LG ANDROID 5.x
INTERIM SECURITY CONFIGURATION GUIDE (ISCG)
OVERVIEW

Version 1, Release 2

25 September 2015

Developed by LG 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

Page

1. INTRODUCTION

1.1 Executive Summary

The LG Android 5.x Interim Security Configuration Guide (ISCG) provides the technical security policies, requirements, and implementation details for applying security concepts to LG Android 5.x devices.

The following devices currently support the LG Android 5.x Platform:

- G3
- G4

Under the authority of DoD Directive 8500.01, DISA is releasing an interim security guide for the LG G3 and G4 smartphone with the caveat that a container application must be used to provide data separation between personal data and DoD data. Component Authorizing Officials (AO) should be aware that the use of a container application adds additional risk when compared to a mobile device that provides data separation integrated into the operating system and be prepared to accept this risk prior to deploying the LG G3 or G4 device.

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 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 ISCG 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, ISCGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Compliance Reporting

All Mobile device Protection Profile (MDFPP) and DoD Annex security functional requirements (SFRs) were considered while developing this ISCG. In DoD environments, devices must implement SFRs as specified in the DoD Annex to the MDFPP.

Requirements that are applicable and configurable will be included in this ISCG.

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/ISCGs. 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.

2. GENERAL SECURITY REQUIREMENTS

2.1 Mobile Device Management (MDM) Configuration

To implement the LG Android5.x ISCG, a security policy created on an MDM administration console must be assigned to the target devices. For the purposes of interpreting this ISCG, it is assumed that all devices in a specific group are assigned the same policy. To implement an ISCG policy on LG Android devices, use an appropriate MDM administration tool to:

- Create a "LG ISCG" policy, and configure policy rules as specified in the LG Android 5.x ISCG
- Create a new device group named "LG ISCG Devices", and assign it the "LG ISCG" policy.

References to "LG ISCG Devices" and "LG Policy" appear in the ISCG 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.

2.2 Android Operating System Updates

The DoD is unable at this time to control automatic over-the-air (OTA) operating system updates and which core and preinstalled apps[1] from Google, LG, or the carriers are installed with those updates. Some apps included in an OS update may have undesirable features (such as adware, bloatware, etc.) in the DoD environment.

The ISCG requirement (LGA5-20-002102) to disable automatic installation of carrier-provided Android operating system updates must be implemented; OS updates will be controlled via the Mobile Device Management (MDM) server. AOs 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 API "application blacklist (launch)" prior to the installation of any OS update. It is recommended the LG 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 LG, Verizon Wireless, or AT&T).