anti-Glare and Night Vision Imagining System (NVIS) filters for their devices.

3.1.1.6. Commanders of units utilizing OMD's in-flight may procure and authorize battery life extenders if they do not connect to an aircraft power source, and they are properly tested IAW **paragraph 2.3**. Power solutions that connect to aircraft power will be approved by the MAJCOM/A3 in conjunction with the MDS SPO IAW AFMAN 11-202V3.

3.1.1.7. If approved for a particular aircraft, approved ADS-B IN devices will be listed on the CAF OMD Baseline Configuration document on the CAF OMD SharePoint®.

3.1.2. MDMS Requirements.

3.1.2.1. Configure MDMS systems to comply with approved DISA STIGs, ATO, and AF Policy.

3.1.2.2. After initial configuration of the MDMS, the only authorized network access is via the approved equipment identified in the CAF OMD Baseline Configuration for updates and content delivery. Ensure only personnel with a need to know, as determined by the unit commander, have an individual username and password established on the MDMS system. For purposes of this instruction, need to know is defined as an individual

who has been issued, configures, or maintains an OMD or the MDMS system and the data stored on either.

3.1.2.3. AFMAN 17-1304, all passwords will follow standard Air Force password requirements.

3.1.2.4. Remove an aircrew's username from the MDMS system once an aircrew leaves the squadron or no longer has a need-to-know within 30 days.

3.1.2.5. Admins are responsible for ensuring all patches and updates are applied to the MDMS as directed by CAF OMD PM. Any issues with updates or administration of the MDMS should be coordinated with the CAF OMD PM or the appropriately designated administrator.

3.1.2.6. The MDMS admins may be required to collect audit records and provides reports to the CAF OMD Program Office for review.

3.1.2.6.1. Audit records for the MDMS may include but are not limited to user Identification (ID), successful/unsuccessful logons, attempts to access security files, date/time/type of the event, success or failure of event, denial of access resulting from excessive number of logon attempts, blocking, or blacklisting a user ID, terminal, or access port, and the reason for the action.

3.1.2.6.2. Follow guidance of AFI 33-322, for audit records disposition.

3.1.3. If an approved remote management solution (e.g., MDM) is utilized for managing the MDMS devices, then the administrators of the management solution will assume the role of MDMS administrator.

3.1.4. Currency of Publications.

3.1.4.1. The user is responsible for ensuring all publications required for flight or in the performance of their duties are current, accessible, and viewable on their issued device prior to flight or conducting their job. Only publications required for flight or for the performance of one's duties are required to be current. Official publications not required for flight or in the performance of one's job duties are permitted on the OMD for reference purposes and are not required to be current.

3.1.4.2. Due to the length of time required to download significant publications updates and electronic flight information publication (eFLIP) databases, aircrew should update their devices as required prior to stepping to the aircraft or the performance of job duties.

3.1.4.3. If critical flight-related content is published while a crew is off-station, crews obtain the current content via any means necessary. If an approved Wi-Fi source is available, those updates can still proceed as normal. Non-critical information may be updated upon return to home-station.

3.1.4.4. The CAF OMD publications library (e.g., MCM) will be used by all units, unless a waiver is granted to individual units for operational reasons. Deployed units that do not have access to an approved Wi-Fi source will use their MDMS to update the content on their OMDs when able. The CAF OMD PM will maintain and update only current operations publications above the Wing level. **(T-3)** Publications are updated in real-time with information for newly assigned TO's, increments, revisions, changes, or supplements

from Enhanced Technical Information Management System (ETIMS). IAW Tasking Order (TO) 00-5-1, *AF Technical Order System*, paragraph 5.6.1, "If AF Portal connectivity problems prevent the updating of ETIMS eTOs on a primary eTool, any eTool updated within seven calendar days of the loss of connectivity will be considered current, as well as its synchronized secondary.".

3.1.4.5. For units utilizing the MAJCOM/A3 publications library, the currency of publications above WG level rests with the designated owner of that library. However, it is still the responsibility of the individual OMD user to synchronize their publications prior to the performance of their duties.

3.1.4.6. OGVs and CCVs will manage updated publications, manage local publications at or below the WG level in the CAF OMD publications library, and provide information on how to access the publications to their assigned aircrew.

3.1.4.6.1. When Wi-Fi is available, that will be the primary method to update publications per the appropriate paragraphs in this instruction. When an approved wireless solution is not available, OMD PM will download OMD- required electronic publications to an approved external Hard Disk Drive (HDD) or read only/re-writeable CD/DVD and manually transfer them to an MDMS computer These computers may be used to transfer the library to the OMD device for updating. AFMAN 17-1301, paragraph 4.4.3, all users must configure virus scanning frequency and real-time protection according to the applicable DISA STIG.

3.1.4.7. WG OMD PM ensures unit assigned OMDs only contain authorized documents and information, and proper authorization has been obtained from the data owners.

3.1.4.8. Organize OMD documents on the device IAW the applicable MAJCOM Stan/Eval office plan or IAW AFI 33-322, paragraph 4.6.2.

