COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

This instruction implements AFPD 11-2, *Aircrew Operations*, and prescribes procedures for Operations Mobile Device (OMD) program implementation, execution, and sustainment. This instruction applies to all Air Force Reserve Command and AFRC Total Force Integration flying units that maintain a reserve association with active duty flying units. It does not apply to the United States Space Force or Air National Guard. 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 of IAW the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes to this publication to Headquarters Air Force Reserve Command Standardization and Evaluation (AFRC/A3MV) at **HQAFRC.A3RM.WORKFLOW@us.af.mil**, 555 Robins Parkway, Robins AFB, GA 31098, DSN 497-0483, using the DAF Form 847, *Recommendation for Change of Publication*. Route DAF Forms 847 from the field through the appropriate Standardization and Evaluation chain of command. This publication may be supplemented at any level, but all direct supplements must be routed to the OPR of this publication for coordination prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Submit requests for waivers in accordance with **paragraph 1.3** 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 Air Force.

Chapter 1

GENERAL INFORMATION

1.1. Purpose.

1.1.1. This instruction provides directive guidance on the Air Force Reserve Command Operations Mobile Device (OMD) program to include its development, processes, operation, procurement, and employment. Failure to follow AFRC OMD guidance contained in this instruction or applicable Air Force and Department of Defense regulations may result in administrative or disciplinary action as determined by the commander.

1.1.2. The OMD program is a sub-set of the Mission Mobile Device program that includes devices utilized by Maintenance Groups and Mission Support Groups.

1.1.3. Electronic Flight Bag (EFB) is a function performed by the OMD. The EFB function consists of downloading, storing, and displaying of electronic publications, electronic Take Off and Landing Data apps, electronic Flight Information Publications, and other approved flight related apps.

1.1.4. The part-time nature of the AFRC workforce drives an additional requirement to have access to productivity apps even when dislocated from the unit. AFRC/A3RM works in partnership with AFRC/A6 and AFRC/A4 to provide a device with as much capability as possible while maintaining a mission first focus.

1.2. Roles and Responsibilities.

1.2.1. AFRC/A3: Will provide overall guidance for the operational requirement and use of AFRC OMDs.

1.2.1.1. AFRC/A3RM: Will serve as the overall program OPR for the AFRC OMD Program and will designate a MAJCOM-level OMD Program Manager and alternate OMD Program Manager.

1.2.1.1.1. Will maintain an AFRC Operations Mobile Device Teams™ and SharePoint™ site. These locations will serve as the primary focal points for the latest information, policy, and guidance affecting the AFRC OMD Program.

1.2.1.1.2. Will establish program baselines and coordinate requirements with AFRC/A3MV, AFRC/A3DV, and AFRC/A3J, along with AFRC/A3 Functional Area Managers (FAMs).

1.2.1.1.3. Will ensure compliance with the Air Force Commercial Internet Service Provider solution IAW the SAF CIO DoDIN Waiver. In addition, AFRC/A3RM will coordinate with lead command and other participating MAJCOMs to maintain an approved Commercial Internet Service Provider solution.

1.2.1.1.4. Will develop and field mobile device training material. This training material will be located on the AFRC OMD Program Teams™/SharePoint™ sites.

1.2.1.1.5. Will maintain a process to verify all documents are approved for electronic distribution and are IAW AFI 11-215, *Flight Manuals Program,* TO 00-5-1, *Air Force Technical Order System*, and 31S5-4-ETool-1, *ETool Setup and Management.*

AFRC/A3RM will maintain a distribution method to provide publications to aircrew in a timely manner.

1.2.1.1.6. Will develop and maintain lifecycle plan including funding, procurement, sustainment, and retirement for OMDs.

1.2.1.1.7. Will develop and maintain agreements with support agencies to assist OMD users and Device Managers.

1.2.1.2. AFRC/A3MV: Will retain primary responsibility for establishing AFRC Mobility Air Forces application and publication baselines and coordinate these requirements through AFRC/A3RM. AFRC/A3MV should coordinate with the applicable AFRC/A3 FAMs to ensure accurate requirement information.

1.2.1.3. AFRC/A3DV: Will retain primary responsibility for establishing AFRC Combat Air Forces application and publication baselines and coordinate these requirements through AFRC/A3RM. AFRC/A3DV should coordinate with the applicable AFRC/A3 FAMs to ensure accurate requirement information.

1.2.1.4. AFRC/A3J: Will retain primary responsibility for establishing AFRC Special Operations Forces application and publication baselines and coordinate these requirements through AFRC/A3RM. AFRC/A3J should coordinate with the applicable AFRC/A3 FAMs to ensure accurate requirement information.

1.2.1.5. AFRC FAMs: Will validate all requirements pertaining to their area of responsibility. AFRC FAMs will assist AFRC/A3RM in development and maintenance of Program Objective Memorandum papers to accurately reflect requirement and funding requests.

