DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Chief Information Assurance Executive (CIAE) 09 May 2013

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Apple iOS 6 Security Technical Implementation Guide (STIG) Version 1

Reference: DoD Directive 8500.1

1. DoD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.

2. Apple iOS 6 devices will not be deployed in the DoD without a device management infrastructure. Required iOS 6 device management components include a Mobile Device Management (MDM) server to manage device security policies and a Mobile Application Management (MAM) server to manage installed applications via an application white list. In addition, DoD Agencies, Commands, or sites deploying iOS 6 devices must set up procedures, compliant with the Mobile Application SRG, for performing a risk-based assessment of applications prior to application approval and installation.

3. Under the authority of DoD Directive 8500.1, DISA hereby releases the Apple iOS 6 STIG Version 1 for immediate use as a DoD-approved security configuration guide. The document is available on http://iase.disa.mil.

4. Point of contact for this action is FSO STIG Support Desk, email: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

ORNDORFF.MARK.STEPHEN.1045813610

MARK S. ORNDORFF
Chief, Information Assurance
Executive

UNCLASSIFIED