3.1.4.9. MDMS Computer Updates. Squadron OMD PM are responsible for keeping the electronic publications and eFLIP current on their unit MDMS computer(s). As electronic publications and eFLIP are changed or updated on the local drive, they will be downloaded to an approved external HDD or read only/re-writeable CD/DVD and then loaded onto the MDMS computer.

3.1.5. Care and handling of the OMD devices.

3.1.5.1. Each user issued an OMD device is responsible for its proper care and handling.

3.1.5.2. Users will not modify the OMD device from the MAJCOM-approved configuration **(T-2)**

3.1.5.3. Report any loss, theft, loss of functionality, display readability, or battery problems to a Squadron OMD PM. Consult DoD Financial Management Regulation (DoDFMR) 7000.14-R, Volume 12, Chapter 7, *Financial Liability for Government Property Lost, Damaged, Destroyed, or Stolen,* for guidance on determining liability. If the OMD is managed by an AF-EMM or MDM, then the Squadron OMD PM coordinates with the WG OMD PM who will contact the CAF OMD program office to attempt to locate the device. If it is determined that the device is lost, destroyed, or stolen, then the CAF OMD PM will conduct a remote wipe of the device.

3.1.5.4. WG OMD PM may contact the CAF OMD office for specific OMD maintenance concerns, not including hardware repair. Do not seek assistance with OMD maintenance issues from Communications Squadrons. Communications Squadron personnel are not funded, staffed, or trained to manage OMD maintenance issues.

3.1.5.5. WG OMD PM may contact the manufacturer for OMD device warranty service or accessory IAW DAFMAN 17-1203. If the warranty period has lapsed, or if the devices require repair for reasons not covered by the warranty, the unit is responsible for funding a replacement device or repair at a manufacturer-authorized service provider. The manufacturer-authorized service providers are typically found on the manufacturer website.

3.1.5.6. Tier 0 Support. Tier 0 support is what the user can do for themselves. If the device is a part of the CAF OMD program and controlled by the CAF OMD MDM, Tier 0 support may be possible and instructions for the user will be included on the CAF OMD SharePoint®.

3.1.5.7. Tier 1 Support. Tier 1 support is the support that the Squadron OMD PM can provide. If proper permissions have been granted to the Squadron OMD PM and are authorized to perform basic functions on the devices. In the absence of trained Squadron OMD PM, the CAF OMD office can provide this service and users are authorized to contact the CAF OMD office only after going through their OMD chain of command at the Squadron and WG.

3.1.5.8. Tier 2 Support. The CAF OMD office service provider provides tier 2 support. Tier 2 support should only be requested after exhausting all Tier 0 and Tier 1 support options.

3.1.5.9. Tier 3 Support. Tier 3 support is also provided by the CAF OMD Office service provider, although Tier 3 support requests must be mission critical. Users requesting Tier 3 support must have exhausted all Tier 0-2 support options or they must have an immediate mission requirement. In the case of an immediate mission requirement, the unit Commander's information must be supplied if asking for Tier 3 support.

3.1.6. Technology Refresh. IAW DAFMAN 17-1203, the technology refresh rate for OMDs is 4-years. However, OMDs may have a serviceable life beyond that period and the refresh rate is at the discretion of the unit Commander if circumstances warrant serviceable life of devices beyond 4-years. It is incumbent upon the Wing to develop a viable technology refresh plan that ensures devices are up to date.

3.1.6.1. Unless authorized directed by the CAF OMD office, each WG will completely refresh their OMD hardware with appropriately National Institute of Standards and Technology (NIST) certified IT every 4-years or sooner to ensure compliance with updates and operating system changes **(T-2)** The WG plan may call for a full set of new OMD devices every 4- years or partial technology refreshes during that 4-year period (i.e., 25% every year or 50% the devices every 2 years). Route this WG budget in the same manner as the rest of their annual budget.

3.1.6.2. When accomplishing technology refreshes, chances are that the old OMDs could be repurposed versus turning them into Defense Reutilization and Marketing Office (DRMO)/Defense Logistics Agency (DLA) Disposition Services.

3.1.7. MDM. To reduce the workload associated with OMD program management, the CAF OMD program office may leverage MDM capabilities to units. **(T-2)** Ensure the Squadron OMD PM and a designated alternate, at a minimum, are trained on OMD MDM requirements, and obtain appropriate training and appropriate rights through the CAF OMD office. Upon MDM implementation, instructions and information will be published on the CAF OMD SharePoint. MDM functions may include:

3.1.7.1. Configuration Control.

3.1.7.2. Operating System and Application Updates.

3.1.7.3. Device Provisioning.

3.1.7.4. Enforcement of Security Policy.

3.1.7.5. Device Auditing.

3.1.7.6. Content Management, including distribution and updating of electronic publications.

3.1.7.7. Access to the DoD, AF, or CAF approved Mobile Application Store.

3.1.8. Reduction of Paper. Once units have fully implemented their OMD program, reduction of paper is fully authorized when the data is available digitally on the OMD device. This includes approval for OMD use during all phases of flight, or as restricted by other provisions of this instruction, or as restricted by local supplements to this instruction.

