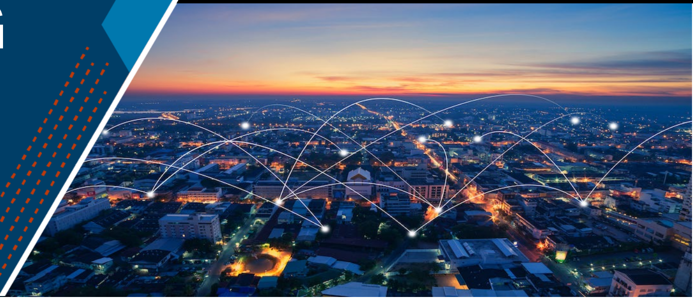
MOBILE APP VETTING FREQUENTLY ASKED QUESTIONS



WHAT IS THE MOBILE APP VETTING SHARED SERVICE?

Mobile App Vetting (MAV) is a software-assurance solution that evaluates the security of government-developed mobile applications (apps) and third-party apps downloaded from Google Play and the Apple App Store. The service conducts static and dynamic scans identifying app vulnerabilities, flaws, and possible risks so Federal Civilian Executive Branch (FCEB) agencies can take the necessary steps to either resolve identified issues or decide against deploying an app to prevent cyberattacks on mobile devices and enterprise systems.

WHAT IS A THIRD-PARTY MOBILE APP?

Third-party apps are developed by organizations or developers who are not the manufacturers of the devices on which the apps run. Most third-party apps are installed by downloading from Google Play Store or Apple App Store.

WHAT IS A GOVERNMENT-DEVELOPED MOBILE APP?

Government-developed apps are created and distributed by a government agency. There are two types of mobile apps developed by government agencies:

- **Enterprise-focused apps:** For internal use to help government employees do their jobs.
- **Public-focused apps:** For use by public citizens in obtaining real-time information, public services, and engagement with government agencies.

HOW DOES MAV WORK?

MAV uses static and dynamic code analysis to scan apps against industry standards:

- National Information Assurance Partnership (NIAP)
- Open Worldwide Application Security Project (OWASP) Mobile Application Security Testing Guide
- National Institute of Standards and Technology (NIST)
- General Data Protection Regulation (GDPR)

These standards are detailed models for mobile app integrity that provide baseline security requirements. Apps submitted to the MAV environment are compared against them. Figure 1 depicts the MAV process.

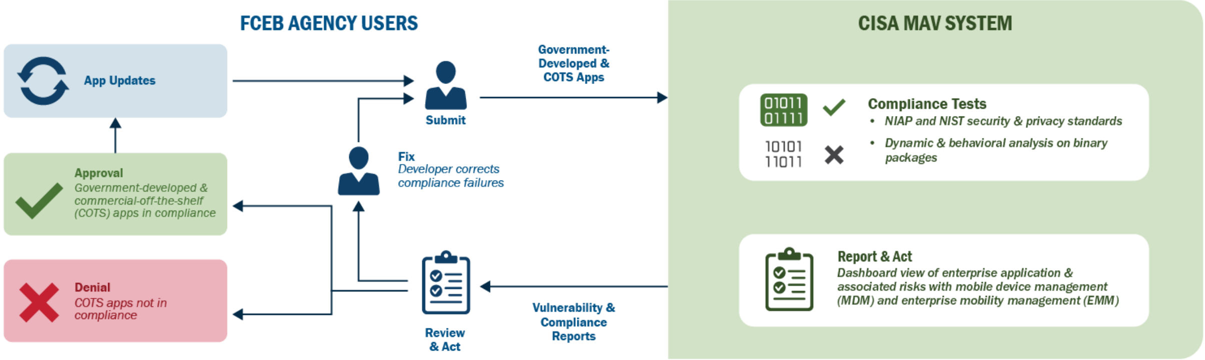

FCEB AGENCY USERS
CISA MAV SYSTEM
App Updates
Submit
Government-Developed & COTS Apps
Approval
Government-developed & commercial-off-the-shelf (COTS) apps in compliance
Fix
Developer corrects compliance failures
Denial
COTS apps not in compliance
Review & Act
Vulnerability & Compliance Reports
01011
01111
10101
11011
Compliance Tests
NIAP and NIST security & privacy standards
Dynamic & behavioral analysis on binary packages
Report & Act
Dashboard view of enterprise application & associated risks with mobile device management (MDM) and enterprise mobility management (EMM)

Figure 1: MAV Process

Once a scan is complete, MAV findings are broken down into critical, high, medium, and low, producing a threat score and detailed reports that users can view and download. These reports include risk findings across standards and remediation recommendations. An agency can then decide to deploy, remediate, or remove any app from circulation based on its established risk tolerance.

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

WHAT IS THE MAV APP LIBRARY?

The MAV App Library is a collection of on-demand scans of third-party apps from the Apple and Android app stores. In this library, users can view the latest versions of the third-party apps analyzed by MAV. The MAV App Library includes apps submitted to the environment by participating agencies as well as popular mobile apps from the Apple and Google stores.

WHAT IF MY APP IS NOT IN THE ANALYZED APP LIBRARY?

If an app is not in the MAV App Library, an agency can utilize the manual app submission process. The MAV support team reviews the submission and approves or rejects for scanning based on information provided by the submitting agency.

HOW LONG DOES A SCAN TAKE?

A typical third-party or government-developed app scan takes two to four hours to complete. The turnaround time will depend on the complexity of the app and how many app scans are already in the queue.

HOW ARE 'ISSUES' DEFINED WHEN FOUND IN A SCANNED APP?

Issues are primarily defined by NIST documents on app vetting, such as NIST Special Publication 800-124 Revision 2. Other references include the NIAP Protection Profile for Application Software 1.4, the OWASP Mobile Application Security Verification Standard, the General Data Protection Regulation, and known vulnerabilities and software weaknesses.

WHAT IS THE THREAT-SCORING MECHANISM?

The calculated threat score—critical, high, medium, and low—is dependent on the level of issues detected from the MAV scan. The threat score calculated for an app's risk level depends on the number of issues identified. The requesting agency can use the threat score as a factor in its decision-making for risk acceptance and app authorization. The threat score is also a good triaging tool for prioritizing which apps to investigate.

DOES THE MAV SERVICE PROVIDE A LIST OF APPROVED APPS?

No, the service does not approve apps. Instead, the service provides robust scans and reports empowering FCEB agencies to make their own risk-based determinations in allowing or disallowing apps for use in their mobile enterprises based on their risk thresholds.

HOW DOES MY AGENCY JOIN THE SERVICE AND IS THERE A COST?

If your agency would like more information about the MAV service, email the MAV service support team at CyberSharedServices@cisa.dhs.gov. A team member will contact you to determine next steps. The MAV service is currently available to FCEB agencies at no cost.

WHAT MAV SUPPORT RESOURCES ARE AVAILABLE TO MY AGENCY?

The MAV team offers several support resources to the FCEB community of existing and prospective MAV users:

- **MAV User Working Group meetings** are quarterly update meetings hosted by the MAV team. These engagements provide attendees with current information about MAV improvements, changes, findings, and opportunities for the user community to provide insights and questions about MAV.
- **MAV Basic Training and Workshop sessions** are hosted by the MAV team on a quarterly basis. These training sessions enable new MAV users to learn more about the service and its uses. Advanced Training sessions are offered to engage existing MAV users with a more focused curriculum.
- **Welcome meetings** are hosted by the MAV team to introduce interested FCEB partners and are tailored to deliver a MAV overview and demonstration.

Current and prospective MAV users can email CyberSharedServices@cisa.dhs.gov to learn more about these resources.