National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

GovShield Version 1.60.05

Report Number: CCEVS-VR-VID11590-2026
Version 1.0
June 08, 2026

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATT: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Swapna Katikaneni, Senior Validator - Aerospace Corporation
Patrick Mallett, Ph. D., Lead Validator - Aerospace Corporation
Seada Mohammed, Lead Validator (Trainee) - Aerospace Corporation

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Rachel Kovach
Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of GovShield Version 1.60.05 provided by General Dynamics Mission Systems. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in May 2026. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the

The PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, January 27, 2020. [CFG_MDM-MDM_AGENT_V1.0] includes the following components:

- Base-PP: Protection Profile for Mobile Device Management, Version 4.0 (PP_MDM_V4.0)
- PP-Module: PP-Module for MDM Agents, Version 1.0 (MOD_MDM_AGENT_V1.0)

The TOE is a Mobile Device Management product and is comprised of an MDM Server component (GovShield Server) and one or more agent components called GovShield Clients. The GovShield Server component provides a centralized enterprise level management capability for a collection of Android Mobile Devices running GovShield Clients. The GovShield Server is also a Mobile Application Store (MAS) Server that allows managed devices to download apps from a trusted repository that resides within the organization managing the device. The management functionality includes management of Administrators and MD users, mobile device enrollment, mobile device status, mobile device policy management, and application management. Administrators access the GovShield Server through a browser-based web GUI on an Administrative Workstation in order to manage users, policies, and the Android Mobile Devices.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the NDcPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the NDcPP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *GovShield Version 1.60.05 Security Target v1.0*, dated February 6, 2026, and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	GovShield Version 1.60.05
Protection Profile	Protection Profile for Mobile Device Management, version 4.0 [MDMPP] Protection Profile Module for Mobile Device Management Agents, version 1.0 [AGENTMOD]
Security Target	GovShield Version 1.60.05 Security Target v1.0, dated February 6, 2026
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "GovShield Version 1.60.05" Evaluation Technical Report v1.0 dated May 27, 2026
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	General Dynamics Mission Systems
Developer	General Dynamics Mission Systems
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Swapna Katikaneni, Senior Validator - Aerospace Corporation Patrick Mallett, Lead Validator - Aerospace Corporation Seada Mohammed, Lead Validator (Trainee) - Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- **A.COMPONENTS_RUNNING** (applies to distributed TOEs only) – [MDMPP] For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
- **A.CONNECTIVITY** – The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
- **A.MDM_SERVER_PLATFORM** – [MDMPP] The MDM Server relies upon a trustworthy platform and local network from which it provides administrative capabilities. The MDM Server relies on this platform to provide a range of security-related services including reliable timestamps, user and group account management, logon and logout services via a local or network directory service, remote access control, and audit log management services to include offloading of audit logs to other servers. The platform is expected to be configured specifically to provide MDM services, employing features such as a host-based firewall, which limits its network role to providing MDM functionality.
- **A.MOBILE_DEVICE_PLATFORM** – [AGENTMOD] The MDM Agent relies upon mobile platform and hardware evaluated against the MDF PP and assured to provide policy enforcement as well as cryptographic services and data protection. The mobile platform provides trusted updates and software integrity verification of the MDM Agent.
- **A.PROPER_ADMIN** – One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
- **A.PROPER_USER** – Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.MALICIOUS_APPS** – [MDMPP] Malicious or flawed application threats exist because apps loaded onto a mobile device may include malicious or exploitable code. An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE, resulting in the compromise of TOE or TOE data.
- **T.BACKUP –** [AGENTMOD] An attacker may try to target backups of data or credentials and exfiltrate data. Since the backup is stored on either a personal computer or end user's backup repository, it's not likely the enterprise would detect compromise.
- **T.NETWORK_ATTACK** – [MDMPP] An attacker may masquerade as an MDM Server and attempt to compromise the integrity of the mobile device by sending malicious management commands.
- **T.NETWORK_EAVESDROP –** [MDMPP] An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the MDM Server and other endpoints.

