



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY
REFER TO: Mission Assurance Executive (MAE)

13 January 2014

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Apple iOS 7 Security Technical Implementation Guide (STIG) Version 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 7 devices will not be deployed in the DoD without a device management infrastructure. Required iOS 7 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 7 devices must set up procedures, compliant with the Mobile Application Security Requirements Guide (SRG), for performing a risk-based assessment of applications prior to application approval and installation.
3. DISA Field Security Operations (FSO) considered all the applicable technical NIST SP 800-53 requirements while developing this STIG. Requirements that are applicable and configurable are included in the final STIG. A report marked For Official Use Only (FOUO) is available for those items that did not meet requirements. The compliance report is available to component Designated Accrediting Authority (DAA) personnel for use in their certification and risk assessment of iOS7. DAA requests for the compliance report may be sent via email to disa.letterkenny.FSO.mbx.stig-customer-supportmailbox@mail.mil.
4. Under the authority of DoD Directive 8500.1, DISA hereby releases the Apple iOS 7 STIG Version 1 for immediate use as a DoD-approved security configuration guide. The document is available on <http://iase.disa.mil>.
5. 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.1045813
610

Digitally signed by
ORNDORFF.MARK.STEPHEN.1045813610
DN: cn=US, o=U.S. Government, ou=DoD, ou=PI,
ou=DISA,
c=ORNDORFF.MARK.STEPHEN.1045813610
Date: 2014.01.13 18:58:49 -0500

MARK S. ORNDORFF
Mission Assurance Executive

UNCLASSIFIED