3.1.8.1. Units establish new Initial Distribution (ID) requirements with their TODO for all applicable flight manuals and technical orders to reduce the paper being printed and distributed to the unit.

3.2. Security Policy and Use.

3.2.1. Security Policy. Any unit who operates their OMDs in more restrictive ways than directed by this ACCI will include those procedures in their unit supplement to this instruction.

3.2.2. CPA. This publication does not give permission for OMDs to enter any classified ground facility. To meet mission requirements, OMDs should be permitted within certain CPAs. Examples include aircrew mission planning facilities, aircraft, simulators, and WST. WG OMD PM are responsible for identifying CPAs where OMD use is required if not already approved by the MAJCOM and coordinating the local approvals and policies necessary to enable OMD operations in these environments in addition to any MAJCOM or Headquarters Air Force (HAF) guidance or approvals.

3.2.2.1. Any MAJCOM approval letters will be located on the CAF OMD SharePoint®.

3.2.2.2. ACC policy on OMD use in CPAs does not apply to non-ACC owned facilities (e.g., Andersen AFB or deployed locations). The owning MAJCOM must grant approval.

3.2.2.3. Do not attempt to introduce an OMD into a CPA until specific authorization for that CPA is published by the MAJCOM or local security office. Consult the responsible security manager if unsure whether this authorization has been obtained. If in doubt, do not bring the OMD into the CPA.

3.2.2.4. If OMDs are approved for entry into classified facilities, units will follow the local security checklist when bringing OMD devices into a CPA and upon exiting the facility.

3.2.3. Configuration.

3.2.3.1. WG OMD PM are responsible for ensuring devices are setup and configured as specified in this instruction. Passcodes for devices will be IAW CAF OMD direction.

3.2.3.2. MDM settings will be IAW HAF, CAF, and other directives unless a waiver has been granted for a local unit to maintain their own OMD program. **(T-2)**

3.2.3.3. Updates to configuration will either be pushed via the MDM or directed by the CAF OMD office via email, SharePoint® notices, or FCIF.

3.2.3.4. Applications installed on OMD devices will be IAW this document and listed in the CAF OMD Baseline Configuration. If a local unit has a waiver to operate their own OMD program, their list of approved applications will be included in that waiver and kept updated on the CAF OMD SharePoint®. **(T-2)**

3.2.3.5. OMD Camera and Microphone. If brought into flight or CPAs, OMDs will have their camera and microphone disabled cameras will be always covered unless authorized by waiver by CAF OMD program office. **(T-2)**

3.2.4. Device Issue and User Agreement Requirements. OMD PMs may download the User Agreements and other documents applicable to OMD device issue from the CAF OMD SharePoint® Site.

3.2.4.1. Ensure each member using a device signs the DAF Form 4433 after receiving required training, and before being issued an OMD device.

3.2.4.2. User Agreements will be maintained by the unit on-file for two years following the date the user signed in which a new user agreement will be required. Digital copies are acceptable.

3.2.4.3. All personnel issued a device will have a DAF Form 1297 completed, signed by user, and will be maintained by issuing OMD PM.

3.2.4.4. Appropriate classification label is required on every OMD device IAW DoDM 5200.01V2_AFMAN16-1404V2, *Information Security Program: Marking of Information,* and AFI 17-130.

3.2.5. Device Performance. During use, personnel will verify the device is performing as expected and configured IAW the MAJCOM-approved baseline configuration, and FCIF notifications. This includes, but is not limited to:

3.2.5.1. Appropriate connectivity icons are displayed based on guidance in this instruction and applicable to the environment where the devices are being operated (e.g., Airplane icon when airplane mode is required, Wi-Fi icon on when Wi-Fi connectivity is authorized and required).

3.2.5.2. Bluetooth is not authorized and to be disabled. Bluetooth icon is to remain disabled unless authorized through CAF OMD program office waiver process.

3.2.5.3. Verify that no device features are operating autonomously, such as the camera, or applications activating without user input.

3.2.5.4. **Note:** and report any unapproved or unexpected application icons appearing on the device. to the CAF OMD program office org box at ACC/A3TV CAF Operations Mobile Devices **ACC.A5A3.EFB@us.af.mil**.

3.2.6. Classified Message Incidents (CMIs) and Cybersecurity Incidents. In the event of a CMI or cybersecurity incident involving an OMD:

3.2.6.1. Individuals will immediately contact their Security Manager and WG Information Assurance Manager (IAM). In most cases, the WG IAM can be reached by contacting the local Communications Focal Point (CFP).

3.2.6.2. Place the device in question in a secure container until the Security Manager and/or WG IAM can take possession of the device. Remove connection to Wi-Fi or the MDMS and keep the device powered on if possible. This is to allow forensic examination of the device and to prevent loss of evidence caused by powering off device.

3.2.6.3. Standard practices and policies for identifying and remediating a CMI or cybersecurity incident will be conducted IAW local guidance.

3.2.7. Physical and Environmental Considerations. The OMD system requires the same physical and environmental conditions as those provided to standard administrative desktop/laptop resources.