- **T.PHYSICAL_ACCESS –** Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the *Protection Profile for Mobile Device Management, version 4.0 [MDMPP] and the Protection Profile for Mobile Device Management Agents, Version 1.0 [AGENTMOD]*, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the MDMPP are claimed by the TOE and documented in the ST.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. All other functionalities provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

The evaluated configuration of the TOE is the GovShield Version 1.60.05 comprising of the GovShield Server and one or more GovShield Clients installed on Android Mobile Devices. The minimum configuration for this evaluation is one GovShield Server, and one GovShield Client installed on an Android Mobile Device. Including additional GovShield Clients installed on multiple Android Mobile Devices as part of an operational configuration will not affect the validity of the functional claims made within this document and the Common Criteria certification.

In the evaluated configuration, the TOE uses the following protocols to secure transmission of security-relevant data:

- HTTPS to secure remote command-line administration and connections between the GovShield Server and the GovShield Client.
- TLSv1.2 to secure transmission to an Oracle Database server in the operational environment.

The TOE includes administrative guidance in order to instruct Security Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The TOE is a Mobile Device Management product consisting of the GovShield Server and one or more GovShield Clients which run on mobile devices. The [MDMPP] states:
"The MDM Server is software (an application, service, etc.) on a general-purpose platform, a network device, or cloud architecture executing in a trusted network environment. The MDM Server provides administration of the mobile device policies and reporting on mobile device behavior. The MDM Server is responsible for managing device enrollment, configuring and sending policies to the MDM Agents, collecting reports on device status, and sending commands to the Agents. The MDM Server may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfill the requirements of this PP."

The MDM Server TOE type is justified because the TOE software provides centralized enterprise level management capabilities for MDM Agents (GovShield Clients) running on mobile devices, including enrollment, policy management and device status and the MDM Server (GovShield Server) runs on Microsoft Windows Server 2022, which is a general-purpose platform.

This statement is re-iterated in the [AGENTMOD]. The MDM Agent TOE type is justified because the MDM Agent software (GovShield Client) is installed on a mobile device as an application developed by General Dynamics Mission Systems and establishes a secure connection back to the MDM Server (GovShield Server) protected by HTTPS.

4.2 Physical Boundary

The TOE is a software product. All hardware that is present is part of the TOE's Operational Environment.

The GovShield Server runs on an environment containing Windows Server 2022, OpenJDK 11, and JBoss EAP 7.4. The software version of the GovShield Server is 1.60.05.

The GovShield Client runs on the Android 15 operating systems in its evaluated configuration. The software version of the GovShield Client is 1.60.05.

The following table identifies the operational environment.

Component	Definition
Android Mobile Device	The MDM Agent Component of the TOE (GovShield Client) is an application that is installed on mobile devices running the Android 15 operating system; so that the TOE can provide management functionality to the device.
Certification Authority (CA) Server	The GovShield Server connects to the CA Server during device enrollment so that the TOE can provide each Android Mobile Device with a unique X.509v3 certificate generated by the CA Server.

E-FOTA Server	Samsung Knox Enterprise Firmware-over-the-air (E-FOTA) Server allows the TOE Administrators to push firmware updates to one or more enrolled Android Mobile Devices.
Java Runtime Environment	Java Runtime Environment is installed on the Windows Server 2022 and provides resources to Java based programs. JBoss EAP and subsequently the TOE operate on this runtime environment. In the evaluated configuration, OpenJDK 11 is used.
JBoss EAP	JBoss Enterprise Application Platform (EAP) is a Java based application server on which the TOE is installed. In the evaluated configuration, JBoss EAP 7.4 is used.
Oracle Database	The RDBMS database used to store the TOE's audit, configuration settings, and device data. In the evaluated configuration, Oracle Database 19 is used.
Samsung Knox Licensing Server	The TOE communicates with the Samsung Knox Licensing Server to verify the Knox licensing key provides to the GovShield Client on an Android Mobile Device. Once the key is verified by the Samsung Knox Licensing Server, it will activate the Android Mobile Device's Knox platform which provides the TOE access to enterprise functions of the Android Mobile Device.
Windows Server 2022	This is the OS that the GovShield Server is installed on.
Workstation	Any general-purpose computer that is used by an Administrator to manage the TOE. For the TOE to be accessed remotely, the workstation is required to have a browser to access the TOE's GUI based interface.

Table 5 – IT Environment Components

5 Security Policy

5.1.1 Security Audit

The GovShield Server component of the TOE creates audit records for auditable events related to administrative actions, configuration of the GovShield Server itself, and server-initiated management activities that affect one or more managed Android Mobile Devices. The GovShield Server's MAS Server functionality also generates audit records when it experiences a failure to push or update an application on a managed mobile device. The audit records are stored in a remote Oracle Database and transferred over a TLS encrypted trusted channel. Audit records can be viewed in the web GUI.

