Mobile Cybersecurity Shared Services

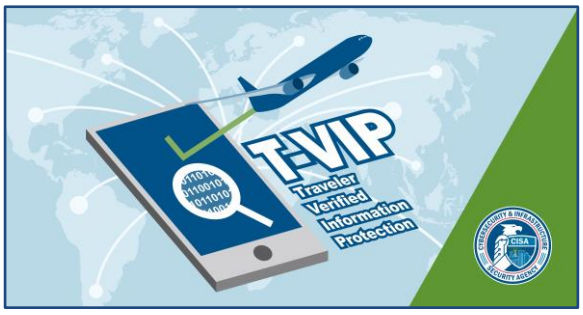
OVERVIEW

The Cybersecurity and Infrastructure Security Agency's (CISA) newly launched Mobile Cybersecurity Shared Services will enhance federal civilian enterprise mobile security by providing a range of mobile-related security services to Federal Civilian Executive Branch (FCEB) agencies. These shared services will increase the security of Government-Furnished Equipment (GFE) mobile devices (e.g. smartphones and tablets) and applications (apps). Mobile Cybersecurity Shared Services will deliver a range of critical cybersecurity services to address Mobile Device Security, Mobile Application Security, and Mobile Network Security. Following are summaries of each service area and the associated benefits.

MOBILE CYBERSECURITY SHARED SERVICES OFFERINGS

Mobile Application Security Service: The most recently launched Mobile Cybersecurity Shared Service is a new Mobile Application Vetting (MAV) service, which evaluates the security of government-developed mobile apps and third-party apps used on GFE mobile devices. The service identifies app vulnerabilities, flaws, and possible risks so steps can be taken to fix discovered issues and, more importantly, prevent critical cyber-attacks on mobile devices and enterprise systems. The MAV service will launch in Fiscal Year 2022 (FY22) with a test pilot consisting of up to three early-adopter FCEB agencies and will then expand to 10 FCEB agencies in FY23.

Mobile Device Security Service: The previously launched Traveler-Verified Information Protection (T-VIP) security service is a device-integrity validation tool that detects software, firmware, and hardware modifications to a smartphone between two points in time. Because government travelers need their GFE mobile devices to stay in contact with their offices while traveling to foreign countries, embassies, or external sites, they can be prime targets for compromise. These travelers cannot monitor what occurs "under the hood" of their mobile devices, so comparisons of pre-travel and post-travel scans by the T-VIP software—developed by Pacific Northwest National Laboratory—will identify suspicious changes on the devices made during their travels, thus increasing the security of sensitive government information. T-VIP is a government-off-the-shelf solution and is for official government use only. It is being piloted for adoption as a full Mobile Cybersecurity Shared Services offering.



Mobile Network Security Service: Currently under development in cooperation with the Department of Homeland Security's Science and Technology Directorate, this Mobile Cybersecurity Shared Service deploys protective Domain Name System (DNS) services to mobile devices. Because government agencies and their employees are increasingly reliant upon mobile devices, a protective DNS solution for mobile traffic will align DNS protections with those provided to traditional enterprise systems. This research-and-development project will design a solution that routes mobile DNS traffic to a protective DNS resolver managed by CISA. This protective DNS capability is part of CISA's Protective DNS service offering.

FUTURE OF MOBILE SHARED SERVICES

Mobile devices have become increasingly more critical to the federal workforce's ability to successfully complete its mission. CISA's Mobile Cybersecurity Shared Services will offer these and future security solutions to safeguard GFE mobile devices and enterprise assets, as well as the sensitive government information stored on and accessed on enterprise networks by mobile devices.

CONTACT THE CYBER QSMO

For any questions or further background on these services, please reach out to the Cybersecurity Quality Services Management Office (Cyber QSMO) team at QSMO@cisa.dhs.gov.

ABOUT THE CYBER QSMO

The Cyber QSMO serves as an online, government storefront for high-quality cybersecurity services, aligning with federal governance, requirements, and priorities. Its mission is to centralize, standardize, automate, and offer high-quality, cost-effective cybersecurity services and products for all federal civilian departments and agencies. As part of the end-to-end service management model, the Cyber QSMO is committed to providing integration and adoption support to customers through a unified shared services platform. The top priorities are to understand our customers' cybersecurity needs, gaps, and risks, and to offer and continually refine service offerings that both meet those demands and align with the ever-changing threat landscape impacting the federal .gov enterprise.