DISA
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DOD Mobility Program
Information Technology Delivery: Innovate | Operationalize | Fully Resource & Deliver

DISA is leading the Department of Defense's (DOD) efforts to create a highly mobile DOD workforce equipped with secure access to enterprise capabilities anywhere, at any time, for greater mission effectiveness. DOD Mission Partners are now empowered with the latest commercial smartphones, tablets, and mobile applications and demand these assets as necessary for increased productivity.

As a priority for the Agency, DOD Mobility offers enterprise-level classified and unclassified mobile communication services that ensure interoperability, increased security, access to information and reliable service to the mobile workforce.

Defense Mobility Unclassified Capability (DMUC)	Enterprise service 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 iOS and Android apps (commercial & government off-the-shelf) • Collaboration Mission partners, consisting of organizations within the various Combatant Commands; Services; Agencies and Field Activities (CC/S/A/FA) no longer need to develop, implement, and manage the technical infrastructure needed to connect their CMD to the network. DMUC leverages the latest commercial technology from industry carriers (Verizon, AT&T, Sprint and T-Mobile), that support operating systems from Apple and Android. DMUC has deployed a PKI derived credentials solution to allow users to do the following: • Send digitally signed and encrypted email • Decrypt encrypted email • Authenticate to DOD websites • Integrate with 3rd party applications DMUC is currently developing a Mobile Content Management (MCM) solution to access the Department of Defense Information Network (DODIN)
Defense Mobility Classified Capability - Secret (DMCC-S)	Is an enterprise service providing classified mobile access to the Secret Internet Protocol Router Network (SIPRNet). • DMCC devices are portals to the classified networks; there is no data at rest compliant with the Commercial Solutions for Classified (CSfC) process. • DMCC leverages commercial technology and products to the greatest extent possible while allowing access to SIPRNet email. • Secure voice communications via a secure Voice over Internet Protocol (VoIP) capability. Bringing these capabilities to a mobile device allows mission partners greater flexibility in secure communication. Currently, there is a DOD Mobility Classified Capability – Secret 2.0.5 fact sheet available on www.disa.mil. The fact sheet provides information on the capabilities, benefits, performance and a Quick Start Guide for the device.
Defense Mobility Classified Capability - Top Secret (DMCC-TS)	DISA Mobility is developing Top Secret – Collateral Mobile capability, Voice Only. DMCC program is delivering mobile TS collateral services, there is no data at rest compliant with the Commercial Solutions for Classified (CSfC) process. As the customer base continues to grow, the infrastructure will grow accordingly to support the additional need.