3.2.8. Emergency Device Destruction. In the event of an isolating event, such as ejection or a forced/emergency landing into hostile territory, crews should destroy devices by an effective means available only after securing or destroying any classified material on-board the aircraft. This can include erasing the data or physically destroying the device.

3.3. Limitations.

3.3.1. Battery Limitations. Prior to flight, make every effort to fully charge the device. AMD device battery levels must have 10% for each hour of planned total flight time plus sufficient time for engine start, taxi, and shutdown, but not less than 50%. Aircraft commanders and individual aircrew are responsible for ensuring that battery charge is sufficient to meet mission requirements. Aircraft power may only be used to power/charge OMD devices if the power supply has been certified by the applicable MDS SPO. The CAF OMD office will maintain a listing of any approved in-flight power supplies on the CAF OMD SharePoint®.

3.3.2. Use of Wireless.

3.3.2.1. Authorized Wireless connections for UNCLASSIFIED OMDs

3.3.2.1.1. Primary connection method should be utilizing the approved AF CISP solution. Identified on the CAF OMD Baseline Configurations.

3.3.2.1.2. Secondary connection method is utilizing a trusted, secure wireless network configured with WPA2 security. Secondary connection method is only authorized if/when the primary connection is not available and Internet connection is necessary.

3.3.2.1.3. Connecting to unsecure “open” wireless networks, such as those found in retail establishments and airports, is only as a last resort. Mission commanders, aircraft commanders, aircrew, etc., must perform a risk assessment before connecting to an unsecure wireless network. Connections must be limited to critical data/document updates and disconnected as quickly as possible.

3.3.2.2. CLASSIFIED OMDs wired and wireless connections will be at the direction of the CAF OMD office.

3.3.2.3. All Government-owned networking equipment procured for OMD support will comply with relevant AF guidance.

3.3.2.4. If OMDs are authorized within designated CPAs, users will abide by the approved checklist for entry into these spaces. Appropriate local security team for (e.g., WG Information Security System Security Manager (ISSM)/Information Protection (IP), SSO or SAP ISSM) will identify what policies and procedures are required for entry into applicable CPA. For OMDs taken into flight, unless specifically authorized by ACC/A3 and listed on the current CAF OMD Baseline Configuration, disable wireless connectivity services by placing the device in "Airplane Mode – ON, Wireless – OFF, Bluetooth – OFF" from the settings menu prior to takeoff and keep them disabled until after landing.

3.3.2.5. Applications will not be downloaded, installed, deleted, modified, or updated while off station, unless connected to a secure wireless network IAW this section.

3.3.3. In-Flight Back-Up Requirements. If operating without paper back-ups, the following restrictions apply as a baseline **(T-2)** Unit Commanders may choose to equip more crew positions with eFLIP readers as required:

3.3.3.1. A-10: Two OMDs total in cockpit.

3.3.3.2. E-3: One OMD per primary occupied crew position. Only pilots, flight engineers, and navigators require an eFLIP reader installed on their device.

3.3.3.3. E-9: One OMD per primary occupied crew position. Only pilots and navigators require an eFLIP reader installed on their device.

3.3.3.4. E-11: One OMD per primary occupied crew position.

3.3.3.5. F-15E/X: Two OMDs total in cockpit. Weapons System Officer (WSO) require eFlip reader installed on their device.

3.3.3.6. F-15C: Two OMDs total in cockpit.

3.3.3.7. F-16: Two OMDs total in cockpit.

3.3.3.8. F-22: Two OMDs total in cockpit.

3.3.3.9. F-35: Two OMDs total in cockpit.

3.3.3.10. EC-130H: One OMD per primary occupied crew position. Only pilots, flight engineers, and navigators require an eFLIP reader installed on their device.

3.3.3.11. HC-130J/P: One OMD per primary occupied crew position. Only pilots, flight engineers (if a part of the crew), and Combat Systems Operators (CSOs)/navigators require an eFLIP reader installed on their device.

3.3.3.12. HH-60: One OMD per primary occupied crew position. Only pilots require an eFLIP reader installed on their device, but the Special Mission Aviators (SMAs) may have one installed per unit Commander's discretion.

3.3.3.13. XC-135: One OMD per primary occupied crew position. Only pilots and navigators require an eFLIP reader installed on their device.

3.3.3.14. T-38: Two OMDs total in cockpit.

3.3.3.15. U-2: Two OMDs total in cockpit.

3.3.3.16. MQ-9: Two OMDs total (Pilot and Sensor Operator) Only pilots, Sensor Operator require eFLIP reader installed on their device.

3.3.4. Nuclear Alert and Operations. Aircrews conducting real-world nuclear alert duty or nuclear operations may use OMD but will have all required TOs and directives onboard the aircraft in paper format. **(T-3)** This paragraph does not apply to nuclear training missions. Flight data (i.e., screen captures, GPS trails, and flight plans) during actual nuclear alert and operations will not be recorded. **(T-3)**

3.3.5. Screen Auto Lock Requirements.

3.3.5.1. Set mobile device screen auto lock to 15 minutes except during flight operations. For OMDs, upon entering the aircraft, the user may set the auto lock feature to "Never" under device settings. Upon exiting the aircraft, the user sets auto lock back to 15 minutes. Failing to do so will constitute a cybersecurity violation.

