LG ANDROID 6.x STIG
SUPPLEMENTAL PROCEDURES

Version 1, Release 1

09 May 2016

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

LIST OF TABLES

1. SECURITY READINESS REVIEW

1.1 General

When conducting an LG Android 6.x Security Readiness Review (SRR), the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with LG Android 6.x, its associated network infrastructure, and the individual devices composing the system.

1.2 Mobile Policy Review

Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website at: http://iase.disa.mil/stigs/mobility/Pages/policies.aspx. Use the Mobility Policy STIG and the CMD Policy STIG to review the Smartphone Handheld asset.

2. LG ANDROID IMPLEMENTATION CONSIDERATIONS

2.1 LG Android Device Disposal

For LG Android devices never exposed to classified data, follow this procedure prior to disposing of (or transferring to another user) a mobile device via site property disposal procedures:

Note: Follow device manufacturer's instructions for wiping all user data and installed applications from device memory.

2.2 Additional Information

2.2.1 Browser Implementation Considerations

The LG browser and Chrome browsers are not FIPS 140-2 validated and therefore have been disabled via Mobile Device Manager (MDM) policy LGA6-991000-12 for the COPE#1 activation type. The browsers can be used in the personal space for COPE#2 activation type. (**Note**: COPE#1 and COPE#2 activation types are described in Section 3 below.) DoD sites deploying LG Android 6.x should select and install a FIPS 140-2 validated browser in the Work Profile. LG Electronics has a FIPS 140-2 validated browser available. Contact support-enterprise-mobility@lge.com for more information.

2.2.2 Screen Mirroring

Miracast is a screen mirroring technology that allows a tablet or smartphone screen to be projected on a TV or monitor via a Wi-Fi connection to a wireless router. Miracast is by default disabled but can be enabled by the user from the following setting:

Settings >> Networks >> Share & connect >> Miracast

Users should be trained to not enable these options unless using an approved DoD screen mirroring technology with FIPS 140-2 validated Wi-Fi. Miracast must only be used with TVs, monitors, and Miracast dongles with FIPS 140-2 validated Wi-Fi clients.

2.3 LG Fingerprints Authentication

LG Fingerprints is the fingerprint sensing system that can be used to unlock some models of LG smartphones and authorize purchases in App Stores. Fingerprints are not authorized to unlock DoD LG Android devices.

In March 2015, the Information Assurance Directorate (IAD) released the unclassified technical brief "(U) Risk Discussion for Biometrics on Mobile Devices". The IAD technical brief provides information on criteria to use when performing a risk acceptance of a biometric authentication system for a mobile device and states "The use of biometrics, prior to establishing requirements that can be used to validate implementations, creates a strategic risk that biometric templates could be harvested from weak implementations."

Version 3.0 of the Protection Profile for Mobile Device Fundamentals, to be released in early 2016, includes new design requirements and assurance activities for biometric authentication systems, including fingerprint authentication.

To date, no evaluation has been conducted on the biometric components of the LG Fingerprints feature; therefore, any AO implementing Fingerprints may be accepting an unknown risk.

3. GENERAL SECURITY REQUIREMENTS

3.1 Mobile Device Activation

DoD Android 6.x LG smartphones can be activated in one of two activation types: Corporate Owned Personally Enabled (COPE) #1 and COPE #2. With COPE #1, only one business environment is used (work or business only). With COPE #2, both work and personal environments are enabled on the device.

3.2 Management (MDM) Configuration

COPE #1 is implemented using both Google-developed Android APIs and LG-developed APIs that have been included in an MDM agent installed on the LG device. In general, MDM agents consist of common agent and LG service agent as a plugin. MDM agents are available from the Google Play app store.

COPE #2 is a hybrid form of Android for Work (AfW). The mobile domain must be registered with Google, and an Enterprise Mobility Manager (EMM) Token has to be obtained from Google and installed on the MDM server (most MDM servers have a semi-automated process for completing these steps). The domain is set up in the Work Profile mode. The Device Policy Controller (DPC) app and MDM agent (with both Android APIs and LG-developed APIs) are installed during the device provisioning process. For COPE#2, the Work Profile is managed by the DPC app while the Personal space is managed by the MDM agent.

