Department of the Army
Headquarters, USAFCOEFS
455 McNair Avenue, Suite 100
Fort Sill, Oklahoma 73503
5 June 2015

***USAFCOEFS Regulation 25-11**

Information Management

Wireless Mobile Device Management (MDM), DOD Mobility Program

---

Summary. This regulation provides policy and procedures for users of mobile devices, mobile service provider plans, personal device use, and Network Enterprise Center (NEC) provisioning on Fort Sill.

Applicability. This regulation applies to all Fort Sill users of government wireless devices.

Supplementation. Supplementation of this regulation is prohibited without prior approval from the NEC Business & Plans Division (B&PD), 475 Ganahl Road, Fort Sill, OK 73503.

Suggested Improvements. The proponent of this regulation is NEC, B&PD. Users are invited to send comments and suggested improvements on Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) directly to NEC, B&P.

Distribution. This regulation is distributed solely through the Directorate Human Resources, Administrative Services Division Homepage at: http://sill-www.army.mil/USAG/publications.html.

---

*This regulation supersedes FS Regulation 25-11, 20 December 2010.

Chapter 1
Introduction

1-1. Purpose. To provide users of Fort Sill a ready reference for mobile devices, provisioning service plans through third party contract, and administration responsibilities.

1-2. References. Required and related publications and prescribed and referenced forms are listed in Appendix A.

1-3. Explanations of Abbreviations and Terms. Abbreviations and terms used in this regulation are explained in the glossary (Appendix C).

1-4. Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to Army Regulation (AR) 25-400-2, The Army Records Information Management System (ARIMS) and DA Pamphlet 25-403, Guide to Recordkeeping in the Army. Record titles and descriptions are available on the ARIMS website: https://www.arims.army.mil.

1-5. Policy

a. Entitlement.

(1) The Army sets forth policy mandating good business practices in determining need, procurement, property management and utilization of government-owned personal, commercial mobile devices. Use of government electronic devices mentioned in this regulation must satisfy a valid mission critical requirement. Government-owned mobile electronic devices will not be used for personal convenience or duly enrich the user through private business. Mobile communications are to be used when office equipment are not available.

(2) Government provided mobile devices will be used to conduct official business only, with the exception of the following:

(a) Extreme emergency situations.

(b) Security situations.

(3) Mobile devices for the purpose of placing or receiving unauthorized calls, with the intent to later reimburse the government, is also prohibited.

(4) Portions of this regulation that prescribe specific conduct are punitive, and violations of these provisions may subject offenders to non-judicial or judicial action under the Uniform Code of Military Justice, or to punishment determined by a U.S. Magistrate.

b. Information Management Practices.

(1) All employees are responsible for the disposition of documents marked “For Official Use Only” (FOUO).

(2) All Employees signed an agreement prior to using computer equipment. Segments of this policy state proper use of information resources is the responsibility of the user including the handling of potential personally identifiable information (PII).

(3) No tablet or portable device will connect to the Army Network unless expressly approved by NEC or operated through a government program such as Defense Information Systems Agency (DISA) (reference 1-5 c.(1)).

(4) Do not store FOUO on a non-approved Department of Defense (DoD) computer. Mobile devices should be used for temporary reference and retained as long as needed then deleted.

(5) Software and information sets such as Occupational Safety and Health Administration standards and law references such as the Code of Federal Regulations, commercial print, and scholarly material from sources such as UMI are all valid uses for a tablet and may be retained on the devices as long as needed.

c. Mandatory Sources of Supply.

(1) Equipment Procurement – Army regulations require all information technology (IT) equipment and services must be sourced through the website Computer Hardware, Enterprise Software and Solutions (CHESS). If equipment is not available through CHESS, the directorate may procure through commercial sources unless specifically prohibited by procurement regulations. See DISA Approved Devices, "Secure Unclassified Mobile Devices and Wireless Services", http://www.disa.mil/Enterprise-Services/Mobility/Devices-and-Wireless-Services .

(2) Mobile Services Infrastructure – In order to support other agency requirements, the DoD Mobility Program office at DISA offers a Secure Unclassified Mobility Infrastructure at DITCO (http://www.disa.mil/Network-Services/Voice). For instance, Sensitive but Unclassified, SBU voice offers the buyer Features and rate to fit the agency needs (http://www.disa.mil/Network-Services/Voice/SBU-Voice).