3.3.5.2. When Auto-Lock is set to "Never," the device may remain "awake" with the screen ON until the user toggles the power button, which could result in excessive battery drain.

3.3.6. Own-Ship Position. Aircrews will not use OMD display of own-ship position and moving map (if equipped) as a primary means of navigation and are used as a reference only. These tools, if available, will be used only as an aid to situational awareness. During real world and combat operations, flight data (i.e., screen captures, GPS trails, and flight plans) will not be recorded. **(T-3)**

3.3.7. Weather Display. Aircrew will not use OMD display of weather data in-flight (if equipped) as a primary means of weather avoidance. Weather data obtained from off-board sources may be outdated due to delays caused by refresh rates and limitations inherent in the system transmitting the data. Experience has shown that weather depictions of this type can be up to 20 minutes old but should be refreshed every 10-minutes by the FAA. Therefore, weather data that may be available on the OMD will be used only as an aid to situational awareness.

3.4. Training.

3.4.1. General. Units will provide aircrew OMD training prior to initial in-flight or workspace use as directed by the CAF OMD office.

3.4.2. Minimum requirements. Demonstration of publications access/update, navigation of device and each approved application, procedures in case of device/app failure, basic battery conservation techniques, using/updating device Apps and operating system, and security practices to protect against sensitive data loss.

3.4.3. Currency OMD PMs may be required to attend initial/reoccurring training provided by the CAF OMD office. At a minimum, users are required to complete the DISA Using Mobile Devices in a DoD Environment on an annual basis.

3.4.4. Training Resources. CAF OMD training slides are available on the CAF OMD SharePoint®. Units may modify this training to suit local requirements and ensure compliance with **paragraph 3.5.1**.

3.5. Flight Operations.

3.5.1. Use In-Flight. Pilot OMDs will be securely mounted (which includes kneeboards) and viewable during takeoff, traffic pattern activity, approach, and landing, or positioned so as not to create a hazard during these phases of flight. Mounting locations, if applicable, will be selected so as not to impede flight controls in any way, and will not obstruct the pilot's view in front of the aircraft. Other crew positions (e.g., Navigators, Electronic Warfare Officers, and Special Mission Operators) may also employ OMD mounts. A listing of approved mounting solutions will be maintained on the CAF OMD SharePoint®. During all phases of flight, aircrew will ensure OMD devices are mounted, positioned, or stowed so as not to impede any required flight-related equipment, or otherwise create a hazard.

3.5.1.1. OMDs are approved for use during all phases of flight, to include operations below 10,000' MSL.

3.5.1.2. Units are authorized paperless in-flight operations as discussed in this instruction.

3.5.1.3. When encountering turbulence, PIC ensure that OMDs are either secured to a kneeboard, secured in an approved OMD mount, or stowed away to prevent the devices from falling around in the aircraft and becoming damaged.

3.5.2. Night Operations. Set device back lighting to have minimum impact on night vision during night operations. NVDs OMD screen filters are approved for use in flight.

3.5.3. Commanders are authorized to procure and utilize any NVIS filters that meet MIL-STD 3009, *Lighting, Aircraft, Night Vision Imaging System (NVIS) Compatible* OMD Audio. Set OMD devices capable of audio, if applicable, at a volume that will not interfere with aircraft communications or normal crew duties.

3.5.4. Screen Protectors, Anti-Glare Filters, and Protective Cases. Screen protectors, Anti-Glare filters, and protective cases are authorized if they do not affect the functionality of the devices or preclude use of authorized aircraft mounting solutions.

3.5.5. ADS-B IN devices are approved for use as directed on the CAF OMD Baseline Configuration:

3.5.5.1. Units will establish check-out and check-in procedures for ADS-B IN devices and include that in their unit supplement. **(T-3)**

3.5.5.2. Units should establish a standard location to mount ADS-B IN devices for their unit based off SPO guidance. **(T-3)**

3.5.5.3. Units will develop egress procedures when ADS-B IN devices are installed if not already incorporated in SPO guidance. **(T-3)**

3.6. Abnormal and Emergency Procedures.

3.6.1. Egress. Stow OMD prior to ejection or ground egress if time and conditions permit. Ejecting or ground egressing the aircraft with the device attached to the aircrew's body increases the risk of injury. Aircrews ensure that their mounting equipment (e.g., kneeboard or suction cup mount) is serviceable prior to flight and that they are aware of the stowage procedures in the event of an egress situation.

3.6.2. Device Failure.

3.6.2.1. If a device fails prior to initial departure, the crew will attempt to obtain a replacement device if there is not already a replacement on board the aircraft. Obtain a spare from the unit OMD PM, operations duty officer, or squadron duty officer. Verify that the operating system, configuration, publications, and Flight Information Publications (FLIP) versions are all current. If no replacement is available, PICs direct distribution of the remaining OMDs backup devices as appropriate or ensure paper publications are available. The PIC will exercise sound judgment to evaluate the risks associated with continued operations after the failure of a device.

