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

IN REPLY REFER TO: Mission Assurance (MA)

17 April 2014

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Samsung Android (with Knox 1.x) Security Technical Implementation Guide (STIG) Version 2

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."

Most wireless carriers add applications to mobile devices that are in addition to core applications included with the Android operating system. These additional applications are sometimes referred to as "bloatware". Bloatware applications have been found to track mobile device user activities, download usage statistics and other device data to third-party servers, and provide additional revenue opportunities for carriers. Unfortunately, it is very difficult or impossible to remove bloatware applications from Android devices. The Samsung Knox security container is used to create a work environment on the Samsung mobile device to separate DoD applications and data from the main device environment where the bloatware applications reside. When Samsung Android (with Knox 1.x) devices are used in the DoD, all applications used by the DoD must be installed in the Knox container and all DoD data must be saved in the Knox container.

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. The compliance report is available to component Designated Accrediting Authority (DAA) personnel for use in their certification and risk assessment of Samsung Android (with Knox 1.x). DAA requests for the compliance report may be sent via email to disa.letterkenny.FSO.mbx.stig-customer-supportmailbox@mail.mil.

DISA Memo, MA, Samsung Android (with Knox 1.x) STIG Version 2

In accordance with DoD Instruction 8500.01, the Samsung Android (with Knox 1.x) STIG Version 2 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.

ORNDORFF.MARK.STEPHEN.1045813610

Digitally signed by ORNDORFF.MARK.STEPHEN.1045813610
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=ORNDORFF.MARK.STEPHEN.1045813610
Date: 2014.04.17 11:49:43 -04'00'

MARK S. ORNDORFF
Mission Assurance Executive