The following table summarizes which agents are used for each activation type:

Table 3-1: App Agents Required for Device Provisioning

Application	Source	Description	Activation Type: COPE #1	Activation Type: COPE #2
MDM Agent	MDM Vendor	Common MDM Agent	✓	✓
MDM LG Service	MDM Vendor	MDM Service Agent to call LG MDM APIs	✓	✓
Device Policy Controller (DPC)	Google or MDM Vendor	Work Profile Agent for Android for Work		✓

3.3 Application Blacklist and Application Whitelist

The implementation of application blacklist and whitelist policy controls for both COPE #1 and COPE #2 are somewhat complex. Please see the Configuration Tables document for a listing of all blacklist and whitelist controls. The following list summarizes how the controls are implemented and work together.

Table 3-2: Application Blacklist and Whitelist Policy Control Capabilities

User Action	Blacklist	Whitelist	Comment
Install	Yes	Yes	Blacklist: User CANNOT install Apps on the blacklist Whitelist: User can install only Apps on the whitelist
Uninstall	Yes	Yes	Blacklist: User CANNOT uninstall Apps on the blacklist Whitelist: User can uninstall Apps only on the whitelist
Launch	Yes	No	Blacklist: User CANNOT run Apps on the blacklist Whitelist: NA – not supported

Note: Blacklist and Whitelist controls cannot be used together in same user action. For example, an app should not be listed both on the App Install Blacklist and App Install Whitelist; otherwise, the operating system will not know which control to enforce. The LG platform supports all blacklist and whitelist controls, but the MDM Administrator must decide if a blacklist or whitelist control will be used to accomplish a specific action.

3.4 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 STIG requirement (LGA6-201031-01) 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. Authorizing Officials (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.

4. CORE AND PREINSTALLED APPLICATIONS

4.1 Disabled Applications

Table A-1 lists core and preinstalled applications that should be disabled. Risk in using these apps in the DoD environment is considered to be high. DoD Commands and Agencies should fully vet these apps, using the Application Software Protection Profile (APPSWPP), prior to approving their use.

4.2 Enabled Applications

Table A-2 lists core and preinstalled applications that are recommended for approval. DoD Commands and Agencies should consider vetting these apps using the Application Software Protection Profile (APPSWPP).

4.3 Auditing/Reviewing Device Applications

Applications are controlled by APIs: application whitelist (install/uninstall) and application blacklist (install/uninstall/launch). The application whitelist and blacklist are used to control installed, core, and preinstalled applications. Approved core and preinstalled applications are added to the whitelist so that updates can be installed. The blacklist control is used to disable undesirable/unapproved core and preinstalled applications and to disable the capability for installing unapproved applications. Core and preinstalled applications listed on the application blacklist are not removed from the device but cannot be launched by the user.

The following procedures are recommended for performing an audit/review of applications on LG Android devices:

1. Installed applications
    - Review the list of applications listed on the whitelist on the MDM Administration console.
    - Verify all apps on the list have been approved by the AO.
      Note: Core and preinstalled applications included in Table A-2 are considered approved for DoD use unless expressly disapproved by the AO.
2. Core and preinstalled applications
    - View the blacklist of applications on the MDM console.
    - Tap the “Apps” menu button on the LG device to view all installed apps.
    - Verify that all apps on the blacklist cannot be launched.
    - Generate a list of applications installed on the LG device:
        - Tap the “Apps” menu button on the device to view all installed apps.
        - Remove any app on the whitelist from this list.
          Note: The whitelist may include approved installed, core and preinstalled apps.
        - Verify all apps remaining on the list of installed applications on the device have been approved by the AO.