3.6.2.2. In the event an aircrew device fails in flight, PICs will manage other aircrew OMD devices and/or spares (as applicable) to minimize aircrew workload, maximize situational awareness and Crew/Cockpit Resource Management (CRM), and maintain safety of flight. In the event of a complete loss of all AMDs on an aircraft, the PIC should land as soon as practical if no paper backups exist. **(T-3)**

3.6.2.3. At enroute stops, PICs may direct distribution of the remaining OMD backup devices as appropriate to minimize crew workload, maximize situational awareness and CRM, and maintain safety of flight. The PIC will exercise sound judgment to evaluate the risks associated with continued operations after the failure of devices.

3.6.3. Disaster Recovery.

3.6.3.1. In the event of a complete loss of information on the OMDs and MDMS system, a restore will need to be accomplished contact appointed Squadron/WG/CAF OMD PM for directions on restoring device.

3.6.3.2. In the event of a complete loss of information on the OMDs, MDMS system, and SharePoint, a system restore will be accomplished in the following manner.

3.6.3.2.1. MDMS administrators will restore the MDMS system utilizing the weekly backup as identified in **paragraph 3.3.3**.

3.6.3.2.2. OMD and MDMS systems will be restored using information from another location.

3.6.3.3. External HDDs or CD/DVD must contain a current copy (within 7 days) of all software, configurations, data, and profiles required to accomplish a complete restoration of both systems OMD and MDMS.

3.6.3.4. Each unit will maintain at least a Primary MDMS system in the event of catastrophic system failure, and to ensure quick system recovery. Recommend that units also have an alternate MDMS system as a backup. Decision for an alternate rest with the unit Commander.

3.6.3.5. In the event of catastrophic failure of the OMD, use the External HDD/CD/DVD backup files and the MDMS to restore the device to its original configuration.

3.6.3.6. In the event of primary system failure, the alternate system will become the primary. To restore the failed MDMS, first perform a wipe of the device and then restore it to its factory settings. Update all software on the device.

DAVID G. SHOEMAKER, Major General, USAF
Director of Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

14 CFR § 121.542, *Flight Crew Duties*

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

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

AFMAN 11-202V3, *Flight Operations*, 10 January 2022

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

AFPD 11-2, *Aircrew Operations*, 31 January 2019

DAFI 90-302, *The Inspection System of the Department of the Air Force*, 15 March 2023

DAFMAN 17-1203, *Information Technology Asset Management (ITAM) and Accountability*, 13 September 2022

DAFMAN 90-161, *Publishing Processes and Procedures*, 18 October 2023

DAFPD 10-9, *Lead Command/Lead Agent Designation and Responsibilities for the United States Air Force Weapons System, Non-Weapon Systems, and Activities*, 25 May 2021

DoDFMR 7000.14-RV12, Chapter 7, *Financial Liability for Government Property Lost, Damaged, Destroyed, or Stolen,* January 2021

DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*, 3 November 2017

DoDM 5200.01V1_AFMAN16-1404V1, *Information Security Program: Overview, Classification, and Declassification*, 6 April 2022

DoDM 5200.01V2_AFMAN16-1404V2, *Information Security Program: Marking of Information*, 7 January 2021

FAA AC 120-76D, *Authorization for Use of Electronic Flight Bags*, 27 October 2017

MIL-STD 3009, *Lighting, Aircraft, Night Vision Imaging System (NVIS) Compatible*, 2 February 2001

RTCA/DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*, 1 December 1992

TO 00-5-1, *AF Technical Order System*, 15 January 2013,

Prescribed Forms

None

Adopted Forms

AF Form 1768, *Staff Summary Sheet*

AF Form 4169, *Request for Waiver from Information Assurance Criteria*

DAF Form 679, *Department of the Air Force Publication Compliance Item Area Waiver Request/Approval*

DAF Form 847, *Recommendation for Change of Publication*

DAF Form 1297, *Temporary Issue Receipt*

DAF Form 4433, *Department of the Air Force Mobile Device User Agreement*

Abbreviations and Acronyms

ACC—Air Combat Command

ACCI—Air Combat Command Instruction

ADS-B—Automatic Dependent Surveillance Broadcast

ADS-B IN—Automatic Dependent Surveillance Broadcast-In

AETC—Air Education and Training Command

AFB—Air Force Base

AFE—Aircrew Flight Equipment

AFI—Air Force Instruction

AFLCMC—Air Force Life Cycle Management Center

AFMAN—Air Force Manual

AFMC—Air Force Material Command

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFSOC—Air Force Special Operations Command

