DoD Mobility

Kim Rice
Mobility PMO
Contact: 301-225-5670

17 Jun 2015
DoD Mobility PMO Concept

**Vision:** Secure, reliable and responsive infrastructure and services for the mobile users across the DoD.

**Mission:** The DoD Mobility Program Management Office provides enterprise capabilities and services to enable global mobility capability to support operations for joint warfighters, National level leaders and coalition partners. Our mission is to extend enterprise services to mobile devices in order to deliver a fully operational secure Mobility Enterprise Service to DoD.

Delivering mobile enterprise capabilities that securely operate and strengthen the defense of the cyber mission space
DoD Mobility PMO

End-to-End Vision

OBJECTIVE
- Robust Tools and Apps for Mobile User Experience
- Mobile Content supporting Unified Communications
- Seamless Authentication
- Cross Domain
- Enhanced Policies
- Hierarchical Policy Structure
- Dynamic Auditing & Threat Detection
- Personal Use Apps & Devices
- DoD Component Email
- Advanced Cyber Mobility Tools

TODAY
- Enterprise Email
- Text Messaging
- Calendar
- Contacts
- Approved COTS & PUMA Apps

Today’s Mobile Device & Productivity

• • •

Enterprise

Mobile Application Development Platform

Gateway

Mobile Device Management / Mobile Application Store

DoD Networks

Wireless Carriers

Identity Management / PKI

Commercial Mobile Devices

DoD Component Back End Services

Access to data, apps and tools necessary for a mobile workforce
Mobility and Security

MOBILITY COMPONENTS
- Applications
- Infrastructure
- Networking
- Gateway
- Mobile Device Management (MDM)
- Mobile Application Store (MAS)
- Mobile Content Management (MCM)
- Enterprise Back End Services

TODAY
- National Information Assurance Partnership (NIAP)
- Manual App Vetting
- Policy

FUTURE
- National Information Assurance Partnership (NIAP) Certifications
- + Bring Your Own Device (BYOD)
- + Corporate Owned Personally Enabled (COPE)
- Derived Credentials / Public Key Infrastructure (PKI)
- Computer Network Defense
- Automatic App Vetting
- Virtual Private Network (VPN)
- Enhanced Policy Violations
- Cyber SA and CSAAC Analytics

THREATS
- Rooting
- Phishing / Whaling
- Malware
- Zero Day Attacks
- Denial Service
- Insider Threats
- Hackers

Grey: Objective
## Mobility Portfolio Priorities

### PRIORITIES: “MUST DO’S”

1. Sustain Deployed Mobility Components
   - DMCC-S 1.0 and DMCC 2.0
   - DMUC Mobile Device Manager (MDM)
   - DMUC Mobility gateways
2. DMCC-S 2.0.5
3. DMUC CAC S/MIME replacement
4. DMCC-TS 1.0 Pilot
5. User experience (voice, e-mail, chat, office, storage)
6. DMUC Mobile Content Management (MCM)
7. Limited soft cert pilot support.
8. DoD deployment of Knox 2.0 capabilities
9. Mobile app development framework
10. Sensor analytics
11. Data at rest
12. MDM Follow-on Contract
13. Ozone Mobile

### Delayed Priorities:

1. Automated PKI support for devices and apps
2. GOTS/COTS mobile vetting tools
3. DMCC-S 3.0
4. Non-DEE e-mail support for DMUC users

### Underlying priorities: program/processes/tools and enhanced ordering experience

### MOBILITY CUSTOMERS

- Air Force
  - Air National Guard (Air Force)
  - Africa Command (AFRICOM)
  - Acquisition Support Center (USAASC)
  - Army Central Command (ARCENT)
  - Army Criminal Investigation Command (CID)
  - Army Cyber Command
  - Army Europe Command (USAREUR)
  - Army Forces Command (FORSCOM)
  - Army Headquarters (HQDA)
  - Army Install Management Command (IMCOM)
  - Army Intelligence & Security Command (INSCOM)
  - Army Materiel Command (AMC)

- Army
  - Medical Command (MEDCOM)
  - National Guard (NG)
  - Network Enterprise Technology Command (NETCOM)
  - North (ARNORTH)
  - Pacific Command (USARPAC)
  - Reserve Command (USARC)
  - South (ARSOOUTH)
  - Space and Missile Command (SMDC)
  - Surface Deployment Distribution Command (SDDC)
  - Test and Evaluation Command (ATEC) G6
  - Training and Doctrine Command (TRADOC)

- Navy
  - Bureau of Medicine and Surgery (BUMED)

- Joint Staff
  - Defense Health Agency (DHA)
  - Europe Command (EUCOM) J6

- Strategic Command
  - Transportation Command (TRANSCOM)
  - United States Army Africa (USARAF)

