DoD’s Strategic Mobility Vision: Needs & Challenges
Agenda

• DoD Mobility Strategy Overview
• End-State Visions
• Implementation Challenges: A Reality Check
• Tactical Environment Consideration
DoD Enterprise Mobility Vision

From This: DoD Must Change

To This: "Enterprise Information Environment"

- Computing
- Mission Applications
- Data

Coalition Forces

Future Devices

Home

Work

Mobile (TDY/Deploy)
DoD Mobility Strategy & Implementation Plan

Information Enterprise Infrastructure to support Mobile Devices

Mobile Device Policies and Standards

Promote the development and User of DoD Mobile & Web-Enabled Apps

DoD Mobility Strategy

DoDI 8100.02  DoD CIO Consolidation Plan  Federal Digital Strategies  Federal Standards  Technology Insertion

United in Service to Our Nation

New Spec?

MDM/MAS Award

Uniclass IOC

Date TBD

PIV 201-2 Integration

BYOD

TBD

Primary Communication for ROUTINE DoD Users Is Wireless

Expeditre Approval Process

CMD Pilot Consolidation

Mobility Gateways FY13-14

New Classified Capability

Phase-out SME PED

Classified FOC

Enterprise Solution

FY13  FY14  FY15 - 17  FY17 - Beyond

MDM

Components Transition Plan

Business Case Analysis
End-User Device Evolution

- **Single Option**
  - **Slow Approval**
    - GOTS Solutions
      - QSEC-800
      - SME-PED
      - QSEC-2700
      - Droid Pro
    - QSEC-800
    - SME-PED
    - QSEC-2700
    - Droid Pro

- **Multiple Vendors**
  - **Approval Keeps Pace with Technology**
    - COTS Based Solutions
      - iOS, Samsung Android, BlackBerry
      - Razr Maxx

DISA
A Combat Support Agency

United in Service to Our Nation
DoD Mobility Unclassified Capability (DMUC) Enterprise End-State Vision

Service Responsibilities Upon Transition
- Service Specific Mobile Applications
- App Vetting and Integration
- Software Licenses
- Tier 1: NetOps
- Tier 1: Mobile Service Desk
- Liaison to Enterprise PMO

BB BlackBerry
DEE Defense Enterprise Email
GW Gateway
IdAM Identity and Access Management
MAM Mobile Application Management
MAS Mobile Application Store
MDM Mobile Device Management
NOC Network Operations Center
PSTN Public Switched Telephone Network
RAN Radio Access Network
UC Unified Capabilities
WLAN Wireless Local Area Network
DoD Mobility Classified Capability (DMCC) Mobile Architecture – End State

Other DMCC Enhancements Expected
- NSS PKI Support for mobility
- Multi-persona devices
- Automated call setup
- VPN interoperability
- WLAN operation

DISA Implements
- DMCC voice
- DMCC DEE
- Global deployment of multiple Gateways
- MDM/MAS capabilities
- Streamlined provisioning
- COOP (redundancy)
- 24/7 Help Desk and NetOps

- MOBILITY GATEWAY
- DMCC Suite
- "Gray" Zone
- "Orange" Zone
- "Red" Zone

COOP Continuity of Operations
CSfC Commercial Solutions for Classified
DECC Defense Enterprise Computing Center
DEE Defense Enterprise Email
DMCC DoD Mobile Classified Capability
DRSN Defense Red Switch Network
MAS Mobile Application Management
MDM Mobile Device Management
RAN Radio Access Network
SCIP Secure Communications Interoperability Protocol
VoSIP Voice over Secure Internet Protocol
Reality Check: What are the Challenges?

• Initial Mobile infrastructure is in place ...

• What’s next on the mobile horizon?
  – Joint Information Environment (JIE) Cloud deployment
  – Better control of network access
  – Increased trust in mobile applications
  – Improved information access
Mobile Device Challenges to the Edge

- Synchronization with different clouds
- Security of data is not guaranteed
- Secure connection back to DoD network
- Mobile apps designed for edge users
- No (or intermittent) availability & support for disconnected use cases
- Increased bandwidth to data access
- Multiple data models and standards
Challenge: How do we provide Mobility from the Cloud?

- Be in line with tenants of JIE
- Provider needs to meet Data Impact Level 5 requirements
- MDM/MAS/MAM operates from Infrastructure as a Service (IaaS) or Platform as a Service (PaaS)
- Needs to support PKI management and derived credentials
- Support synchronization across various clouds
- Much more ......
Challenge: How Can DoD Better Control Network Access?

- Primary Credentials: Derived from Common Access Card (CAC)
- Derived Credentials: Derived from approved mobile devices
- Moving toward Derived Credentials:
  - New Identity Management policy
  - Interim guidelines emerging
Challenge: How can DoD increase trust in mobile Applications?

- Security Hazard: Preloaded software – “bloatware”
- Satisfy DoD Security Requirements Guides: New app vetting and development tools
- Ensure Device Integrity:
  - Open MDM controls on mobile platforms
  - Supplement with continuous monitoring
- Employ hardware-based security controls
Challenge: How Can DoD Improve Information Access?

- Enable Mobile Apps: Adapt DoD software and data sources
- Design mobile apps to use cloud-based services
- Utilize common mobile app development frameworks
- Leverage established national information exchange data models
Tactical Environment Considerations

- Communications Infrastructure
- Mission Critical Voice
- Spectrum
- Battery Power
- Ruggedness (MILSPEC dust, vibration, waterproofing, etc.)
- Ergonomics (display, human-machine interface, buttons, works with gloves)
- Electronic Warfare (RF and optical signatures, EMI/EMC, disable features in theater)
- (NV/Chem-Bio, sunlight, etc.)
- Environmental/Climate Flexibility
- Intrinsically Safe (HERO, HERF, HERP)
CMD Tactical Edge Deployments

• Commercial solutions can be brittle – our environment can be harsh, and significant work is needed.

• Mobility challenges include:
  – Security
  – Spectrum management
  – Interoperability
  – Adapting new Technology
Questions?