AMIC—Acquisition Management and Integration Center

ANG—Air National Guard

AO—Authorizing Official

App—Application

ATO—Authority to Operate

BECO—Base Equipment Custodian Officer

Blvd—Boulevard

CAF—Combat Air Forces

CBT—Computer Based Training

CCV—Squadron Stan/Eval

CD—Compact Disc

CFP—Communications Focal Point

CISP—Commercial Internet Service Provider

CMI—Classified Message Incident

COMPUSEC—Computer Security

COMSEC—Communication Security

CONOPS—Concept of Operations

COTS—Commercial Off-The-Shelf

CPA—Classified Processing Area

CRM—Crew Resource Management

CSA—Client Support Administrator

CSO—Combat Systems Operator

CUI—Controlled Unclassified Information

DAA—Designated Approval Authority

DAF—Department of the Air Force

DAFPD—Department of the Air Force Policy Directive

DAFI—Department of the Air Force Instruction

DAFMAN—Department of the Air Force Manual

DISA—Defense Information Systems Agency

DLA—Defense Logistics Agency

DoD—Department of Defense

DoDFMR—Department of Defense Financial Management Regulation

DoDI—Department of Defense Instruction

DoDIN—DoD Information Network

DoDM—Department of Defense Manual

DRMO—Defense Reutilization and Marketing Office

DSN—Defense Switched Network

DVD—Digital Video Disc

ECO—Equipment Custodian Officer

EFB—Electronic Flight Bag

eFLIP—Electronic Flight Information Publications

EKB—Electronic Knee Board

EMI—Electro Magnetic Interference

EMM—Enterprise Mobile Management

EMSEC—Emission Security

EPUBS—Electronic Publications

ETIMS—Enhanced Technical Information Management System

eTO—Electronic Technical Order

FAA—Federal Aviation Administration

FAM—Functional Area Manager

FCIF—Flight Crew Information File

FLIP—Flight Information Publications

FOC—Full Operational Capability

GIG—Global Information Grid

GPC—Government Purchase Card

GPS—Global Positioning System

GSU—Geographically Separated Unit

HAF—Headquarters Air Force

HDD—Hard Disk Drive

HERO—Hazards of Electromagnetic Radiation to Ordinance

HHQ—Higher Headquarters

HQ—Headquarters

IA—Information Assurance

IAM—Information Assurance Manager

IATT—Interim Authority to Test

IAW—In Accordance With

ICU—iPhone Configuration Utility

ID—Identification

ID—Initial Distribution

IOC—Initial Operational Capability

IP—Information Protection

ISSM—Information System Security Manager

ISSO—Information System Security Officer

IT—Information Technology

ITAM/AIM—Air Force Information Technology Asset Management

ITEC—Information Technology Equipment Custodian

MAJCOM—Major Command

MAM—Mobile Application Management

MCM—Mobile Content Management

MCSL—Mobile Cybersecurity Liaison

MDM—Mobile Device Management

MDMS—Mobile Device Management System

MDS—Mission Design Series

MFR—Memorandum for Record / Military Flight Release

MSL—Mean Sea Level

NGB—National Guard Bureau

NIST—National Institute of Standards and Technology

NVD—Night Vision Devices

NVIS—Night Vision Imagining System

OG/CC—Operations Group Commander

OGV—Operations Group Stan/Eval

OMD—Operations Mobile Device

OPR—Office of Primary Responsibility

OSS—Operational Support Squadron

PACAF—Pacific Air Forces

PCS—Permanent Change of Station

PED—Portable Electronic Device

PEM—Program Element Monitor

PIC—Pilot in Command

PIP—Product Improvement Program

PM—Program Manager

PMO—Program Management Office

PUB—Publication

SAP—Special Access Program

SAPF—Special Access Program Facility

SAPMO—Special Access Program Management Office

SCI—Sensitive Compartmentalized Information

SCIF—Sensitive Compartmentalized Information Facility

SDC—Standard Desktop Configuration

SEB—Standard and Evaluation Board

SMA—Special Mission Aviators

SMP—System Management Plan

SPO—System Program Office

SQ/CC—Squadron Commander

SSO—Special Security Office

SSS—Staff Summary Sheet

Stan/Eval—Standardization and Evaluation

STC—Supplemental Type Certificate

STF—Safe To Fly

STIG—Security Technical Implementation Guide

TC—Type Certificate

TDY—Temporary Duty

TFI—Total Force Integration

TO—Technical Order

TODA—Technical Order Distribution Account

TODO—Technical Order Distribution Officer

TOLD—Takeoff and Landing Data

TS—Top Secret

TTP—Tactics, Techniques, and Procedures

UCNI—Unclassified Controlled Nuclear Information

USAF—United States Air Force

USAFE-AFAFRICA—United States Air Forces Europe-Air Forces Africia

VA—Virginia

VMC—Visual Meteorological Conditions

WG—Wing

WG/CC—Wing Commander

WLAN—Wireless Local-Area Network

WSO—Weapons System Office

WST—Weapon System Trainer or Team

Office Symbols

ACC/A3—ACC Director of Operations

ACC/A35—ACC Future Operations Division

ACC/A3R—ACC Resource and Budget Division

ACC/A3T—ACC Flight Operations Division

ACC/A3TO—ACC Flight Operations and Training Branch

ACC/A3TV—ACC Standardization and Evaluation

ACC/A5—ACC Directorate of Requirements

ACC/A5/8/9—Directorate of Plans, Programs and Requirement

ACC/A5/8Z—CAF SAPMO Security and Policy Division

ACC/A6—ACC Communications Directorate

ACC/AMIC—ACC Acquisition Management and Integration Center

ACC/FM—ACC Comptroller

ACC/JA—ACC Judge Advocate

ACC/PA—ACC Public Affairs

ACC/SE—ACC Chief of Safety

AFLCMC/WNU—Air Force Life Cycle Management Center Air Force Uniform Office (Human Systems Division)