The GovShield Server provides Authorized Administrators with the ability to view information about enrolled mobile devices and to review alerts when various events occur. Alerts are generated based on information provided by the GovShield Client during a reachability event. The GovShield Client also generates audit records for the activities it performs as a result of its interactions with the GovShield Server.

5.1.2 Communication

The GovShield Client's Android Mobile Devices are registered with the GovShield Server for enrollment. This requires an Administrator to enable communications between these TOE components by managing a whitelisted set of Android Mobile Devices that are allowed to enroll with the GovShield Server. The enrollment process occurs over an HTTPS/TLS trusted channel that is handled by each TOE components' underlying platform. An Administrator can disable the communications between a GovShield Client and the GovShield Server by unenrolling or wiping the enrolled Android Mobile Device.

5.1.3 Cryptographic Support

Cryptographic services for the GovShield Server and the GovShield Client are provided by their respective underlying platforms. The cryptographic services include encryption/decryption services, credential/key storage, key establishment, key destruction, hashing services, signature services, and hashed message authentication. All cryptographic services use the respective TOE components' platform provided DRBG functionality to support their cryptographic operations.

The GovShield Server invokes the Java Runtime Environment Platform and its BSafe cryptographic library for cryptographic services to establish TLS and HTTPS/TLS trusted channels and paths to ensure secure communications of data in transit. The MAS Server is integrated with the GovShield Server, so it invokes the same cryptography services. The GovShield Server also invokes its platform to digitally sign policies sent to the GovShield Clients.

The GovShield Client invokes its underlying Android Mobile Device platform's BoringSSL cryptographic module for cryptographic services to also establish trusted communications. The GovShield Client also invokes its underlying platform to verify the digital signatures of all policies received from the GovShield Server.

5.1.4 Identification and Authentication

The GovShield Client registers with the GovShield Server so that the Android Mobile Device can be enrolled into management by the GovShield Server. This is accomplished by MD user or Administrator installing the GovShield Client software using a QR code, and then entering their authentication credentials through the GovShield Client interface. This will initiate the enrollment connection to the GovShield Server. The GovShield Server will authenticate the user as well as verify that the Android Mobile Device is allowed to enroll based upon being included within a whitelisted set of Android Mobile Devices. The GovShield Server will then send the GovShield Client its initial payload to include a unique X.509v3 certificate for trusted communications and the public key to verify the signature of policies. The GovShield Client then downloads its assigned policy from the GovShield Server to complete the enrollment process.

Administrators (through the web GUI and GovShield Client) and MD users (through the GovShield Client) cannot access the GovShield Server without being authenticated. Administrators and MD users can view the configurable consent warning banner prior to authentication via their respective interfaces.

The GovShield Server relies on the underlying platform to provide X.509v3 certificate services for signing policies that are sent to GovShield Client. The GovShield Server also relies on its platform to provide its X.509v3 certificate as part of TLS and HTTPS/TLS session establishment in all cases where the GovShield Server needs to provide an X.509v3 certificate. The GovShield Client relies on the underlying platform's cryptographic modules to provide X.509v3 certificate services for signature verification for signed policies sent from the GovShield Server, and in support of HTTPS/TLS connections from the GovShield Client to the GovShield Server.

5.1.5 Security Management

Authorized Administrators manage the TOE through the GovShield Server's web GUI which provides the ability to manage users, policies, and the Android Mobile Devices. An Administrator or MD user initiates the installation of the TOE's GovShield Client on the Android Mobile Device; which will communicate with the GovShield Server to enroll in management. Once enrolled, the TOE will prevent user-directed unenrollment from management.
The GovShield Server can be used to transmit specific commands to an Android Mobile Device such as forcibly locking the device or initiating a wipe operation. The GovShield Server can also define policies that specify the configuration settings for an Android Mobile Device. These configuration settings can include functionality such as configuration of the password policy and what settings are applied to Wi-Fi connections. The GovShield Server transmits commands and policies to the GovShield Client for enforcement on the Android Mobile Device. The GovShield Server invokes its underlying platform to sign all policy data and the GovShield Agent invokes its underlying platform to validate the signed policies when they are received.