APPENDIX A: APPLICATION LISTS

Table A-1: Applications Recommended for Disapproval

Application Package Name	Application Name
com.amazon.kindle	Amazon Kindle
com.amazon.mp3	Amazon Music
com.amazon.mShop.android	Amazon
com.audible.application	Audible
com.android.chrome	Chrome (For COPE#1 activation type only)
com.google.android.apps.cloudprint	Cloud Print
com.vcast.mediamanager	Cloud
com.google.android.apps.docs	Drive
com.google.android.gm	Gmail
com.google.android.apps.books	Google Play Books
com.google.android.play.games	Google Play Games
com.google.android.videos	Google Play Movies & TV
com.google.android.music	Google Play Music
com.google.android.apps.magazines	Google Play Newsstand
com.google.android.apps.plus	Google+
com.google.android.talk	Hangouts
com.imdb.mobile	IMDb
com.lge.bnr	LG Backup
com.google.android.feedback	Market Feedback Agent
com.vzw.hss.widgets.infozone.large	My InfoZone
com.vzw.hss.myverizon	My Verizon Mobile
com.gotv.nflgamecenter.us.lite	NFL Mobile
com.slacker.radio	Slacker Radio
com.asurion.android.verizon.vms	VZ Protect (Support & Protection)
com.lge.lgdmsclient	System updates
com.telecomsys.directedsms.android.SCG	Verizon Location Agent
com.motricity.verizon.ssodownloadable	Verizon Login
com.vznavigator.Generic	VZ Navigator
com.google.android.youtube	VZ YouTube
com.telenav.app.android.cingular	AT&T Navigator
com.wildtangent.android	Games
net.aetherpal.device	AT&T Remote Support
com.matchboxmobile.wisp	AT&T Hot Spots
com.att.android.attsmartwifi	AT&T Smart Wi-Fi
com.lge.aab	AT&T Address Book
com.lge.lgworld	SmartWorld
com.twitter.android	Twitter
com.asurion.android.mobilerecovery.att	AT&T Protect Plus
com.facebook.katana	Facebook
com.ubercab	Uber

Application Package Name	Application Name
com.wavemarket.waplauncher	AT&T FamilyMap
com.att.myWireless	myAT&T
com.lookout	Lookout
com.mobitv.client.tv	Mobile TV
com.android.chrome	Chrome
com.android.browser	Browser (For COPE#1 activation type only)
com.yahoo.mobile.client.android.mail.att	AT&T Mail
com.google.android.apps.walletnfcrel	Android Pay
com.google.android.apps.docs.editors.docs	Docs
com.google.android.apps.docs.editors.sheets	Sheets
com.google.android.apps.docs.editors.slides	Slides
com.lge.appbox.client	App Updates
com.lge.myplace	My Places
com.lge.lgdmwebviewer4vzw	System updates
com.instagram.android	Instagram
com.google.android.apps.photos	Photos
com.directv.drvscheduler	DIRECTV
Com.americanexpress.plenti	Plenti

Table A-2: Applications Recommended for Approval

Application Package Name	Application Name
com.android.settingsaccessibility	Accessibility
android	Android System
com.android.bluetooth	Bluetooth
com.android.browser	Browser (for COPE#2 activation type only)
com.android.calculator2	Calculator
com.android.providers.calendar	Calendar Storage
com.android.calendar	Calendar
com.android.incallui	Call
com.cequint.ecid	Caller Name ID
com.lge.camera	Camera
com.android.captiveportallogin	CaptivePortalLogin
com.android.certinstaller	Certificate Installer
com.android.chrome	Chrome (For COPE#2 activation type only)
com.lge.clock	Clock
com.android.backupconfirm	com.android.backupconfirm
com.android.wallpapercropper	com.android.wallpapercropper
com.android.providers.contacts	Contacts Storage
com.android.contacts	Contacts
com.lge.privacylock	Content Lock
com.android.managedprovisioning	Device Provisoner
com.android.documentsui	Documents
com.android.providers.downloads	Download Manager
com.android.providers.downloads.ui	Downloads
com.lge.drmservice	DRM Service
com.LogiaGroup.LogiaDeck	DT Ignite
com.lge.easyhome	EasyHome
com.lge.eltest	ELTest
com.lge.email	Email
com.lge.cmas	Emergency Alerts
com.lge.filemanager	File Manager
com.lge.formmanager	FormManager
com.android.gallery3d	Gallery
com.lge.gnss.airtest	GNSS Air Test
com.lge.gnsstest	GnssTest 1.2
com.google.android.gsf.login	Google Account Manager
com.google.android.partnersetup	Google Partner Setup
com.google.android.gms	Google Play Services
com.android.vending	Google Play Store
com.google.android.googlequicksearchbox	Google App
com.google.android.gsf	Google Services Framework
com.google.android.tts	Google Text-to-speech Engine
com.lge.helpcenter	Help