SAF/CN—Chief Information Officer

USD(I)—Under Secretary of Defense for Intelligence

Terms

Class 1 Electronic Flight Bag (EFB) Hardware—Portable commercial off-the-shelf (COTS)-based computers, considered to be portable electronic devices (PED) with no aircraft manufacturer and/or SPO design, production, or installation approval for the device and its internal components. Class 1 EFBs are not mounted to the aircraft, connected to aircraft systems for data, or connected to a dedicated aircraft power supply. Class 1 EFBs can be temporarily connected to an existing aircraft power supply for battery recharging. Class 1 EFBs that have Type B applications for aeronautical charts, approach charts, or an electronic checklist must be appropriately secured and viewable during critical phases of flight and must not interfere with flight control movement. (**Note:** Portable Class 1 EFB components are not considered to be part of aircraft type design, i.e., not in the aircraft type certificate (TC) or Supplemental Type Certificate (STC).) (FAA AC 120-76D, *Authorization for Use of Electronic Flight Bags*)

Class 2 EFB Hardware—Portable COTS-based computers, considered to be personal electronic devices with no aircraft manufacturer and/or SPO design, production, or installation approval for the device and its internal components. Class 2 EFBs are typically mounted. They must be capable of being easily removed from or attached to their mounts by flight-crew personnel. Class 2 EFBs can be temporarily connected to an existing aircraft power supply for battery recharging. They

may connect to aircraft power, data ports (wired or wireless), or installed antennas, provided those connections are installed in accordance with aircraft manufacturer or SPO guidelines. (Note: Portable Class 2 EFB components are not considered to be part of aircraft design.) (FAA AC 120-76D)

Class 3 EFB Hardware—EFBs permanently installed in the aircraft in accordance with applicable airworthiness regulations. (FAA AC 120-76D)

Critical Phases of Flight—Includes all ground operations involving taxi, takeoff, and landing, and all other flight operations conducted below 10,000 feet, except cruise flight. (Title 14, Code of Federal Regulations, Section 121.542, *Flight Crew Duties*).

Electronic Flight Bag (EFB)—An electronic display system intended primarily for flight deck use that includes the hardware and software necessary to support an intended function. EFB devices can display a variety of aviation data or perform basic calculations (e.g., performance data, fuel calculations, etc.). In the past, some of these functions were traditionally accomplished using paper references or were based on data provided to the flight-crew by a flight dispatch function. The scope of the EFB functionality may include various other hosted databases and applications. Physical EFB displays may use various technologies, formats, and forms of communication. An EFB must be able to host Type A and/or Type B software applications. (FAA AC 120-76D)

Hosted Application—Software running on an OMD that is not installed or considered part of aircraft type design. (FAA AC 120-76D)

Interactive Information—Information presented on the OMD that, via software applications, can be selected and rendered in a number of dynamic ways. This includes variables in the information presented based on data-oriented software algorithms, concepts of decluttering, and selectable composition as opposed to pre-composed information. (FAA AC 120-76D)

Mounted—Any portable device that is attached to a permanently installed mounting device. (FAA AC 120-76D)

Mounting Device—These include arm-mounted, cradle, clips, docking stations, etc. (FAA AC 120-76D)

Stowed—A portable device that is placed in a secure stowage location but is not available for use or view by the pilot in that location. (FAA AC 120-76D)

Type A Software Applications—Type A applications are those paper replacement applications primarily intended for use during flight planning, on the ground, or during noncritical phases of flight having a failure condition classification considered to be a minor hazard or less. (FAA AC 120-76D)

Type B Software Applications—Type B applications are those paper replacement applications that provide the aeronautical information required to be accessible for each flight at the pilot station and are primarily intended for use during flight planning and all phases of flight. Type B applications include miscellaneous, non-required applications (e.g., aircraft cabin and exterior surveillance video displays, maintenance applications) having a failure condition classification considered to be a minor hazard or less. (FAA AC 120-76D)

Type C Software Applications—Software approved using RTCA/DO-178B, December 1, 1992, *Software Considerations in Airborne Systems and Equipment Certification* compliance or another acceptable means. These are non-OMD software applications found in avionics and include

intended functions for communications, navigation, and surveillance that require aircraft manufacturer and/or SPO design, production, and installation approval. Type C applications are for airborne functions with a failure condition classification considered to be a major hazard or higher. (FAA AC 120-76D)

Viewable Stowage—A portable device that is secured in an existing provision with the intended function to hold charts or acceptable temporarily secured portable device viewable to the pilot (e.g., kneeboards, suction cups, etc.) (FAA AC 120-76D)