



Marine Corps Commercial Mobile Device Strategy

What is it?

The Marine Corps Commercial Mobile Device Strategy establishes a secure mobile framework (SMF) that enables the USMC to identify mobile device capability requirements, leverage existing resources, and promote the use of approved personally owned mobile devices.

With the increased use and functionality of mobile devices, maintaining security of the Marine Corps Enterprise Network (MCEN) has never been more critical. As a proactive measure against potential security threats, the SMF has been designed to ensure that standardized Information Assurance (IA) requirements are incorporated into each phase of the mobile systems design life cycle process. Ensuring that mobile devices are properly developed, procured, and tested will enhance the overall security of the MCEN and support the Marine Corps way ahead. In accordance with senior organizational strategies, and in recognition of the increasing mobile workforce requirements for IT consumerization across the DoD, this Strategy identifies four goals for mobile device implementation across the Marine Corps: 1) Establish a Secure Mobile Framework; 2) Transition the Unclassified Mobile Device Infrastructure to a Cost Effective and Platform Agnostic Environment; 3) Collaborate with DoD and Industry Partners to Develop a Classified Mobile Device Capability; and 4) Incorporate Personally Owned Mobile Devices.

Why is it important for the Marine Corps?

The demand for and use of mobile devices in the USMC has increased significantly in recent years, due primarily to their convenience, ease of use, and productivity benefits. Currently, the use of mobile devices on the MCEN is limited to those individuals deemed as privileged or mission-essential users; however, with an increase in recent trends towards teleworking and mobile computing, the Department of Defense (DoD) is starting to shift to an environment where mobile access to networks and information is no longer limited by this parameter. An example of this shift is evidenced by DoD Instruction 1035.01 (April 2012), which addresses the use of personally owned computers on unclassified DoD systems and networks. With personnel in garrison increasingly working in non-traditional workspaces, the DoD recognizes the need to access enterprise resources for performing tasks, such as delivering information or decision briefs (through development of presentations), face-to-face conversations over distance (through VTC systems), information sharing (through file and web services) and messaging, which facilitates information sharing (through email, chat, and social media).

What is the current status?

Following a thorough review and adjudication process, the Marine Corps Commercial Mobile Device Strategy was approved and signed by the Director, C4 in April 2013.

What is next?

The Marine Corps will continue participating in the DOD CIO Commercial Mobile Device Working Group, the DoN Enterprise Mobility Integrated Product Team, and working with other Federal Agencies and industry partners. This will provide greater visibility in order to eliminate duplication of efforts, and will ensure that Marine Corps mobility requirements are identified in mobile device capability development. Additional efforts involve developing an implementation plan and conducting a voluntary Bring Your Own Device (BYOD) pilot program. The implementation plan, driven by a plan of action and milestones with achievable dates, is being developed to execute the goals of the Strategy. The BYOD beta and pilot program, which supports Goal 4: Incorporate Personally Owned Mobile Devices, will be used for gathering critical data prior to future stages of execution.