

Greg Gardner, PhD, CISSP
Colonel, U.S. Army (Retired)
Chief Architect, Defense and Intelligence, NetApp
greg.gardner@netapp.com

The Future of Federal IT: Innovation in the Department of Defense

The Challenge: “Any Information to Any Authorized User Anywhere, Anytime, Securely, Limited Only by Policy Not Technology”

The Start: June 8, 2012: “DoD’s Mobile Device Strategy identifies information technology (IT) goals and objectives to capitalize on the full potential of mobile devices. It focuses on improving three areas critical to mobility: wireless infrastructure, the mobile device itself, and mobile applications.”

A Leading Tech Company’s Approach:

- Customer Obsession
- Long Term Thinking
- If you want to be innovative, you have to be willing to fail
- You also have to be willing to be misunderstood for a long time

That Company’s Cloud-Based, Quickly-Built, Inter-Related Micro-Services:

- Each is single purpose
- Connect via APIs
- Connect over HTTPS
- Built using tools developed other teams
- Appear as a “Black Box” to one another
- Small Teams with P&L Responsibility

How the Defense Information Systems Agency (DISA) addressed the Challenge: **Defense Mobility Unclassified Capability (DMUC)** (and classified variants)

- An enterprise service that allows government purchased Commercial Mobile Devices (CMD) access to: Department of Defense Information Network (DODIN), Defense Enterprise Email (DEE), Encrypted Email capability, Access to hundreds of approved Apple and Android apps (Commercial & Government Off the Shelf),
- Mobile Device Management (MDM) capability provides the CMD and user level controls necessary to enforce security policies within and for the use of the mobile device. The purpose of the enterprise MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime.
- The Mobile Application Store (MAS) is an online digital electronic software distribution system that allows DMUC users to browse and download approved apps for their Apple or Android devices. DISA has hundreds of approved apps available in the DMUC MAS.
- An August 2018 upgrade allows government-issued devices to access any internal government network and service for unclassified purposes.
- Contractors, mission partners, services & agencies can purchase DMUC for a monthly rate of \$4.31 per device.
- DISA's mobility service keeps devices automatically up-to-date on the latest cybersecurity policies and capabilities.
- More than 200,000 people currently use DMUC & over 1,000 new devices are signed up daily, DISA notes.
- “Mission partners save time, funding and resources not having to worry about the development, implementation, operations and sustainment of the infrastructure because DISA’s DMUC service does it all for them. As new devices and software updates roll out, we are constantly testing, integrating and making them available to our DOD customers as quickly as possible” Al Smith, program manager for DMUC.
- **DMUC was the dominant communications means for Federal Government personnel responding to the recent hurricanes and flooding in the Carolinas.**
- <https://www.disa.mil/Enterprise-Services/Mobility/DOD-Mobility/DMUC>