GOOGLE ANDROID 13
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

30 January 2025

Developed by Google 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 the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Google Android 13 Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Google Android devices running Android 13 that process, store, or transmit unclassified data marked as Controlled Unclassified Information (CUI) or below. The STIG is based on the Protection Profile for Mobile Device Fundamentals (MDFPP) version 3.2 STIG template. Requirements compliance is achieved by leveraging a combination of configuration profiles, user-based enforcement (UBE), and reporting.

The scope of this STIG covers Corporate Owned Personally Enabled (COPE) and Corporate Owned Business Only (COBO)[1] use cases. The Bring Your Own Approved Devices (BYOAD)[2] use case is not included.

This STIG assumes that for the COPE use case, the technology used for data separation between work apps, data and personal apps, and data that has been certified by the National Information Assurance Partnership (NIAP) is compliant with the data separation requirements of the MDFPP[3]. As of the publication date of this STIG, the only data separation technology or application that is NIAP-certified for a Google Android 13 device is the native Android Enterprise work profile technology.

The configuration requirements and controls implemented by this STIG allow unrestricted activity by the user in downloading and installing personal (unmanaged) apps and data (music, photos, etc.) with Authorizing Official (AO) approval and within any restrictions imposed by the AO. Refer to the STIG Supplemental document, Section 6.2, Configuration of Personal Space, for more information.

Zero-touch enrollment enables large-scale Android deployments across multiple device makers so organizations can mobilize their employees with ease. Zero-touch enrollment allows DOD mobile service providers to deploy corporate-owned devices (COBO and COPE) in bulk without having to manually set up each device. It is recommended that DOD mobile service providers consider deploying all Google Android devices via the zero-touch enrollment service to improve enterprise management, control, and enrollment of DOD-owned Google Android 13 phones and tablets. Refer to the STIG Supplemental document, Section 3.3.1, COPE Deployments and User Privacy, for more information.

Note: If the AO has approved the use/storage of DOD data in one or more personal apps, allowing unrestricted activity by the user in downloading and installing personal apps on the Google Android 13 device may not be warranted due to the risk of possible loss of, or unauthorized access to, DOD data.

---

[1] Work data/apps only – no personal data/apps
[2] Also called Choose Your Own Device (CYOD).
[3] The primary Protection Profile requirement is FDP_ACF_EXT.1.2.

This STIG assumes that if a DOD Wi-Fi network allows a Google Android 13 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

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that 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 [National Security Agency/Central Security Service], 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 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 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). Department of Defense 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.
- DODIN Approved Products List (APL) (https://aplits.disa.mil/processAPList.action) IAW DODI 8100.04.