1.2.2. NAF/A3: Will designate NAF OMD managers (minimum 1 primary and 1 alternate) and submit documentation of appointment to AFRC/A3RM. Appointed device managers will be responsible for maintaining NAF staff OMDs.

1.2.2.1. NAF/A3V: Will ensure NAF level oversight, advocacy, and support for the EFB functionality of OMDs.

1.2.3. Operations Group Commander (OG/CC): Will designate OMD managers (minimum 1 primary and 1 alternate) and submit documentation of this to AFRC/A3RM. May be delegated to Sq/CC if individual squadrons are to provide device managers.

1.2.3.1. OG/OGV: Will ensure OG level oversight, advocacy, and support for the EFB functionality of OMDs.

1.2.4. Unit Commanders: May designate OMD managers (minimum 1 primary and 1 alternate) and submit documentation of appointment to AFRC/A3RM.

1.2.5. OG/Unit OMD managers: Maintain overall responsibility for the Unit OMD program as follows:

1.2.5.1. Identify, address, and elevate (as necessary), OMD requirements and concerns to Unit leadership, the OG OMD manager, the NAF OMD manager, and the AFRC OMD program manager.

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

1.2.5.3. Coordinate with Technical Order Distribution Officers 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 publication.

1.2.5.4. Provide feedback on operational usability of OMD.

1.2.5.5. Assist in setup, maintenance, restoration, and disposition of OMDs to include:

1.2.5.5.1. Device/App unlock.

1.2.5.5.2. Device/App password resets.

1.2.5.5.3. Device wipes.

1.2.5.5.4. Device activations.

1.2.5.5.5. Manage lost mode.

1.2.5.5.6. Device enrollments.

1.2.5.5.7. Device/User derived Purebred credentials.

1.2.5.5.8. Device offboarding and turn-in.

1.2.5.6. Perform all setup, maintenance, and restoration functions on Exclusive Use Stand Alone (EUSA) systems to include:

1.2.5.6.1. Facilitating the EUSA setup (based on the Mobile Device Management provider or configuration profile provided by the AFRC OMD Program Office).

1.2.5.6.2. Initiating EUSA operating system updates as approved by DISA and AFRC OMD Program Office.

1.2.5.6.3. Collecting audit logs to be provided back to AFRC OMD Program Office.

1.3. Waivers, Product Improvement Program, and Supplements.

1.3.1. Requests. Submit waiver requests through the unit's chain of command to AFRC OMD office for processing, coordination, and approval by MAJCOM/A3 or the appropriate agency.

1.3.2. AFRCI 11-270 Waivers. 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,* and route the waiver request through the appropriate Operations Group Commander, the Group OMD Manager, to AFRC/A3RM. **(T-2)** Upload all waiver requests to the "Waivers" section of the AFRC OMD Teams™ or SharePoint™ site. The AFRC OMD program manager will work with the unit to process the waiver and will publish the results of the waiver request on the AFRC OMD Teams™ and SharePoint™.

1.3.3. Product Improvement Program. Submit all product improvement program ideas (i.e., new apps, websites, accessories, etc.) through the Group OMD Manager. For any Process Improvement Program submission that will result in funding requirements outside of the unit or manpower outside of the unit, route the Process Improvement Program form through the Operations Group Commander and Group OMD Manager. All Process Improvement Program

ideas will use the AF Form 1768, *Staff Summary Sheet,* or equivalent, and submitted on the AFRC OMD Program Teams™ or SharePoint™ site under the Waivers section.

1.3.4. AFRCI 11-270 Unit Supplement. Units may supplement this AFRCI. Route any unit supplements through their Operations Group Commander for approval. File any Unit supplement with the Group OMD Manager using the AF 1768, *Staff Summary Sheet,* on the AFRC Ops Mobile Program Teams™ or SharePoint™ site. Attach the unit Supplement to the Staff Summary Sheet approval package and upload to the AFRC Ops Mobile Teams™ or SharePoint™ site under the Waiver section.

1.3.5. OMD Configuration Waivers. Configuration waivers, deviations, and change requests will be submitted to AFRC/A3RM on AF Form 4169, *Request for Waiver from Information Assurance Criteria*, for coordination with the Authorizing Official. The waiver will be submitted via the AFRC Ops Mobile Program Teams™ or SharePoint™ site under the Waiver section and routed to the appropriate Authorizing Official for approval by AFRC/A3RM.

Chapter 2

OPERATION AND EMPLOYMENT

2.1. General.

2.1.1. The goal of the OMD program is to provide all operations group users with a government furnished commercial mobile device capable of fulfilling their mission requirements, while increasing their ability to accomplish readiness items and additional duties. To ensure compliance with DoD directives and continued program success, specific management and administration measures must be in place.

