



## Mobile Computing and Mobile Device Management Capabilities

### What is it?

Mobile Computing provides Army users access to Network data wherever they are, and whenever they need it. It also combines that information with situational data from mobile devices (e.g., location, events and images) via mobile applications (apps). Mobile Device Management (MDM) enables Mobile Computing in an efficient, economic, secure and defensible manner.

### Why is this important to the Army?

Mobile Computing will enhance the user experience and realize significant efficiencies. Mobile computing for many business processes, such as logistics and medical response, will increase efficiency; others will produce savings, such as replacing desktop computers with cheaper handheld devices. These capabilities will allow Soldiers to bring the strength of the entire information infrastructure to bear at the tactical edge.

### What has the Army done?

Together, the Services, the Defense Information Systems Agency and the National Security Agency released an MDM request for information. Testing and pilot programs are being coordinated with the Office of the Secretary of Defense, NSA, DISA, and the other Services. In addition, some mobile devices are becoming available through normal acquisition channels. Tablets running full Windows 7 operating systems have been cleared for connection to the Army Network. Tactical evaluations involving battlefield command and control and situational awareness are under way, as are tests of a barcode scanning app (item-unique identification) that leverages existing infrastructure and will save thousands of man-hours by automating routine transactions. The Army also is evaluating a public-facing application marketplace that will serve as the blueprint for the enterprise software marketplace.

### What continued efforts does the Army have planned for the future?

The Army will finalize requirements for the MDM solution, to include devices and mobile apps. The Army also is drafting a mobile strategy, which will be followed by a mobile concept of operations tied to DoD guidance and covering mobile computing from the tactical edge to garrison. In addition, the Chief Information Officer/G-6 is looking at comprehensive solution sets to help commanders manage data security risks associated with use of mobile devices.

ARMY CIO/G-6