DoD CIO Mobility Industry Day
Mobility Update / Overview

Department of Defense
Chief Information Officer
July 9, 2015
DoD CIO Mobility Industry Day

“Capitalizing on Commercial Innovation”

2 Major Themes: Security and Applications

10:00 11:15 Panel 1: Streamlining Security Approval Processes to Keep Pace with Industry

11:45 12:15 Keynote: Mobility to the Joint Warfighter

13:15 14:30 Panel 2: Improving Productivity through Mobile Applications and Services

14:45 16:00 Panel 3: MILDEP CIO / CTO Perspectives on the Day

15:30 16:00 Closing Keynote
Over 500K Mobile Devices Under Carrier Contract ($40/month)*

- **Big Three:**
  - ARMY ~180K
  - NAVY ~105K
  - AIR FORCE ~90K

- **Device Type:**
  - 190K Smart Phones
  - 40K Tablets
  - 120K Feature Phones
  - 70K Air Cards and Hotspots
  - 7K Two-Way Pagers

- 4 Mobile Device Management (MDM) Architectures
- 4 Mobile Operating Systems
- 3 Wireless Service Contract Vehicles

*Snapshot of commercial mobile device (CMD) counts from May 2015 OMB submission*
# DoD Commercial Classified Portfolio

<table>
<thead>
<tr>
<th>Past</th>
<th>Present</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>- <strong>GOTS Based Solutions</strong>&lt;br&gt;- Cellular 2G Only&lt;br&gt;- Not user friendly</td>
<td>- <strong>COTS Based Solutions</strong>&lt;br&gt;- NIAP approved components&lt;br&gt;- Over the Air Updates</td>
<td>- <strong>More Capabilities</strong>&lt;br&gt;- Data-at-rest (DAR)&lt;br&gt;- Apps/widgets&lt;br&gt;- TS/SCI capability&lt;br&gt;- Other approved devices</td>
</tr>
</tbody>
</table>

**GOTS Based Solutions**
- QSEC 800<br>- QSEC 2700<br>- SME PED

**COTS Based Solutions**
- Droid Pro<br>- Razr Maxx<br>- BlackBerry Bold 9900<br>- Samsung S4

**Commercial Solutions for Classified (CSfC)**
- BlackBerry Bold 9900
- Samsung S4

**S/TS/SCI Capability**
- QSEC 800
- QSEC 2700
- SME PED
- Droid Pro
- Razr Maxx
- BlackBerry Bold 9900
- Samsung S4

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

**Present**
- COTS Based Solutions
- NIAP approved components
- Over the Air Updates

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

• **Security Requirements**
  - National Information Assurance Partnership (NIAP) Common Criteria (CC) Evaluation & Validation

• **Over 14 Mobile Related Protection Profiles**
  - **Major Mobile Profiles:**
    - Mobile Device Fundamentals (MDF)
    - Mobile Device Management (MDM)
    - Application Software

• **Current Mobile Device Vendors Participate in the NIAP:**
  - Samsung
  - Apple
  - Boeing
  - Microsoft
  - LG
  - BlackBerry
DoD Managed vs Personal Mobility

Finding The Right Balance

DoD Managed

Government Owned

Personal Applications

Government Protections (Maximum)

BYOD

User Owned

Government Applications

Personal Use (Maximum)

Unsolved:
- Data Spills
- Installed Malware
- Certificate Management

Security / IA

Legal / Privacy Issues

DoD Managed vs Personal Use

SUPPORT THE WARFIGHTER
Authentication on Mobile Devices - Past

- Same needs as our office computers
  - Sign, send, and encrypt email
  - Web authentication

- Hardware challenge
  - Connect smartphone to a smart card

- Common Access Card (CAC) sled issues
  - Cost
  - Separate battery
  - User expectations
Identity and Access Management (IdAM) - Present

• DoD CIO Interim Guidance on Derived Credentials, 23 Sept 2014
  o Link to Common Access Card (CAC)
  o Eliminate smartcard readers
  o Simplify credential management
  o Hardware-backed encrypted keystores

• DoD CIO Manual issuance current options:
  o Helpdesk manual provisioning via side-loading certs
  o BlackBerry certificate option (May 2015)
Identity And Access Management (IdAM) - Future

• ‘Trusted’ Issuance Infrastructure
  o Certificate authority (CA) interfaces, for over-the-air (OTA) provisioning with trusted agents
  o Purebred demonstration ~ July 2015

• Automated OTA “Factory to User” provisioning
  o Enrollment protocol security (SCEP vs EST)
    • EST – Enrollment over Secure Transport
    • SCEP – Simple Certificate Enrollment Protocol
  o Biometrics Integration
  o MDM agnostic
DoD Mobile Application Environment

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

Logistics

Tactical
- Android Tactical Assault Kit (ATAK)

Operations
- Army Field Inspection Tool
- Air Force Electronic Flight Bag

Tailored Applications Demonstrate the Advantages of Adapting to Military Needs

SUPPORT THE WARFIGHTER
Mobile Cloud Computing

- Beyond Mobile Device Management (MDM)......

- Cloud adaptations for:
  - Federated mobile management
  - Application Hosting
  -Disconnected use case

- Cloud Providers to meet FEDRAMP requirements
Help from Industry: 
Wide Range of Operations

- Operating Systems/MDM’s/Carrier: Multi vendor
- Policy/Guidance: Security Guides to NIAP PPs
- Personal use: Managed to BYOD
- Information Access: Email to Managed Cloud
- Applications: Commercial and Custom
- Identity Management: Hard token to derived credential

SRG – Security Requirements Guide
NIAP – National Information Assurance Partnership
PP – Protection Profile
BACKUP
References

- NSA Commercial Solutions for Classified Program (CSfC) Program: http://www.nsa.gov/ia/programs/csfc_program/
- DISA Mobility Program: http://www.disa.mil/Services/Enterprise-Services/Mobility
- DoD Interim Guidance on the Use of DoD PIV Derived PKI Credentials on Unclassified CMDs, 24 Sep 2014
- DoD Developers Page: http://www.defense.gov/developer/
- NIAP Protection Profiles: https://www.niap-ccevs.org/pp/