MOBILE APP VETTING FACT SHEET

MOBILE APP VETTING OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow.

CISA's Mobile App Vetting (MAV) service is a mobile application (app) security solution currently offered to federal civilian executive branch (FCEB) agencies. The service evaluates the security of government-developed mobile apps and third-party apps (found through the Google Play Store and Apple App Store) for government-furnished mobile devices. The service identifies app vulnerabilities, flaws and possible risks so that agency users can take the necessary steps to resolve discovered issues and prevent cyberattacks on mobile devices and enterprise systems.

MAV's capability to evaluate mobile apps aides FCEB agencies in making risk-based decisions about which apps to authorize on their networks. Additionally, MAV users benefit from enhanced security standardization and cost-savings that can be redirected to other cybersecurity priorities.

SERVICE BENEFITS

CISA's MAV service provides multiple benefits, including the following:

- **Standardized Security:** Ensures cost-savings and quality service delivery to meet long-term cybersecurity objectives by scanning both government-developed and third-party developed apps with the same strict standards to ensure single-point coverage.
- **App Scanning:** Provides a higher level of confidence that agency information and enterprise systems are protected from mobile cybersecurity threats.
- **Enhanced Security Posture:** Enables FCEB agencies to make risk-based determinations about government developed mobile apps before publishing, and about third-party mobile apps designated for use on government-furnished mobile devices.
- **Increased Visibility:** Grants visibility into the security posture of the federal mobile infrastructure as well as the broader federal enterprise system. This means CISA is empowering each agency's mobile and enterprise security posture early in the app development process, rather than after apps are authorized for use.

TIMELINE TO LAUNCH

The MAV service is expected to receive its Authorization to Operate in 2023 and CISA plans to announce this at the appropriate time so all agencies may take advantage of this valuable shared service.

Until then, a limited number of FCEB agencies are testing the service during an Initial Operational Capacity phase to establish service viability, implement lessons learned and refine the service. During this process, the MAV team will host user trainings to gather feedback, address questions and discuss possible service updates.

FUNDING AND COST

CISA currently provides the MAV services to FCEB agencies at no cost. CISA hopes to expand the availability of this mobile security solution to state, local, tribal and territorial agencies to enhance the security of their critical mission-support functions.

REGISTRATION AND CONTACT

CISA is working to identify FCEB agencies interested in implementing the MAV service. Interested agencies can email MAV@cisa.dhs.gov with their organization's name and a designated point of contact's name, title and email.