(3) Acquiring Data Service Plans -The Defense Information Technology Contracting Organization can assist with obtaining cellular service plans to support mobile device technology. Organizations can also elect to use their own contracting offices to establish cellular service by procuring plans directly through their local contracting office or Mission & Installation Contracting Command.

Chapter 2
Responsibilities

2-1. Installation Commander will—

a. Ensure an appropriate control process is in place for all mobile assets and service acquisition requirements/usage.

b. Ensure decisions to obtain cellular telephones, electronic call pagers, and Personal Data Assistant services are based on valid/mission critical requirements.

c. Ensure internal control procedures via local policy or standard operating procedures are established and address such issues as physical security, accountability, misuse/abuse, issuance, and procedures for acquiring adequate support.

2-2. Network Enterprise Center will—

a. Update this policy.

b. Assist in providing information to obtain the most favorable rates by establishing negotiated ordering agreements with cellular telephones, electronic call pagers, and Personal Data Assistant vendors.

c. Provide government and industry information on developing trends in the mobile community.

d. Review service, equipment, and rate plans with organizations to assist in determining optimum suppliers and the most efficient service available.

e. NEC will not determine organizational need, nor procure equipment for an organization.

f. NEC will provide technical assistance to each organization based on their requirements and application.

g. NEC may recommend not to procure equipment based on requirements, but the organization has the final decision on expending funds.

2-3. Commanders/Directors will-

a. Implement this policy.

b. Appoint a Telephone Control Officer (TCO) to assist users in setting up their command's mobile devices. Setting up the device includes custody receipt, property book, common access card sled, computer mobile device interphase, contact listing, password reset and user account details. TCOs shall provide and audit and review of organization usage and accountability to their commander/director for proper stewardship. The TCO will be the designated individual to manage and request cellular/Personal Data Assistant service/telephones.

c. TCOs will-

(1) Serve as main point of contact between their unit and the NEC.

(2) Validate requests for administrative cellular telephone service from their organization.

(3) Submit work orders for mobile devices via the Army Enterprise Service Desk (AESD). TCOs can access the AESD by calling 1-866-335-2769. Only TCOs can submit a telephone work order.

(4) Disseminate information and instructions received from NEC to their respective organization.

(5) Ensure listings in Area Military Directory are current and accurate.

c. Prepare an internal justification/requirement and validate the mission essential need for the cellular telephone, electronic call pager, and Personal Data Assistant. Only a commander (06 level) or director can sign the statement; no delegation of authority is authorized. Revalidate annually mission/critical need for this service no later than 15 August each year. Budget and provide funding for all wireless accounts.

d. Maintain records as required by AR 25-1 and AR 25-400-2. Be accountable for cellular/pager/service. Ensure turned-in cellular telephones and electronic call pagers are immediately deactivated by timely notification to the providing service or activity.

e. Review and certify monthly bills for cellular telephone, tablet, electronic call pager, GPS, and Personal Data Assistant services for actual services used and costs incurred. Investigate and resolve all questionable calls and billing anomalies in a timely manner.

2-4. Users are responsible for-

a. The data and content on any mobile device; personally owned or Government issued (cellular telephone, tablet, electronic call pager, GPS, Mobile appliance and Personal Data Assistant) are not stored permanently if not needed to perform Government business. Do not warehouse data on mobile devices.

b. Ensuring any mobile devices (as listed above in a.) in their possession are secured against unauthorized access to Government information at the SBU Level and above.

c. Users are responsible for the disposition of information contained on any mobile device in their possession, and comply with their organization’s MDM policy. They may be subject to discipline for the loss of the equipment and/or the information contained on the device.

d. Providing updated FS Form 845 to TCOs (Appendix C).

e. Using only when other means of communication is unavailable and/or cannot be supported by other available government telephones, radios, or other services.

f. Driving with mobile devices (defined in a, above).

(1) Ensure personal and government cellular telephones are used in accordance with the following guidelines while driving on post. Mobile devices used improperly while driving may be classified as driving impaired. In accordance with DoDI

6055.04of 20 APR 2009, driving privileges may be suspended in compliance with 32 CFR 634.9.

