DoD CIO’s Areas of Focus

David A. Cotton
Deputy CIO for Information Enterprise
May 20, 2015
DoD CIO’s Areas of Focus

• Joint Regional Security Stacks
• Cloud Computing & Data Center Consolidation
• Mission Partner Environment
• Mobility
• Cyber Basics
• Business Process & Systems Review
• Pentagon IT Consolidation
  – Joint Base Pentagon
Modernization Objectives

• **More Secure**
  – Mission commanders understanding network posture
  – Network operators and defenders with shared situation awareness
  – Consistent IT architecture to enable resiliency and defensibility
  – Safe sharing with widest array of mission partners

• **More Effective**
  – Timely and secure access to data and services regardless of location or device
  – Access to information/services in the face of network disruption, degradation, or damage
  – End-to-end trustworthy connections between user and systems
  – Rapid and dynamic capability evolution to meet mission needs across all operational scenarios

• **More Efficient**
  – Reduce duplication of effort across Components, increase IT ROI, and reduce total IT operating costs
  – Consistent IT architecture to support faster fielding of new IT capabilities
  – Budget transparency for DoD IT expenditures
CIO’s Areas of Modernization

• **Network Modernization**
  – Optical Carrier Upgrades
  – Multiple Protocol Label Switching (MPLS)

• **Cyber Security Architecture**
  – Joint Regional Security Stacks (JRSS)
  – Joint Management System (JMS)
  – Perimeter, Network, Data, Endpoint Security

• **Enterprise Operations**
  – JIE Management Network
  – Enterprise Operations Centers

• **Computing Environment**
  – Data Center Consolidation / Designation
  – Commercial Cloud / Cloud Access Point
  – milCloud

• **Enterprise Services**
  – Unified Capabilities
  – Common IT apps
  – Defense Enterprise E-mail
  – Collaboration Capabilities

• **Mission Partner Environment**
  – Coalition/Partner Info Sharing
  – Mission Partner Gateway

• **Identity & Access Mgt (IdAM)**
  – Dynamic Access and Entity Discovery
  – Activity Monitoring

• **Mobility**
  – Defense Mobile Unclass Capability (DMUC)
  – Defense Mobile Classified Capability (DMCC)
CIO’s Areas of Modernization

• **Network Modernization**
  – Optical Carrier Upgrades
  – Multiple Protocol Label Switching (MPLS)

• **Cyber Security Architecture**
  – Joint Regional Security Stacks (JRSS)
  – Joint Management System (JMS)
  – Perimeter, Network, Data, Endpoint Security

• **Enterprise Operations**
  – JIE Management Network
  – Enterprise Operations Centers

• **Computing Environment**
  – Data Center Consolidation / Designation
  – Commercial Cloud / Cloud Access Point
  – milCloud

• **Enterprise Services**
  – Unified Capabilities
  – Common IT apps
  – Defense Enterprise E-mail
  – Collaboration Capabilities

• **Mission Partner Environment**
  – Coalition/Partner Info Sharing
  – Mission Partner Gateway

• **Identity & Access Mgt (IdAM)**
  – Dynamic Access and Entity Discovery
  – Activity Monitoring

• **Mobility**
  – Defense Mobile Unclass Capability (DMUC)
  – Defense Mobile Classified Capability (DMCC)
Joint Regional Security Stacks (JRSS)

- Addresses immediate need to **defend the cyber warfighting domain** & resolve JIE ICD gaps
- **Shrinks attack surface**
  - From ~1000 disparate ingress points to 50 ingress points (U&C networks)
- Achieves a **standard network security architecture**
- Accelerates achieving a **standardized Command and Control** platform for the Joint Information Environment
- JRSS suite fielded is an enabler of global **synchronized** network operations

**JRSS Value Proposition = Security + Network Modernization + Cyber SA**
Accelerate adoption of commercial clouds

- DoD Cloud Security Requirements Guide (SRG) v1, release 1, January 12, 2015
  - [http://iase.disa.mil/cloud_security/Pages/index.aspx](http://iase.disa.mil/cloud_security/Pages/index.aspx)

Promoting cloud adoption -- approved solutions:

