# SAMSUNG ANDROID OS 5 WITH KNOX 2.x SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

## Version 1, Release 3

## 22 April 2016

## Developed by Samsung and DISA for the DoD

## Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

## TABLE OF CONTENTS

**Page**

## LIST OF TABLES

## 1. INTRODUCTION

### 1.1 Executive Summary

The Samsung Android OS 5 (with Knox 2.x) Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Samsung Android 5.x (with Knox 2.x) devices.

The following devices currently support the Samsung Android 5.x (with Knox 2.x) Platform:

- Galaxy S6
- Galaxy S6 Edge
- Galaxy S6 Active
- Galaxy Note 5
- Galaxy Tab S2 8" and Galaxy Tab S2 9.7"

The Samsung Android 5.x (With Knox 2.x) is also available as an update on select variations of the following devices:

- Galaxy S5
- Galaxy S4
- Galaxy Note 4, Galaxy Edge
- Galaxy Note 3
- Galaxy Tab S 10.5, Galaxy Tab S 8.4
- Galaxy Alpha

Models are continuously being added through new model launches and software updates.

### 1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (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 using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

## 1.3    Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

**Table 1-1: Vulnerability Severity Category Code Definitions**

|         | **DISA Category Code Guidelines** |
|---------|-----------------------------------|
| CAT I   | Any vulnerability, the exploitation of which will, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity. |
| CAT II  | Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity. |
| CAT III | Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity. |

## 1.4    STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

## 1.5    MDFPP Compliance Reporting

All [Mobile Device Fundamentals Protection Profile (MDFPP) or Mobile Device Management Protection Profile (MDMPP)] and DoD Annex security functional requirements (SFRs) were considered while developing this STIG. In DoD environments, devices must implement SFRs as specified in the DoD Annex to the [MDFPP or MDMPP].

Requirements that are applicable and configurable are included in this STIG.

## 1.6    Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

## 1.7    Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configurations settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of

environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100% secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

## 1.8    Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

**UNCLASSIFIED**

Samsung Android OS 5 with Knox 2.x STIG Overview, V1R3
22 April 2016
DISA
Developed by Samsung and DISA for the DoD

## 2. MOBILE DEVICE MANAGEMENT (MDM) CONFIGURATION

To implement the Samsung Android OS 5 (with Knox 2.x) STIG, a security policy created on a MDM administration console must be assigned to the target devices. For the purposes of interpreting this STIG, it is assumed that all devices in a specific group are assigned the same policy. To implement a STIG policy on Samsung Android devices, use an appropriate MDM administration tool to:

- Create a "Knox STIG" policy, and configure policy rules as specified in the Samsung Android OS 5 (with Knox 2.x) STIG
- Create a new device group named "Knox STIG Devices" and assign it the "Knox STIG" policy.

References to "Knox STIG Devices" and "Knox Policy" appear in the STIG, and are provided to facilitate comprehension of the implementation guidance. Some organizations may have multiple device groups and policies depending on the organization's concept of operations. For example, some devices may need additional restrictions placed on them for specialized use cases. For similar reasons, multiple policies may be assigned to a single device group.

### 2.1 Android Operating System Updates

The DoD is unable at this time to automatically control which core and preinstalled apps[1] from Google, Samsung, or the carriers with an operating system (OS) update. Some apps included in an OS update may have undesirable features (such as adware, bloatware, etc.) in the DoD environment.

The STIG requirement, (KNOX-35-023700), to disable automatic download and installation of carrier provided Android operating system updates must be implemented; OS updates will be controlled via the Mobile Device Management (MDM) server. Approving Official's must review/vet Android core and preinstalled apps included in any OS update to determine the risk acceptance of each app. Disapproved apps must be disabled via the MDM using the "disable API" prior to the installation of any OS update. It is recommended the Samsung Android devices and/or users be grouped by carrier on the MDM to facilitate management of OS updates.

---

[1] A core app is defined as an app bundled by the operating system vendor (for example, Google). A preinstalled app is included on the device by a third-party integrator, including the device manufacturer or cellular service provider (for example, Samsung, Verizon Wireless, or AT&T).