5.1.6 Protection of the TSF

The communications between the GovShield Server and GovShield Client is protected using HTTPS/TLS which is provided by the underlying platforms of the TOE components.

The GovShield Server relies on its platform to perform the self-test functionality. This includes the platform performing self-tests to verify the integrity and operation of the operational environment components (operating system, hardware and cryptographic module), and the integrity of stored TSF executable code against known SHA-256 checksums.

The Administrator invokes the GovShield Server's underlying platform to update the GovShield Server software, and the platform will verify the GovShield Server's software digital signature as part of the installation process. The Administrator distributes updates to the GovShield Client software through the GovShield Server's MAS Server functionality, and the GovShield Client will invoke the Android Mobile Device to verify the software update's digital signature before installing it. The TOE components' software contains third-party libraries. The TOE components use only documented APIs from their underlying platforms.

5.1.7 TOE Access

The GovShield Server displays a configurable consent warning banner on the web GUI's login page. The GovShield Client displays a configurable consent warning banner on the GovShield Client's login page.

5.1.8 Trusted Path/Channels

The trusted communication channels between the GovShield Server and the GovShield Client, and the GovShield Client and the Oracle Database, make use of HTTPS/TLS and TLS respectively. The trusted communication channels are provided by the TOE components' underlying platforms.

The GovShield Server platform uses HTTPS/TLS to provide a trusted path between itself and remote Administrators through the web GUI and mobile device users during the enrollment of a GovShield Client on an Android Mobile Device.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- GovShield User Guide v1.0 (AGD) for GovShield Version 1.60.05
- GovShield Installation Guide v1.0 (AGD) for GovShield Version 1.60.05

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is GovShield Server Version 1.60.05 and GovShield Client version 1.60.05. Section 4.2 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- Certificate Authority (CA) for distribution of certificates and CRLs
- Management Workstation for local and remote administration
- Audit Server for remote storage of audit records

To use the product in the evaluated configuration, the product must be configured as specified in the *GovShield Installation Guide, Version 1.0 and GovShield User Guide, Version 1.0* documents.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Assurance Activity Report for a Target of Evaluation "GovShield Version 1.60.05" Assurance Activities Report v1.0,* dated April 29, 2026.

8.1 Test Configuration

The evaluation team configured the TOE for testing according to the *GovShield Installation Guide, Version 1.0 and GovShield User Guide, Version 1.0* (AGD) documents. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network.

ESXi 8.0.3 host server

The GovShield Server platform operating environment:

- ESXi 8.0.3
- Microsoft Windows 2022
- OpenJDK 11
- JBoss Enterprise Application Platform 7.4

The GovShield Server was configured to communicate with the following environment components:

- Oracle Database 19 (GovShieldDB) using TLS
- CA Servers (GovShieldRootCA, GovShieldRootIntermediateCA, GovShieldCA)
- Administrator Workstation to access GovShieldWeb administrative interface (HTTPS/TLS)
- Samsung Android Mobile Devices

The GovShield Client platform operating environment:

- Samsung Android Mobile Devices
    - Galaxy Tab Active5
    - Android 15

The GovShield Client was configured to communicate with the following environment components:

- Samsung Knox Licensing Server
- Samsung Knox Enterprise Firmware-over-the-air (E-FOTA) Server
- CA Servers (GovShieldRootCA, GovShieldRootIntermediateCA, GovShieldCA)

Operational Components:

- Function: Switch
    - Model: Cisco Catalyst WS-C Switch, WS-C3560X-24P
    - OS: Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 12.2(55)SE3
    - Protocols: N/A

- Function WAP
    - Model: UniFi PRO Wireless Access Point (WAP)
    - Firmware: 4.0.27.10067

- Function: GovShieldRootCA, GovShieldIntermediateCA, GovShieldCA
  - ESXi server 8.0.3
  - OS: Red Hat Enterprise Linux 8.4 (Ootpa)

- Function Oracle Database Server
  - ESXi 8.0.3
  - Microsoft Windows Server 2022 Standard 10.0.20348 Build 20349
  - Oracle SQL*Plus: Release 19.0.0.0.0 - Production on Sun Feb 22 17:18:22 2026 Version 19.3.0.0.0
- Administrator Workstation
  - ESXi 8.0.3
  - Microsoft Windows 2022
  - OpenJDK 11
  - JBoss Enterprise Application Platform 7.4