- Southern Europe Task Force (SETF)

- Central Command (CENTCOM)
- Defense Command (EUCOM) J6
- Northern Command (NORTHCOM)
- Southern Command (SOUTHCOM) HQ
- Strategic Command (STRATCOM)
Secure Mobile Infrastructure

End-to-end architecture secures mobile device access to DoD enterprise services

**Secure Mobility Infrastructure**

- **Mobility Gateways**
  - Secure access to DODIN through VPNs and private carrier networks
  - Integrated at the Internet Access Points (IAPs) to leverage enterprise Computer Network Defense

- **PKI Authentication**
  - DoD PKI certificates authenticate users to enterprise services (user certificates, CAC cards)

- **Mobile device, operating system, applications**
  - MDM enforced security policies
  - Access only to applications vetted through DISA app vetting process

**Operating system security, strong authentication, secure remote access, and continuous monitoring are the keys to successful mobile security**
# DMCC-S R2.0

## The New Generation of DoD Secure Mobile Communications

### Device Basics
- Samsung Galaxy Commercial Smartphone
- Quality super-AMOLED screen
- 5-inch, 1080-pixel display
- Extensive memory storage
- Strong battery life and processor
- Approved and integrated components with National Information Assurance Partnership (NIAP)

### Advantages
- Delivered in partnership with the National Security Agency (NSA)
- Compliant with NSA’s Commercial Solutions for Classified (CSfC) process
- Secure voice and web-browsing
- Outlook Web Application (OWA) capability for SIPR access
- Mobile Device Management (MDM) and policy enforcement
- Supporting service desk
- Constantly evolving capabilities to meet user requirement

### Capabilities
- Provides SECRET (DMCC-S) mobile access to select DoD voice and data networks capabilities.
- Replaces the Secure Mobile Environment Portable Electronic Device (SME PED) and DMCC-S 1.0 supported mobile devices.
- Provides enhanced graphics and email experience through the new Integrated Commercial Solution (ICS) device.

### Security Overview
- Phone calls securely placed through Cellcrypt
- Embedded FIPS IPSec Virtual Private Network (VPN) accessible through native Samsung VPN client
- Pre-loaded items managed through Quark Security Shield for streamlined, user-friendly interface
- Data-in-transit protection
- Device wipe capability
DMCC-S R2.0.5 – May 2015

Full Deployment View

- **2 Mobility Gateways**
  - Secures device before features utilized

- **Internet Ingress Point**

- **DoD Enterprise Capabilities**
  - **OWA Email for DEE and Non-DEE**
  - **Secure Phone Calls to DMCC, DRSN, ECVoIP, VoSIP, SCIP Devices**

- **Mobile Device Management**
  - Replacement of Nanny App with SE Android & Enterprise MDM capability

- **NSA Approved Mobile HotSpots**
  - International roaming capability

- **Order Entry via DISA Portal**

- **Wireless Carrier**
  - Secure CONUS Access over Verizon APN

- **Components under NIAP Assessment:**
  - Samsung Galaxy Device (complete)
  - Apriva/Authentec VPN concentrator (partial)
  - MobileIron MDM
  - CellCrypt VoIP client

- **Legacy Smartphone Support**
  - Motorola RAZR MAXX
  - • Plan to EOL six months
  - > Rel. v3.0 (TBD)
  - • MDM – N/A

- **Grey: Delivered in DMCC-S 2.0.5**
**Objective State:** Deliver initial pilot voice capability and posture for SCI in future releases

**DMCC-TS R.1.0 Pilot Capabilities**

- **Mobility Gateway:** Secures device before features utilized
- **Internet Ingress Point**
- **Continuous Monitoring**

**DoD Enterprise Capabilities**

- **Mobile Device Management:**
  - Instances of DMCC-S MDM established at primary and COOP sites on SIPRNet

- **ICS Device Configured for TS**

- **Wireless Carrier:**
  - **Secure CONUS Access over Verizon APN**

- **NDA Approved Mobile HotSpots International Roaming Capability**

- **Order Entry via DISA Portal**

---

*United in Service to Our Nation*

**UNCLASSIFIED**
Pace of Mobility

- What is the best way to deliver for mobile?
- How should we engage and utilize vendor expertise?
- What should the driving policies (new STIGs/SRGs, etc.) be for mobility?
- How do we integrate commercial time to market with DoD processes?

- Rapidly evolving technology
  - Reacting to release of new HW/SW
  - New cyber threats
  - Integration across vendor technology

- Developing mobile policies & business processes

- Meeting wide range of DoD mission requirements

- PMO re-looking the way mobility is being delivered (what & how)
- How does DoD leverage commercial mobile best practices and technology?