DoD Mobility

Kim Rice
PM, Mobility PMO
21 April 2016
"The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to United States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments."
Mobility – Objective State

Any User, Any Device, Any Data… Anywhere

**Mobility:** Providing freedom of action for personnel to securely work in any location, over any device across any network

**Device:** Laptop, smartphone, tablet / iPad, executive kit, peripherals

**Mobile Application:** Software application developed specifically for use on small, wireless computing devices, such as smartphones and tablets, rather than desktop or laptop computers
Mobility Challenges Today

- Limited CAC-Authentication
- Cyber Threat Growing
- Limited Data at Rest
- Limited Ability to Modify Mobile Artifacts
- Limited Access to DoD Source Data (Legacy Data)
- Existing Business Processes and Systems
Mobility-Wide Transformation

- Mobile Device Management
- Enterprise E-mail
- Approved GOTS, COTS, and PUMA Apps
- Text Messaging
- Calendar
- Contacts

- Mobile Content Supporting Unified Capabilities
- Seamless Authentication
- Networking
- Cross Domain
- Enhanced Policies
- Mobile Content Management
- Hierarchal Policy Structure
- Dynamic Auditing and Threat Detection
- Personal Use Apps and Devices
- DoD Component Email
- Advanced Cyber Mobility Tools
DoD Mobility - Objective State

**CURRENT**

- **INFRASTRUCTURE COMPONENTS**
- **SECURITY & IDENTITY MANAGEMENT**
- **POLICY & STANDARDS**
- **BUSINESS SYSTEM & PROCESS**
- **USER**
- **APPS**

**END STATE**

- **INFRASTRUCTURE COMPONENTS**
- **SECURITY & IDENTITY MANAGEMENT**
- **POLICY & STANDARDS**
- **BUSINESS SYSTEM & PROCESS**
- **USER**
- **APPS**

---

**USER**

Office package with content management; variety of apps, device/carrier agnostic; limited BYOD

**APPS**

Federated apps stores, common SDKs, easy access to PUMA, GOTS and COTS apps, monitoring tools

**INFRASTRUCTURE COMPONENTS**

MDM/MAS/MCM services in the cloud, modular components, automated access to gateways & VPNs

**BUSINESS SYSTEM & PROCESS**

One stop shopping and telephony management

**SECURITY & IDENTITY MANAGEMENT**

Dynamic security tools; automated IDAM; use of biometrics

**NETWORK & SERVICE PROVIDERS**

Carrier agnostic; network detection tools and monitoring; WiFi access points worldwide

**POLICY & STANDARDS**

Used across DoD and Federal Government to enable reuse and interoperability
Single Service Manager (SSM) capability consisting of software, computing, and network infrastructure; and integration, engineering, and support services designed to enable end-to-end mobility services for the DoD user community across three classifications: UNCLASSIFIED/FOUO, SECRET, and TOP SECRET (TBD).

Major SSM Capability Areas:

- Telephony Expense Management (TEM)
- Devices & Infrastructure Components
- Security and Identity Management
- Service Desk and Ticketing
- Business Processes
Economies of Scale

Department of Defense

How can DOD rapidly take advantage of technical innovations?

How does DoD scale to true enterprise services?

How does DoD leverage economies of scale?

Industry Innovations

Fitbit

Biometrics Scanning

Radio Frequency Tagging

Smart Watch
DoD Mobility Capabilities

**Capability Snapshot**

**DoD Mobility Unclassified Capability (DMUC)**
- Soft Cert Pilot – 300 iOS Users; Android next
- 200 iOS and Android Applications
- Transition to MobileIron Spaces for improved tiered access for administrators
- Reduced infrastructure footprint by 1/3
- Initial automated Wi-Fi connection for DMUC users – DISA HQs only

**DoD Mobility Classified Capability Secret (DMCC-S)**
- Operational offering starting in June 2015
- Overwhelming, positive response from users – progressing rapidly towards enterprise interoperability
- Includes MDM and enhanced monitoring, new secure commercial device and access to voice and email capabilities

**DoD Mobility Classified Capability Top Secret (DMCC-TS)**
- TS-SCI Pilot deployed to one user
- Recognition that policy and use case needs to be revisited
- Department relooking SCI vs collateral requirement
DoD Mobility Capabilities – Next 6-12 Month Targets

**Capability Snapshot**

**DoD Mobility Unclassified Capability (DMUC)**
- Enhanced CAC access and requirements
- Derived credentials supporting iOS, Android, and Windows
- Introduction of content management app
- Increased WiFi policy implementation for DMUC

**DoD Mobility Classified Capability Secret (DMCC-S)**
- Coalition pilot addition of new Android phone
- Introduction of tablet
- Full MACP compliance
- Additional 2.0.5 users – contract awarded for additional users

**DoD Mobility Classified Capability Top Secret (DMCC-TS)**
- Initial TS pilot in support of 200 users
- Voice only capability
User Snap Shot

As of 29 March 2016

UNCLASSIFIED

Total Devices: 38,837
Total VIP Devices: 1,516

Army 56% (22K)
Air Force 33% (13K)
DoD 10% (4K)
COCOM 1% (483)
Navy 0% (87)

As of 29 March 2016

CLASSIFIED

Total Devices: 928
Total VIP Devices: 408

Army 31% (289)
Navy 13% (118)
Air Force 18% (171)
DoD 32% (292)
Marines 6% (57)
Coast Guard 0% (1)

As of 29 March 2016
Questions?
UNITED IN SERVICE TO OUR NATION