DoD Mobility briefing for the AFCEA Mobility Summit

Mr. Randall Conway
Principal Deputy,
Deputy Chief Information Officer, Information Enterprise
US Department of Defense

January 21, 2016
Agenda

- DoD Mobility Evolution
- DoD Mobility Portfolio
- Modernized DoD Security Approval Process
- Tactical Implementations
- Related Topics
## DoD Mobility Evolution

<table>
<thead>
<tr>
<th>Mobility Elements</th>
<th>Decentralized BlackBerry &lt;2013</th>
<th>Enterprise BlackBerry 2013</th>
<th>DMUC/DMCC 2014</th>
<th>Next Era 2015+</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Devices</strong></td>
<td>BlackBerry</td>
<td>BlackBerry</td>
<td>Apple Android</td>
<td>Apple Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BlackBerry</td>
<td>BlackBerry</td>
</tr>
<tr>
<td></td>
<td>![BlackBerry Icon]</td>
<td>![BlackBerry Icon]</td>
<td>![Apple Icon]</td>
<td>![Windows Icon]</td>
</tr>
<tr>
<td><strong>Infrastructure</strong></td>
<td>Distributed BES with BlackBerry Control Centers</td>
<td>Consolidated BES with BlackBerry Control Centers</td>
<td>• Mobile Device Mgmt (MDM) • Mobile App Mgmt (MAM)</td>
<td>• Automated PKI Issuance • VPN, Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td>![BES Icon]</td>
<td>![BES Icon]</td>
<td>![MDM Icon]</td>
<td>![VPN Icon]</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>• Email, Calendar, Contacts • Selected apps</td>
<td>• Email, Calendar, Contacts • Selected apps</td>
<td>• DoD App Store • App Vetting • Defense Connect • Personal Use • Mobile Content Mgmt (MCM)</td>
<td>• Derived Credentials • App Development Framework • Multi-MDM’s</td>
</tr>
<tr>
<td></td>
<td>![Email Icon]</td>
<td>![Calendar Icon]</td>
<td>![Contacts Icon]</td>
<td>![DoD App Icon]</td>
</tr>
</tbody>
</table>

*Operating Systems*
DoD Mobility Unclassified Capability (DMUC)

Information Enterprise Infrastructure to Support Mobile Devices

Mobile Device Policies and Standards

Promote the Development and Use of DoD Mobile & Web-Enabled Apps

DoD Mobile Device Strategy

Mobile Device Mgmt (MDM)

Personal Use

Mobile App Store (MAS)

Mobile Content Mgmt (MCM)

Mobile App Dev Framework

Next Gen MDM

Bring Your Own Device (BYOD)

FY14

FY15

FY16-17

FY18 - Beyond

Mobility Gateways FY13-14

Blackberry, Samsung, & iOS devices

Derived Credentials

Wearables

Internet of Things (IoT)

Wireless Enabled Comms

DoD Wireless Policy

NIAP Protection Profiles

Federal Digital Gov Strategy

Federal Standards

Technology Insertion

Biometrics

1/28/2016
Modernized Security Approval Process

- In partnership with NSA, DoD is leveraging the National Information Assurance Partnership (NIAP) Common Criteria (CC) Evaluation & Validation Scheme for mobility approvals:
  - MDM Protection Profile (PP) v2.0
  - MDM Agents PP v2.0
  - Mobile Device Fundamentals (MDF) PP v2.0
    - Samsung – validated
    - Apple - submitted
    - Windows – submitted
    - Boeing Black – validated (DMCC potential)
  - Application Software PP v1.1 – Guidance for vetting apps on all platforms, including mobile

- Protection Profiles (PPs) have an associated DoD Annex for meeting additional DoD requirements
DoD Mobility Classified Capability (DMCC)

**GOTS Based Solutions**
- QSEC 800
- QSEC 2700
- SME PED

**COTS Based Solutions**
- Droid Pro
- Razr Maxx
- BlackBerry Bold 9900
- Samsung Initial Classified Solution
- Boeing Black

**Commercial Solutions for Classified (CSfC)**

**Past**
- **GOTS Based Solutions**
- Cellular 2G Only
- Not user friendly

**Present**
- **COTS Based Solutions**
  - NIAP approved components
  - Over the Air Updates
  - DMCC-S Fielded (1000 and growing)

**Future**
- **More Capabilities**
  - Data-at-rest (DAR)
  - Apps/widgets
  - TS/SCI capability
  - Other approved devices

1/28/2016
Tactical Implementations

Training
- DoD Mobile App Stores (150+ Commercial Apps)
- DoD App Gallery
- (50+ DoD-Developed Apps)
- NGA GEOINT App Store (80 Apps)

Operations

Tactical

Combat Training Centers
- Android Tactical Assault Kit (ATAK)

Program
- Army WIN-T Wireless CP
- Air Force Electronic Flight Bag

Tailored Applications Demonstrate the Advantages of Adapting to Military Needs
Related Topics

• Disruptive technologies
  – Internet of things; security is paramount (authentication)
  – Spectrum sharing example: LTE “unlicensed” (concept of LTE operating in the WIFI spectrum); new standards and protocols
  – Wearable technology

• Bi-Directional Sharing Provides Improved Opportunities for Increased Spectrum Access
  – Specifically, shared access by Federal users to non-Federal bands
  – Moves beyond relocation, which is not sustainable
  – Intended to support DoD access to spectrum for advanced commercial technology capabilities

• We’re reaching out
  – Recent trips to Silicon Valley, New York and Boston
  – Understand risks before adopting

• BYOD
  – Very small pilot to shake out some technical interfaces

• Pentagon Wireless
  – Exemplar for broader DoD wide use
Questions?