(2) In accordance with 32 CFR Section 634.25, using hand-held cellular telephones while driving a U.S. government vehicle or privately-owned vehicle on Fort Sill is prohibited. This prohibition applies to the driver of the vehicle only and shall not be enforced against any passenger in or on the vehicle. A driver who wants to use a hand-held cellular telephone must move his/her vehicle safely off or to the side of the road and bring the vehicle to a complete stop, out of the way of moving traffic, before using a cellular telephone.

f. All suspected violations of HIPAA are to be handled in accordance with DOD 8520.02-R. Mobile users are strongly advised to practice administrative and physical safeguards to prevent incidents and violations (IBID Chapter 2)

Appendix A
References

Section I
Required Publications
AR 25-400-2
Army Record Information Management System
AR 25-1
Information Management
DA PAM 25-403
Guide to Recordkeeping in the Army

Section II
Prescribed Forms
FS Form 845
Request for Wireless Service
Section IV
Referenced Forms

DA Form 2028
Recommended Changes to Publications and Blank Forms

On-line References

 Army Mobility Strategy_26NOV201	- Memorandum, Headquarters, United States Army Command, 21 November 2013, Subject : Army Mobile Strategy
 NexGen_DoD_Wirel essBPA_Memo_Sign	- Memorandum, Headquarters, United States Army Command, 03 April 2013, Subject: Army Policy Requiring the use of Next-Generation (NexGen) Department of Defense (DoD) Handheld Wireless Enterprise Blanket Purchase Agreements (BPAs) to Identify and Eliminate Devices Based on Usage.
 CordlessTelephone Policy20140204.pdf	- Memorandum, Headquarters, United States Army Command, 04 February Subject: Cordless Telephone Policy
DISA Policy http://www.disa.mil/Enterprise-Services/Mobility/Policy-and-Guidance	1. DoD Mobility Program - 2. DISA Strategic Plan 2013-2018
DOD CIO Policy	- Commercial Mobile Device (CMD) Implementation Plan - DoD CIO Mobile Device Strategy

Appendix B
Glossary

Section I
Abbreviations

AESD
Army Enterprise Service Desk

AR
Army Regulation

ARIMS
Army Records Information Management System

B&PD
Business & Plans Division

HQ
Headquarters

NEC
Network Enterprise

TCO
Telephone Control Officer

Section II
Terms
Note:

Data at rest. Information that resides on electronic media while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated. Data at rest can be archival or reference files that are changed rarely or never. Data at rest also includes data that is subject to regular but not constant change.

Data Integrity. Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Mobile Device Management (MDM)
Mobile Device Management (MDM) is a term for the administration of wireless, mobile devices. The use of smartphones, tablets, laptops and desktop computers are covered under MDM. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices. Data Integrity. Condition existing when data is unchanged from its source and has not accidentally or maliciously modified, altered, or destroyed.

DoD Mobility
DoD mobility is the term for how the Department of Defense operates, connects, and supports its stakeholders – most significantly, through the use of mobile solutions to provide mission-essential tools to our warfighters.

Bring Your Own Device
Bring Your Own Device (BYOD) is an IT policy where employees are allowed to use their personal mobile devices to access enterprise data and systems. Use of the term wireless device refers to government devices unless specifically identified as a personal device.

Mobile Device - Cellular Radio/Telephone, Electronic Call Pager Technology, and Personal Data Assistant
Mobile Device - Cellular Radio/Telephone, Electronic Call Pager Technology, and Personal Data Assistant is defined as devices, equipment and services which provide direct dial telephone communications or call paging services to and from hand-held portable and stationary telephones and/or call pager devices that interconnect with the public telephone or paging networks.

Business Agnostic
Focus on Information not the platform

Appendix C
Request for Wireless Service FS 845

REQUEST FOR WIRELESS SERVICE	
1. Mobile Number:	
a. Equipment:	b. Model:
c. SIM Number:	d. IMEI Number:
e. Pin Number:	f. ESN Number:
g. Organization:	h. Name of User:
i. Duty Position:	j. Phone Number:
2. I understand I am responsible for ensuring all usage of the above device is FOR OFFICIAL USE ONLY.	
a. Name: (Last, First, MI)	b. Date:
c. Signature:	c. Date:

PREVIOUS EDITION ARE OBSOLETE

FS Form 845
(DOIM) 2 Feb 07

APD PE v1.00

NETC-SFB-DL

TRACY P. BANISTER
COL, GS
Chief of Staff

JAMES A. MILLER
Director of Human
Resources

DISTRIBUTION:
Fort Sill Intranet