2.2. Device Management.

2.2.1. All OMDs and supporting devices will be enrolled in the current AFRC Mobile Device Management solution. This includes tablets, laptops, desktops, and capable peripherals. These devices are the only devices allowed to be on the mission dedicated wireless network and will receive the network configuration through automated profiles.

2.3. Authorized Hardware/Software List.

2.3.1. AFRC/A3RM will maintain an Authorized Hardware and Software List on the AFRC Operations Mobile Device Teams™ and SharePoint™. For notification of list changes, interested parties should subscribe to the Teams™/SharePoint™ list for notifications.

2.3.2. Only government-issued, Enterprise Mobile Management devices may be used for EFB functionality.

2.4. Hardware Asset Management.

2.4.1. All OMDs shall be entered in the AF Information Technology Asset Management module. Units shall not procure mobile devices without prior coordination and approval from AFRC/A3RM. Unit procured devices should be reported to the AFRC Program Manager for entry into the Device Enrollment Program.

2.4.2. Care and handling. Each member issued an OMD is responsible for its proper care and handling. Report any loss, theft, loss of functionality, display readability, or battery problems to a unit designated OMD manager immediately. Consult the AFRC OMD Program Manager (PM) and/or other applicable programmatic guidance as published by the OMD Program Office for guidance on determining liability. All lost or stolen devices shall also get reported to the base IT Equipment Custodian by the unit designated OMD manager.

2.4.3. Repair and Maintenance. Consult OMD PM and/or other applicable programmatic guidance as published by the OMD Program Office. 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 (as required) via HQ AFRC/A3RM coordination or repair at a manufacturer-authorized service provider. The MAJCOM tech refresh plan includes a 4% overage to account for breakage; if the unit exceeds this rate and has no spare devices, the unit is responsible for purchasing required devices with coordination and approval from AFRC/A3RM. **Note:** In order to protect CUI info on Air Force devices; unit OMD managers must sanitize/wipe devices using the native, Mobile Device Management, or Apple

Configurator 2 process before being returned for repair. If a wipe cannot be accomplished, then the device must be considered non-serviceable and must be destroyed. **(T-0)**

2.4.4. Units will establish check-in/check-out procedures for all MAJCOM supplied OMD equipment to include Automatic Dependent Surveillance-Broadcast receivers and removable aircraft mounting solutions.

2.5. Hardware Refresh. OMDs must be periodically replaced on pace with manufacturer recommended lifecycles. AFRC will plan a 33% annual refresh rate, regardless of current device usage. This rate will afford predictable and manageable budgeting and device manager workload.

2.6. User Training and Documentation. OG/Unit OMD managers will ensure users have completed applicable DoD Mobile Device User training. Training completion certificate, along with completed AF Form 4433, *US Air Force Mobile Device User Agreement*, will be submitted to AFRC/A3RM prior to account creation. OG/Unit OMD managers should also establish a basic user training program. In the absence of a local training program, user guides may be found on the AFRC Operations Mobile Device Teams™/SharePoint™ or the AFRC Commercial Mobile Device Users Teams™.

2.7. EUSA Backup System Requirements. Group OMD managers will ensure their sites maintain a EUSA backup system. Guidance for configuration, maintenance, operational use, and recovery of EUSAs can be found on the AFRC Operations Mobile Teams™/SharePoint™. An approved external hard drive is required for any backup system to work in the event of a network outage.

2.8. Network Connections.

2.8.1. OMD users will use secure wireless networks to the maximum extent possible. If the use of an unsecure network is required for mission accomplishment, users will utilize secure data transfer to the maximum extent possible (example: VPN). If at any point an OMD is connected to an OCONUS (non-US owned) network, the user is required to provide details of use and the device will be wiped and reprovisioned. These details should include (at a minimum): location of network, apps used, and what data was transferred.

2.8.2. Government-owned wireless routers procured for OMD support will be configured by AFRC designated personnel. **(T-2)** All routers supporting EFB requirements must be approved and listed on the AFRC Ops Mobile Teams™. **(T-2)**

2.8.3. Government-procured cellular hotspot use (pucks or phones) is authorized. These devices must also be properly managed and secured to prevent unauthorized access.

2.9. Publication Currency. Each aircrew member is responsible for ensuring all publications required for flight are current, accessible, and viewable on their issued device prior to flight. Crewmembers should synchronize/update their files at the start of each flying period. Only publications required for flight IAW Mission Design Series (MDS)-specific guidance are required to be current. Units should identify publications releases that are critical for the mission and ensure off-station crewmembers receive them as soon as practical by any means necessary.

