TRAVELER-VERIFIED INFORMATION PROTECTION SERVICE FACT SHEET

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 established the Traveler-Verified Information Protection (T-VIP) service to provide the means to determine and monitor the integrity of government-furnished mobile devices (smart phones and tablet computers), including their configurations, applications, firmware, hardware and software. The T-VIP service supports Apple iPhone and Samsung Galaxy models and can be updated to support new mobile devices as they become available.

HOW T-VIP WORKS

The T-VIP service is a cost-effective solution for securing agency mobile devices from adversaries during certain high-risk encounters such as international travel or visits to foreign embassies. The T-VIP service gives agencies the ability to safely identify and detect mobile-based cybersecurity threats. The service will gauge real world threats by detecting unauthorized or suspicious changes to the mobile device. This solution is a direct response to known vulnerabilities and real customer needs.

HIGHLIGHTS

The T-VIP service enables government agencies to conduct pre-travel and post-travel scans on mobile devices. The results of each scan are compared to determine if a mobile device has been compromised, faces increased security risks or has new vulnerabilities.

- **Pre-Travel Scans:** Users provide their mobile devices to their agency's T-VIP personnel before foreign travel for pre-travel baseline scanning. T-VIP personnel conduct a post-travel scan upon the user's return from their travels.
- **Post-Travel Scans:** The post-travel scan detects risks that resulted from travel. Scanned data is uploaded and stored in the reference database repository. Following analysis, if T-VIP personnel detect increased risk, they may export the collected data for further forensic analysis and decide to remove the mobile device from service.
- **Agency Review:** Agencies can apply their unique policies to determine whether to continue using the device based on risk tolerance or escalate it to the next tier for forensic evaluation.

BENEFITS

CISA's T-VIP service supports integrity checking of mobile government-furnished equipment used by VIPs during international travel, travel to foreign embassies in the U.S. and in high-risk scenarios. The service is a government-off-the-shelf solution and restricted to official use only on a case-by-case request — lessening the likelihood of it becoming available to potential adversaries.

T-VIP provides value to agencies through:

- **Minimal Cost**: CISA utilizes a shared service approach and covers all costs directly associated with the T-VIP service (software and software maintenance), providing optimal cost savings to agency customers.

- **Secure Management and Storage:** All T-VIP software components reside in a secure and trusted government space, which strengthens enterprise security.
- **Validated Mobile Device Integrity:** T-VIP determines the integrity of mobile devices through software digital inspection before and after government travel.
- **Increased Mobile Device Security:** T-VIP baselines the device pre-travel and detects changes such as malicious additions post-travel. These scans increase the capability of agencies to detect compromises of mobile devices that could expose sensitive government and personal information.
- **Rapid Analysis:** Most T-VIP pre-and-post travel scans take one-to-45 minutes for comparison and analysis, providing rapid results.