The following test tools were installed in the operational environment on multiple test workstations and servers for testing purposes:

- OpenSSL 1.1.1n 15 Mar 2022 (Library: OpenSSL 1.1.1k 25 Mar 2021)
- Wireshark 4.6.4
- Oracle SQL*Plus: Release 19.0.0.0.0 - Production on Sun Feb 22 17:18:22 2026 Version 19.3.0.0.0
- ZenMap 7.90
- tcpdump 4.99.0 and 4.9.3

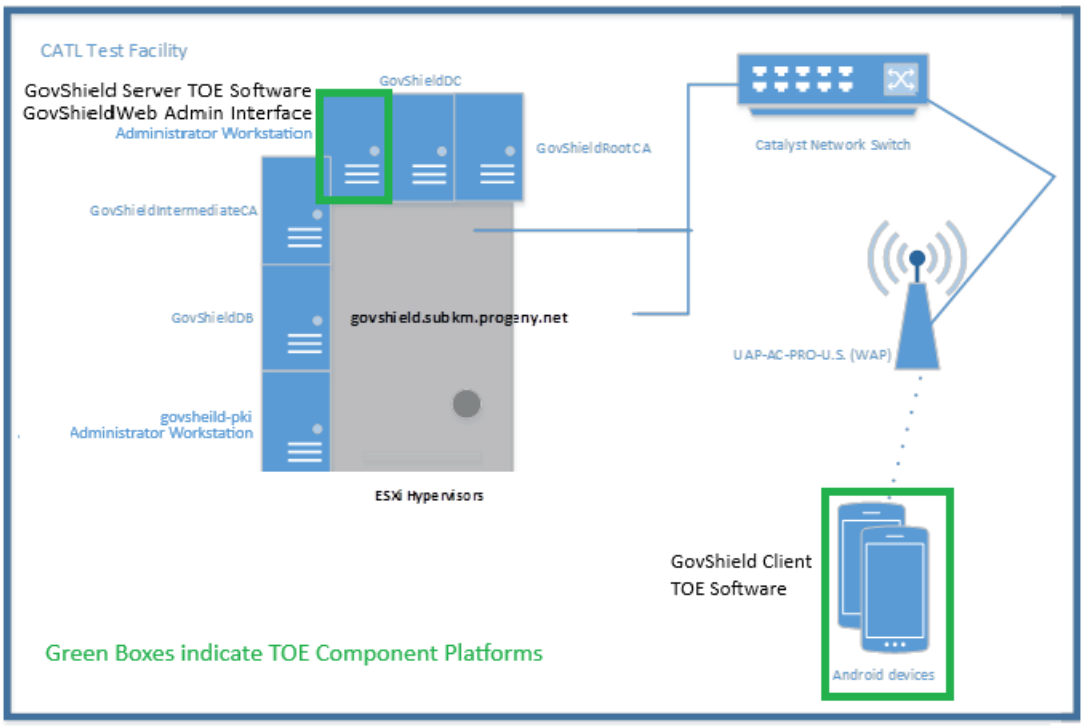

Figure 1 - Test Configuration

8.2 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with NDcPP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords (version information used for refining results) were identified:

Keyword	Description
Progeny	This is a generic term for searching for known vulnerabilities for the specific product (Former name)
GovShield	This is a generic term for searching for known vulnerabilities for the specific product. Use version 1.60.05 only if necessary
General Dynamics Mission Systems	The vendor.
JBoss EAP 7.4	TOE is installed on JBoss enterprise application platform.
Generic Terminology	
Mobile Device Manager	Generic term
Mobile Device Agent	Generic term
Host Agent	Generic term
Third-Party Libraries	
Third-Party Libraries for GovShield Server	List defined in the ST
Third-Party Libraries for GovShield Client app	List defined in the ST

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources on May 27, 2026. The following public vulnerability sources were searched:

- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- National Vulnerability Database: https://nvd.nist.gov/vuln/search#/nvd/home
- CISA KEV databases: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

* Network Exploitation and Network Interception : Any TOE communication over the network could be prone to eavesdropping and interception by a malicious party. The TOE should provide appropriate encryption and authentication mechanisms to secure all data in transit to mitigate eavesdropping, man-in-the-middle attack, and arp-poisoning.

