MOTOROLA SOLUTIONS ANDROID 11 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 2

26 August 2022

Developed by Motorola Solutions DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Motorola Solutions Android 11 Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Motorola Solutions (MSI) LEX L11 handheld devices running Android 11 that process, store, or transmit unclassified data marked as "Controlled Unclassified Information (CUI)" or below.

This STIG leverages the Google Android 11 STIG. All requirements in this STIG are based on the Google Android 11 STIG with several Motorola Solutions-specific changes.

The scope of this STIG covers the Corporate Owned Business Only (COBO)[1] use case. The Corporate Owned Personally Enabled (COPE), Bring Your Own Device (BYOD), and Choose Your Own Device (CYOD)[2] use cases are not in scope for this STIG.

Note: This STIG requires that a NIAP-approved version of Android 11 be installed on DoD-owned MSI LEX L11 Android phones. See the STIG Requirement MOTS-11-010800 for more information.

Note: If the Authorizing Official (AO) has approved the use/storage of DoD data in one or more personal (unmanaged) apps, allowing unrestricted activity by the user in downloading and installing personal (unmanaged) apps on the MSI LEX L11 device may not be warranted due to the risk of possible loss of or unauthorized access to DoD data.

This STIG assumes that if a DoD Wi-Fi network allows an MSI LEX L11 device to connect to the network, the Wi-Fi network complies with the Network Infrastructure STIG; for example, wireless access points and bridges must not be connected directly to the enclave network.

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.

[1] Work data/apps only – no personal data/apps

[2] Similar to BYOD, but only select models of personal devices are allowed.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls must 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

Category	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 DoD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 MDFPP Compliance Reporting

All Mobile Device Fundamentals Protection Profile (MDFPP) 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.

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 configuration 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 AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DoD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable 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 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 the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (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) (https://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. LEX L11 OVERVIEW

The Motorola Solutions LEX L11 is a ruggedized Android 11 device designed for mission-critical use cases. The LEX L11 can be configured during initial deployment for either the COBO use cases (also called Device Owner), or the COPE use cases (Profile Owner) but only the COBO use case is approved for use in the DoD at this time.

2.1 LEX L11 Description

The LEX L11 is a high-end smartphone that is a purpose-built, mission-critical LTE device to meet the needs of public safety users. It is a mobile device to support enterprises and individual users alike. The Android 11 operating system includes a Linux 4.19 kernel. Additional libraries are provided to developers to help ensure secure application development and use for features such as Sensitive Data Protection.

Figure 2-1: LEX L11 Device

2.2 LEX L11 Android Enterprise Compliance

LEX L11 is fully compliant with GMS (Google Mobile Services). It is certified for GMS each time before publishing an official release. LEX L11 using Android 11 is in the process to be certified as an Android Enterprise Recommended (AER) rugged device. Note that it is already certified as an Android 9 AER rugged device. This implies that any Mobile Device Management (MDM) system certified for Android Enterprise can be used on the LEX L11. The customer can choose any of the MDMs and use those to configure the LEX L11.

LEX L11 is fully compliant with Android Enterprise provisioning/enrollment methods, including QR Code, NFC, Google Account, Zero-Touch for both COBO and COPE provisioning. Zero-Touch simplifies the out-of-the-box experience and enables enterprise customers to automatically provision devices they own with no administrator/user action required.

Details about the Android Enterprise Recommended program and the different components can be found in Google Android Enterprise documentation.

2.2.1 LEX L11 Enterprise Work Profile Support

The enterprise program enables the administrator to define a work profile on the device. Fully managed devices with work profiles are for company-owned devices used for both work and personal purposes. This is equivalent to COPE deployment, meaning the organization still manages the entire device. However, the separation of work data and apps into a work profile allows organizations to enforce two separate sets of policies. For example:

- Stronger set of policies for the work profile that applies to all work apps and data
- More lightweight set of policies for the personal profile that applies to the user's personal apps and data

LEX L11 supports enterprise WORK profiles to provide separation between private user applications and work (enterprise) applications, including the separation of private and enterprise applications' data. That is, applications installed into the enterprise versus personal profiles cannot access each other's secure data and applications and can have separate device administrators/managers. This functionality is built into the device upon being enrolled as COPE and it does not require an application download.

2.3 LEX L11 Security Overview

LEX L11 has enhanced software and hardware security components in order to meet the highest information assurance and integrity standards. LEX L11 supports all kinds of network authentications and encryption and provides the means for applications (such as TLS lib-s, Keystore) to support end-to-end encryption.

LEX L11 includes several different levels of execution including (from lowest to highest) hardware, a Trusted Execution Environment, Android's Linux kernel, Android's user space, Android's Android Runtime (ART) environment for mobile applications, and the mobile applications themselves. LEX L11 owns a secure mobile platform with multiple levels of security to protect devices' data and communication.

