



DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY
REFER TO: Mission Assurance (MA)

MEMORANDUM FOR DISTRIBUTION

SUBJECT: BlackBerry Enterprise Service (BES) 10.2.x Universal Device Service (UDS)
Security Technical Implementation Guide (STIG) Version 1

Reference: DoD Instruction 8500.01

DoD Instruction 8500.01 tasks DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders” and DoD Component heads “ensure that all DoD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs.”

The BES 10.2.x UDS is approved for use managing Apple iOS7 devices in the DoD. The Apple devices managed by UDS must comply with the Apple iOS7 STIG. The BES 10.2.x UDS may only be used for pilot programs with Android devices.

DISA 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. This report is available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

In accordance with DoD Instruction 8500.01, the BES 10.2.x UDS STIG Version 1 is released for immediate use. The document is available on <http://iase.disa.mil>.

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

MARK S. ORNDORFF
Mission Assurance Executive

UNCLASSIFIED