* Bypass MDM / smart-phone Gatekeeper:

  - Malicious MDM/EMM Enrollment : Installing a malicious management profile (via phishing links, SMS, or QR codes). Once the device is enrolled in an attacker-controlled EMM (Enterprise Mobility Management) system, the attacker has administrative control, including the ability to install, update, or remove apps.

  - Silent App Installation : On Android devices, especially those with Samsung Knox or specific managed profiles, an MDM can push apps without user interaction. A malicious MDM can abuse this to silently install spyware or banking Trojans.

  - Bypassing Security Controls : Just as SideStepper bypassed trust prompts in iOS, attackers can use malicious profiles to bypass Android's "Unknown Sources" restriction or "Restricted Settings" (introduced in Android 13).

  - Man in the middle on MDM commands : Attackers can intercept the communication between the Android device and the MDM server, allowing them to hijack commands and force the device to install malicious apps signed with a rogue certificate.

* Malicious Code : There is a possibility of a software product being infected with a virus or malicious code even when coming directly from a vendor.

During the course of the evaluation, the GovShield product had 8 third-party libraries that needed to be updated to mitigate medium through critical vulnerabilities before the completion of testing. The continuation of IND testing showed that the patches did not have an effect on the operations of the TOE. A final public search was performed May 27, 2026, using the keywords and list of libraries and versions defined in the ST, resulted in 0 vulnerability findings.

Based on the results of the above penetration testing, the evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

The evaluation team determined that the TOE was not vulnerable to any of the defined attacks or had unsatisfied publicly known vulnerabilities. There were no vulnerability issues discovered with the final version of the TOE, that could affect the security posture of a deployed system.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the MDMPP and AGENTMOD.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the GovShield product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the MDMPP and AGENTMOD in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the MDMPP and AGENTMOD related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the MDMPP and AGENTMOD related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work units. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the MDMPP and AGENTMOD, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the MDMPP and AGENTMOD were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the MDMPP and AGENTMOD, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the MDMPP and AGENTMOD, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the guides listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *GovShield 1.60.05 Security Target v1.0,* dated February 6, 2026.

13 List of Acronyms

Acronym	Definition
AGD	Administrative Guidance Documents
CA	Certificate Authority
CC	Common Criteria
CPU	Central Processing Unit
CSP	Critical Security Parameter
EAP	Enterprise Application Platform
E-FOTA	Samsung Knox Enterprise Firmware-over-the-air
ESXi	Elastic Sky X Integrated
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure over a bidirectional TLS encrypted tunnel
IP	Internet Protocol
IT	Information Technology
Java SE	Java Standard Edition
MAS	Mobile Application Store
MD	Mobile Device
MDM	Mobile Device Management
NFC	Near-Field Communication
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
USB	Universal Serial Bus
WAP	Wireless Access Point
WLAN	Wireless Local Area Network

14 Terminology

Term	Definition
End User	An individual who possesses a mobile device that is managed by GovShield and who has limited authority to perform management functions using the Self-Service Portal
Role	The level of access given to Administrator accounts. The TOE comes with pre-defined roles but new roles with custom sets of privileges can be created.

System Administrator	The class of TOE Administrators that have complete access to a GovShield environment, including the underlying Windows Server 2022 platform.
Administrator	The claimed Protection Profile defines an Administrator as the person who is responsible for management activities, including setting the policy that is applied by the enterprise on the mobile device. This TOE defines separate user roles.
Authorized Administrator	Synonymous with Administrator.
MD User	User with a mobile device (MD).
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-001
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-002
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-003
4. Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-004
5. Protection Profile for Mobile Device Management, dated April 25, 2019 version 4.0
6. Protection Profile Module for Mobile Device Management Agents, dated April 25, 2019 version 1.0
7. GovShield Version 1.60.05 Security Target, dated February 6, 2026, v1.0
8. GovShield Installation Guide, dated February 6, 2026, v1.0
9. GovShield User Guide, dated February 6, 2026, v1.0
10. GovShield Version 1.60.05 Assurance Activities Report (AAR), dated 05/27/2026, version 1.0
11. GovShield Version 1.60.05 Evaluator Technical Report (ETR), dated 05/27/2026, Version 1.0
12. GovShield Version 1.60.05 Test Plan, dated 02/24/2026, Version 1.0