Figure 2-2: LEX L11 Security Platform Functions

TRUSTED BOOT PROCESS	Automatically checks the authenticity and integrity of the firmware during the device boot processes.
REAL-TIME INTEGRITY	Detect and prevent tampering of firmware and the injection of malware into the running firmware and receive alerts of attempted breaches.
OPERATING SYSTEM AND APPLICATIONS	The Operating System and applications on the LEX L11 are security hardened following and adapting industry best practices and standards.
REAL-TIME PROTECTION OF OPERATING SYSTEM AND APPLICATIONS	Real-time defense against device rooting, privilege escalation, zero days, code execution flow attacks, malware installation/ execution, bypass of internal kernel security and access controls.
SECURE DEVICE MANAGEMENT AND CONFIGURATION	Secure device management based on industry standards with control capability including remote configuration, remote firmware and software upgrades, application whitelisting, and over-the-air wipe and lock capability.
POLICY-BASED CONTROLS AND RESOURCE MANAGEMENT	Restricts which applications may run on the LEX L11, as well as which applications the user may access. Additionally restrict device resources applications and the user may access (for example: camera, microphone, contacts list, etc.).
DATA-AT-REST AND DATA-IN-TRANSIT SECURITY	Credentials, certificates, keys and all other device data is securely stored when at rest as well as in transit. Configurable enhanced “data at rest” encryption based on AES256 (NIAP certified).
DEVICE USER	The LEX L11 supports configurable single-factor and multifactor authentication, including PIN and fingerprint.
AUDITING/ LOGGING	Security and operational event logging is done by the operating system and applications to produce retrievable audit trails for troubleshooting, security monitoring, and forensics.
RESTRICTED RECOVERY MODE	Enhanced fastboot mode to block uncertified image upgrade.
ENHANCED VPN RESTRICTIONS	Block outbound traffic when VPN is enabled.

2.3.1 LEX L11 Commercial Solutions for Classified (CSfC) and NIAP Compliance

The CSfC Program provides the ability to securely communicate based on commercial standards, protocols, algorithms, and modes to meet stringent NSA directives for classified information in solutions, ensuring users are equipped with devices at the cutting edge. This includes:

- Hardened device
- Protecting data at rest and in transit
- Controlling, managing, and enforcing mobile security policies

LEX L11 using Android 11 is in the process to be certified for NIAP and CSfC.

Note that LEXL11 is already certified for CSfC and NIAP for Android 9 (refer to Figure 3). It leverages the National Security Agency (NSA) cryptography standards that promote the CSfC protection profiles for secure sharing of classified information over wireless mobile networks.

LEX L11 Android 9 is compliant with NIAP-approved Protection Profile for Mobile Device Fundamentals. Evaluation was carried out in accordance with the NIAP Common Criteria. (Refer to LEXL11 NIAP Certificate.)

Figure 2-3: LEX L11 NIAP Compliance

Product	Carrier	OS version	Kernel	Build number	WFA Cert#
Motorola Lex L11	Open	Android 9.0	4.4.153	PIE.L11_P_R30.21.10	WFA91727

2.3.2 LEX L11 Auditing and Logging

Security and operational event logging is done by the operating system and applications to produce retrievable audit trails for troubleshooting, security monitoring, and forensics. LEX L11 leverages the standard Android logging mechanism to record the auditable events to help monitor secure-related objectives. For this purpose, Android logs are configured to record each audit record, including date and time of events, type of event, subject identity, and outcome of the event. Thus, the integrity of audit logs must be protected from modification. This protection is achieved by SELinux policy and DAC.

LEX L11 logging methods are described below:

- **Security Logs:** A table that depicts the list of all auditable events can be found here: https://developer.android.com/reference/android/app/admin/SecurityLog. The following link provides the additional information that can be grabbed when an MDM requests a copy of the logs: https://developer.android.com/reference/android/app/admin/SecurityLog.SecurityEvent. Each log contains a keyword or phrase describing the event, the date and time of the event, and further event-specific values that provide success, failure, and other information relevant to the event.
  - These logs can be read by an administrator via an MDM agent.
- **Logcat Logs:** Similar to Security Logs, Logcat Logs contain date, time, and specific values within the logs. In addition, Logcat Logs provide a value that mapped to a user ID to identify which user caused the event that generated the log. Logcat Logs tend to be more human-readable than Security Logs and are descriptive, not requiring the user to know the template of the log or code values to understand its reported values.
  - Logcat Logs can be configured to be exported to SD card and can always be viewed via an ADB shell to the device.
  - For the Logcat Logs, logging policy can be configured by MDM: Level of audit, log size, and list of logs to be recorded.