2.10. Use within Classified Processing Areas (CPA). AFRCI 11-270 does not give permission for OMDs to enter into any classified ground facility**.** To meet mission requirements, OMDs should be permitted within certain CPAs such as aircrew mission planning facilities and Weapons System Trainers. Group OMD managers are responsible for identifying CPAs where OMD use is

required and coordinating with wing Cybersecurity Office for any local authorization and security requirements that go above and beyond guidance/checklists already provided by the OMD Program office. Specific approval from the site security manager is required to carry an OMD into any area where classified information is being used or processed.

2.10.1. When operating OMDs authorized for use within designated CPAs, users will ensure that the OMD CPA entry checklist is followed verbatim. OMDs are intended for handling only unclassified information.

2.10.2. In the event of classified spillage, classified messaging incidents, malicious logic, or a COMSEC incident involving an OMD, individuals will notify applicable information protection personnel, and contact the AFRC OMD PM for guidance.

2.11. OMD In-Flight Usage.

2.11.1. Device in-flight configuration will be per MDS specific guidance. In the absence of guidance wireless connectivity services will be disabled by placing the device in "Airplane Mode—On, Wireless—Off" prior to takeoff and will remain disabled until after landing. **(T-2) Exception**: If Automatic Dependent Surveillance-Broadcast IN devices are authorized to be used in a particular MDS. In this case, then the EFB device may only connect to Automatic Dependent Surveillance-Broadcast IN devices that are equipped with encrypted Wi-Fi connections, such as the Stratus 2S/3.

2.11.2. Mounting Locations. Mounting locations must not impede flight controls in any way or obstruct the pilots' view in front of the aircraft. **(T-0)** Other crew positions (i.e. Navigators, Flight Engineers, etc.) may also employ device mounts. Time and circumstances permitting, OMDs, peripheral equipment, charging devices and cables that are not a permanent part of the aircraft should be stowed prior to egress.

2.11.3. Use of Electronic Checklists. Approved digital versions of aircraft checklists may be used on the OMD if authorized by MDS-specific guidance.

2.11.4. AFRC users will utilize in-app features to disable screen lock (as required) for in-flight usability.

2.11.5. 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)**

2.11.6. 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.

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

2.12.1. Appropriate connectivity icons are displayed based on guidance in this instruction and applicable to the environment where the devices are being operated (i.e. Airplane icon when airplane mode is required, Wi-Fi icon on when Wi-Fi connectivity is authorized and required, Bluetooth icon not on unless required).

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

2.12.3. Note and report any unapproved or unexpected application icons appearing on the device.

2.12.4. Maintain device compliancy as approved software updates/patches are released by the AFRC OMD PM

2.13. OMD Device Failure. If OMD fails and function cannot be restored during flight, the aircraft commander will direct the use of other crewmembers' OMD devices and/or spare OMD devices (as applicable) to minimize aircrew workload, maximize situational awareness, and maintain safety of flight.

2.13.1. If a device fails while in use during a critical phase of flight, obtain a backup device and seek another crewmember's assistance with accessing required information. User's individual password may be shared if needed to back-up a primary crewmember's failed device, but common group passwords will not be used.

2.13.1.1. Device failures shall be noted in detail to include date, time, application, and/or hardware failure. Findings will be forwarded to the AFRC OMD PM.

2.13.2. OMD Back-Up Requirements. As required per MDS guidance. In the absence of MDS guidance, a minimum of one OMD per crewmember will be carried, loaded with current electronic Flight Information Publications. **(T-2) Exception**: Optional for Aeromedical Evacuation crewmembers, Flight Attendants, and as required by MDS-specific guidance for non-primary crew members.

2.14. OMD Disposition. Devices shall be maintained during their 3-year lifecycle unless otherwise directed by AFRC OMD PM for an extension. At device End-of-Life, OMD manager shall perform factory resets to ensure device is clear of all data. Devices shall not be crushed, shredded, or pulverized as a sanitization method unless there has been an incident of classified information spillage. OG OMD managers shall coordinate with local IT Equipment Custodian and BECO on proper disposition or reutilization of End-of-Life devices. OMD manager shall maintain the Mobile Device Management system for asset removals and update the AFRC Ops Mobile Device Teams™/SharePoint™ Asset Disposition Tracker list.

MICHAEL T. SCHULTZ, Brigadier General, USAF
Director of Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

31S5-4-ETool-1,*ETool Setup and Management*, 13 January 2016

AFI 11-215, *Flight Manuals Program,* 25 March 2019

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

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

TO 00-5-1, *Air Force Technical Order System,* 15 February 2019

Prescribed Forms

None

Adopted Forms

AF Form 1768, *Staff Summary Sheet*

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

AF Form 4433, *US Air Force Mobile Device User Agreement*

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

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

CPA—Classified Processing Area

EFB—Electronic Flight Bag

EUSA—Exclusive Use Stand Alone

FAM—Functional Area Manager

MDS—Mission Design Series

OG—Operations Group

OMD—Operations Mobile Device

PM—Program Manager