- **Level 2 (Unclassified, Low-Impact):** 26 approved commercial cloud services with more on the way
- **Level 4/5 (Controlled Unclassified Information):** milCloud and one commercial cloud solution with more on the way
- **Level 6 (Secret):** milCloud

Cloud Access Point
Mission Partner Environment
Top Requirement for Regional Commanders

1. Chat
2. Voice
3. E-Mail w/attachments
4. Geo-Situation Awareness (aka: “COP”)
5. Video (VTC & FMV)
6. Directory / GAL
7. Web & Web Base File Sharing
8. File Share
9. Access Control
10. Office Automation
11. Print
12. Organizational Message Service (OMS)
13. Language Translation
DoD Enterprise Mobile Device Management (MDM) Evolution

Next-Gen MDM:
- Platform-Agnostic

MDM Capabilities:
- Registration
- Provisioning
- Policy Management
- Configuration
- Over-the-Air (OTA) Updates

Timeline:
- 2011: Distributed-BES 5
- 2013: Enterprise-BES 5
- 2014 - 2015: Enterprise-BES 10, Enterprise-BES 12, BB 10
- 2016+: TBD

Platforms:
- Apple iOS
- BB OS7
- BB 10
- Android
- Windows Mobile
- BlackBerry

Cloud Services:
- DMUC MDM
- MobileIron
- BlackBerry
- Android
- Windows Mobile
- Apple iOS
DoD Mobility Classified Capability (DMCC)

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

**COTS Based Solutions**
- Droid Pro
- Razr Maxx
- Samsung S4

**FY07:** SME-PED GOTS NSA designed solution
**FY12:** FISHBOWL NSA Feasibility Pilot
**FY13:** DMCC-S R1.0 NSA/DISA COTS tailored solution
**FY15:** DMCC-S & DMCC-TS R2.0 NSA/DISA COTS tailored solution
**FY16:** DMCC-S 3.0 COTS procured and integrated solution based on Commercial Solutions for Classified (CSfC)

**S/TS/SCI Capability**

**Commercial Solutions for Classified (CSfC)**
- 2G: QSEC-800, QSEC-2700, SME-PED
- 3G: Droid Pro, Razr Maxx, Samsung S4
- 4G/LTE: Droid Pro, Razr Maxx, Samsung S4

DMCC-S – DMCC Secret Device
DMCC-TS – DMCC Top Secret Device (Voice Only)
Applying Mobility Everywhere

Training → Logistics → Operations → Tactical → Training

Combat Training Centers
Army Field Inspection Tool
Android Tactical Assault Kit (ATAK)
Air Force Electronic Flight Bag

Tailored Applications Demonstrate the Advantages of Adapting to Military Needs
Cyber Basics

• Simple concepts...always been a challenge
  – Why?

• Passwords/credentials

• Patching

• Operating Systems
CIO’s Areas of Modernization

• **Network Modernization**
  – Optical Carrier Upgrades
  – Multiple Protocol Label Switching (MPLS)

• **Cyber Security Architecture**
  – Joint Regional Security Stacks (JRSS)
  – Joint Management System (JMS)
  – Perimeter, Network, Data, Endpoint Security

• **Enterprise Operations**
  – JIE Management Network
  – Enterprise Operations Centers

• **Computing Environment**
  – Data Center Consolidation / Designation
  – Commercial Cloud / Cloud Access Point
  – milCloud

• **Enterprise Services**
  – Unified Capabilities
  – Common IT apps
  – Defense Enterprise E-mail
  – Collaboration Capabilities

• **Mission Partner Environment**
  – Coalition/Partner Info Sharing
  – Mission Partner Gateway

• **Identity & Access Mgt (IdAM)**
  – Dynamic Access and Entity Discovery
  – Activity Monitoring

• **Mobility**
  – Defense Mobile Unclass Capability (DMUC)
  – Defense Mobile Classified Capability (DMCC)
How You Can Help

• Help us communicate openly, transparently, flexibly across government and industry

• Help us successfully drive cultural change across the Department’s worldwide workforce

• Help government focus on communicating requirements to industry for creating solutions