



# Demystifying DoD Mobility

**Mark Long, Al Smith, Jaime Berrios, MAJ  
Lee, Eugene Kim, and Ethan Miller**



# Managed Mobility Enterprise Service Offerings

The DoD Mobility Portfolio Management Office provides *UNCLASSIFIED* and *CLASSIFIED* managed mobility service offerings composed of commercially available Mobile Devices and Enterprise Mobility Management solutions.

## Mobility Enterprise Services Unclassified (MES-U)

**DMUC** |

DoD Enterprise service offering enabling government owned Mobile Devices access to Unclassified Department of Defense Information Network (DoDIN) and Commercial information services.



## Mobility Enterprise Services Classified (MES-C)

**DMCC-S** |

DoD Enterprise service offering enabling government owned Mobile Devices access to Classified Secret Department of Defense Information Network (DoDIN) telephony and information services.



**DMCC-TS** |

DoD Enterprise service offering enabling government owned Mobile Devices access to Classified Top Secret select networks and Department of Defense Information Network (DoDIN) telephony services.





# DoD Mobility - Mission Partner Support

## DoD Mobility Unclassified Capability (DMUC)

*DoD Mobility Unclassified Capability* offers select iOS and Android commercial mobile devices approved by National Information Assurance Partnership (NIAP) to DoD customers.

### **DMUC: We are more than just email!**

- **Users: ~140k**
- **Provides managed service to DoD Users**
- **DMUC Mobile Application Store**
- **Purebred**
- **Signed and Encrypted Email**
- **Cybersecurity**
- **VPN into NIPR**
- **App Vetting Service**
- **DEE and NGA Mail Integration**
- **Mobile Endpoint Protection**
- **Tiered Permissions**





# DoD Mobility – Mission Partner Support

## DoD Mobility Classified Capability (DMCC)

*DoD Mobility Classified Capabilities* offer classified Secret and Top Secret collateral mobility services, utilizing devices configured against CSfC requirements, and available to customers spanning DoD, non-DoD, other federal agencies/organizations, and select non-US DMCC-S stakeholders.

### DMCC-S



- **Users: +4200**
- **Provides service to DoD, Non-DoD Federal, and select Foreign National Users (NATO, etc.)**
- **Commercial Mobile Devices and Tablets configured to comply with NSA's Commercial Solutions for Classified (CSfC) Program Office's requirements.**

### DMCC-TS

- **Users: ~110**
- **Provides service to DoD, Non-DoD Federal, and Intelligence Community users with a mission need.**
- **Commercial Mobile Devices configured to comply with CSfC requirements.**





# DoD Mobility – What’s Next?

## DoD Mobility Unclassified Capability (DMUC)

Future efforts based on official mission partner requirements, security enforcement, capability enhancement, and user experience.

### Mobile Applications



- DoD CIO Vision for Mobile Application Vetting
- Securely Deploy Enterprise Capabilities: DCS Chat, EVoIP, DTS
- Enable new capabilities via new policies and procedures: PHI and PII Apps
- Secure DoD Application Development

### Mobile Devices



- Providing Mission Partners guidance with app development
- Understand unique Mission partner requirements.
- Phones=Computers, DMUC providing simple management. Expanding Android OEM supported devices
- Supporting macOS

### Mission Partner Engagement



- Collaborate with Mission Partners and DISA organizations to provide new capabilities
- Supporting unique customer requirements
- Provide path for organizations outside of Mobility to deploy their mobile applications

### Security Compliance



- Maintain Security Compliance; remain on top of current and emerging mobile threats
- Deploy Mobile Endpoint Protection Solution
- Improve security posture through proactive collaboration; address risks with coordination with DCC, JFHQ DoDIN & RME
- Develop mechanisms for immediate action on non-compliance devices through policy and technical responses



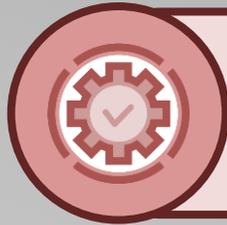
# DoD Mobility – What’s Next?

## DoD Mobility Classified Capability (DMCC)

Future efforts based on official mission partner requirements, security enforcement, capability enhancement, and user experience.

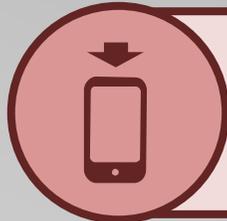
### DMCC-S

#### System Enhancements



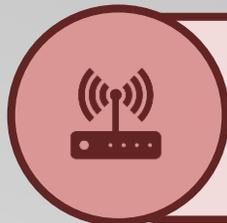
- 3rd Gateway
- Converged CSfC Gateway
- Gray CA automated CRL distribution
- Transition from NSA generated to DISA PKI generated Gray CA

#### Service Offering Enhancements



- FVEYs/Coalition support; restricted dialing based on mission partner requirements
- DAR Solution; Secure Email Client
- Piloting Win 10 Tablet

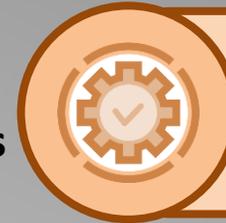
#### Device Enhancements



- Vetted and approved Dual Hotspots usage
- Vetted and approved CradlePoint usage

### DMCC-TS

#### System Enhancements



- Additional Gateway
- Standing up COOP site

#### Cyber-Security



- Partnership between DMCC CSSP stakeholders to enhance CSSP architecture and services



- **Both Capabilities are now registered against the NSA’s CSfC Mobile Access Capability Package**



**DEFENSE INFORMATION SYSTEMS AGENCY**  
The IT Combat Support Agency

 [www.disa.mil](http://www.disa.mil)

 /USDISA

 @USDISA

**DoD Mobility User Corner (CAC req'd - use email cert): [https://disa.deps.mil/ext/cop/dod\\_mobility](https://disa.deps.mil/ext/cop/dod_mobility)**

visit us

**DISA  
Booth** **1929**

follow us



Facebook/USDISA



Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at [www.disa.mil/about/industry-partners](http://www.disa.mil/about/industry-partners).