Application Package Name	Application Name
com.lge.homeselector	Home Selector
com.lge.launcher2.theme.optimus	Home Theme - LG
com.lge.launcher2 (or com.lge.launcher3)	Home
com.android.htmlviewer	HTML Viewer
com.android.keychain	Key Chain
com.lge.gnsspostest	LG GNSS 2.1
com.lge.lifetracker	LG Health
com.lge.ims	LG IMS
com.lge.ime.theme.black	LG Keyboard Black Theme
com.lge.ime	LG Keyboard
com.lge.sync	LG Bridge Service
com.ipsec.vpnclient	LG VPN
com.lge.android.atservice	LGATCMD Service
com.android.LGSetupWizard	LGSetupWizard
com.lge.smartcover	LGSmartCover
com.lge.eulaprovider	License Provider
com.android.wallpaper.livepicker	Live Wallpaper Picker
com.qualcomm.location	LocationServices
com.lge.lockscreensettings	Lock Screen Settings
com.maluuba.android.qvoice	Maluuba Qvoice Interface
com.google.android.apps.maps	Maps
com.android.providers.media	Media Storage
com.verizon.messaging.vzmsgs	Message+
com.android.mms	Messaging
com.lge.livewallpaper.multiphoto	Multi-photo
com.lge.music	Music
com.android.nfc	NFC Service
com.android.packageinstaller	Package Installer
com.android.phone	Call Services (or Phone)
com.lge.networksettings	Network (or Phone)
com.android.printspooler	Print Spooler
com.lge.hotspotprovision	Provision
com.lge.qmemoplus	QuickMemo+
com.lge.qremote	QuickRemote
com.lge.servicemenu	ServiceMenu
com.android.settings	Settings
com.lge.settings.easy	Settings
com.google.android.setupwizard	Setup Wizard
com.lge.AppSetupWizard	Setup Wizard
com.android.shell	Shell
com.android.stk	SIM Toolkit
com.lge.springcleaning	Smart Cleaning
com.lge.concierge	Smart Notice

Application Package Name	Application Name
com.lge.doyouknow	Smart Tips
com.lge.smartsharepush	SmartShare Push
com.lge.smartshare.dlna	SmartShare.DLNA
com.lge.smartshare	SmartShare.MediaServer
com.lge.lgfota.permission	FOTA Test
com.android.systemui	System UI
com.google.android.tag	Tags
com.google.android.marvin.talkback	TalkBack
com.lge.thinkfreeviewer	ThinkFree Viewer
com.lge.touchcontrol	Touch Control Areas
com.android.facelock	Trusted Face
com.lge.eula	Unified EULA
com.lge.videoplayer	Video
com.lge.videotool	Video Trim
com.lge.voicecommand	Voice Command
com.lge.vvm	Voice Mail
com.lge.qvoiceplus	Voice Mate
com.lge.voicerecorder	Voice Recorder
com.android.vpndialogs	VpnDialogs
com.lge.wapservice	WAP Service
com.lge.sizechangable.weather	Weather
com.lge.sizechangable.weather.platform	Weather Service
com.lge.wv.hidden	Widevine Keybox Test
com.lge.ime.dictionary.xt9	Xt9 Dictionaries
com.lge.shutdownmonitor	Shutdown Monitor
com.lge.pcsyncui (or com.lge.remote.setting)	LG AirDrive
com.lg.ATTDeviceHelp	DeviceHelp
com.drivemode	DriveMode
com.lge.settings.shortcut	Usage Manager
com.google.android.inputmethod.latin	Google Keyboard
com.yellowpages.android.ypmobile	YP
com.lge.acms	Message Backup & Sync
com.cequint.ecid	Caller Name ID
com.lge.exchange	Exchange
com.locationlabs.cni.att	Smart Limits
com.lge.bluetoothsetting	Bluetooth
com.lge.wifisettings	Wi-Fi
com.lge.LGSetupView	EULA
com.lge.hotspotlauncher	Mobile Hotspot
com.lge.videostudio	Quick Video Editor
com.crucialsoft.fido.client	CrucialTec FidoClient
com.lge.email	Email