U.S. DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL

OIG-26-09 June 22, 2026

FINAL REPORT

Secret Service's Deficient Mobile Device Management Increased the Risk to Protectees and Sensitive Information

DHS OIG HIGHLIGHTS

Secret Service's Deficient Mobile Device Management Increased the Risk to Protectees and Sensitive Information

June 22, 2026

Why We Did This Review

During the course of other reviews of the Secret Service after the attempted assassination of then-former President Trump on July 13, 2024, we learned that Secret Service personnel frequently used personal cell phones for official business, raising security concerns. We conducted this review to determine whether the Secret Service effectively manages and secures mobile devices used to conduct official Government business, including its protective mission.

What We Recommend

We made five recommendations to improve the Secret Service's mobile device security and reduce the use of unmanaged personal mobile devices.

OIG Access

The Secret Service delayed the DHS Office of Inspector General's access to its asset management and travel systems for more than 130 days and delayed providing requested documents, which limited our planned work and analysis and negatively impacted the review timeline.

What We Found

The United States Secret Service (Secret Service) did not effectively secure and manage mobile devices, including during protective operations. As a result, adversaries could have intercepted and exploited Secret Service information, placing at risk our Nation's leaders, other protectees, and employees — especially when unsecured devices were used overseas.

- Government-furnished equipment (GFE) mobile devices lacked capabilities needed to carry out mission operations, which led employees to use personal devices for official business, including for protective operations domestically and overseas. Personal devices are less secure and unmanaged by the Government, creating security vulnerabilities in violation of Department of Homeland Security and component policies.
- The GFE mobile devices used abroad lacked required security applications to ensure real-time, continuous protection from cyberattacks by foreign adversaries or individuals. We also found apps with security vulnerabilities on GFE mobile devices.

This heightened risk occurred because the Secret Service's process for identifying and implementing mobile device capabilities did not always fully identify employees' operational needs, leaving employees without essential capabilities such that they resorted to using personal devices. The Secret Service's processes for securing mobile devices for international use were insufficient, and it did not have a policy of testing mobile device app code before installation.

Secret Service Response

The Secret Service concurred with all five recommendations. Appendix C contains the Secret Service's response in its entirety.

Table of Contents

Abbreviations

GFE	Government-furnished equipment
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
Secret Service	United States Secret Service
U.S.C.	United States Code
VPN	virtual private network

Background

The United States Secret Service (Secret Service) is responsible for protecting the President, the Vice President, their immediate family members, former presidents, presidential candidates, visiting foreign heads of state, and national security events and facilities. When our country's most important leaders travel — both domestically and internationally — Secret Service employees provide protection. As of November 2025, the Secret Service had more than 8,000 special agents, officers, and support personnel in more than 150 offices throughout the United States and abroad.

The Secret Service manages approximately 8,000 Government-furnished equipment (GFE) mobile devices, e.g., smartphones and tablets, and issues them to its personnel, other Department of Homeland Security employees during special events, and contractors. These devices facilitate voice, video, text, and email communication; access to Secret Service systems and resources; and mobile hotspot connectivity. The Secret Service also allows its personnel to download and install pre-approved third-party and Secret Service–developed applications (apps) from an official Secret Service portal. For example, one Secret Service–owned app provides employees with emergency relocation sites, procedures, and contacts.

The Secret Service's Office of the Chief Information Officer (OCIO) oversees the security of the component's information technology and ensures the Secret Service complies with information system security requirements. Secret Service OCIO is responsible for, among other things, establishing security standards for mobile devices; providing operation and administrative support for Secret Service-issued mobile devices; maintaining a list of apps and digital media approved for official Government business use; and monitoring the activity on all Secret Service mobile devices to ensure compliance with Secret Service policies.

Although mobile devices increase workforce mobility and productivity, they also can lead to cyberattacks or loss of sensitive data if improperly managed and secured. To reduce those risks, Secret Service OCIO centrally manages mobile devices using a Mobile Device Management system that enforces Secret Service security policies. Secret Service OCIO performs several important functions through the Mobile Device Management system, such as managing how mobile devices connect to Secret Service networks, restricting device capabilities, and implementing and monitoring security settings on the devices. The main goal of centrally managing GFE mobile devices is to ensure that devices are secure.

While conducting other reviews of the Secret Service stemming from the attempted assassination of then-former President Trump on July 13, 2024, we identified and reported to the Department, via electronic letter, "particularly serious or flagrant problems, abuses, or deficiencies relating to the administration of programs and operations" of the Secret Service as

required by the *Inspector General Act of 1978, as amended*.[1] Central to our October 24, 2024 letter to the DHS Secretary were credible whistleblower accounts and corroborating information from the *Report of the Independent Review Panel on the July 13, 2024 Assassination Attempt in Butler, Pennsylvania,*[2] indicating that Secret Service personnel frequently used personal cell phones for official communication, creating serious security risks and potential violations of the *Federal Records Act*.[3]

We initiated this review to determine whether the Secret Service effectively manages and secures mobile devices used to conduct official Government business, including its protective mission.

Results of Review

Key Finding 1: Secret Service Employees Relied on Personal Mobile Devices for Mission Operations

Secret Service employees relied on personal mobile devices for mission operations because GFE mobile devices lacked the capabilities employees needed to perform their mission, including mobile messaging required for operations outside the United States. Without the necessary capabilities, Secret Service employees were driven to use their personal mobile devices to communicate with stakeholders, law enforcement partners, and colleagues in violation of Secret Service policy. Because the Secret Service does not manage or secure employees' personal devices, communicating through these devices increased risks to protectees and employees.

Secret Service employees and their personal devices are attractive targets for both foreign and domestic adversaries. If an adversary gains access to an employee's personal mobile device or intercepts its communications, they could obtain mission-related data, including contacts, user history, geolocation, and photos. Such access could also reveal sensitive personal information, such as home addresses and family members' identities. Adversaries could use this information

[1] 5 United States Code (U.S.C.) § 405(e) provides: "Each Inspector General shall report immediately to the head of the establishment involved whenever the Inspector General becomes aware of particularly serious or flagrant problems, abuses, or deficiencies relating to the administration of programs and operations of the establishment. The head of the establishment shall transmit any such report to the appropriate committees or subcommittees of Congress within 7 calendar days, together with a report by the head of the establishment containing any comments the establishment head deems appropriate." Appendix D contains a copy of our October 24, 2024 letter to the Department while Appendix E contains the Department's October 31, 2024 transmittal letter and comments to the Senate Committee on Homeland Security and Government Affairs.

[2] October 15, 2024; https://www.dhs.gov/sites/default/files/2024-10/24_1017_opa-Independent-Review-Panel-Final-Report-and-Accompanying-Materials.pdf.

[3] 44 U.S.C. §§ 2101–2118, 2901–2911, 3101–3107, 3301–3303a.

to plan attacks against protectees or Secret Service employees. Use of personal devices also posed records retention challenges.

Secret Service Employees Used Personal Mobile Devices Internationally and Domestically

Through interviews and analysis of Secret Service records, we identified cases in which employees used personal devices instead of GFE mobile devices to conduct official business.

- We reviewed travel vouchers for employees who traveled internationally between October 2022 and April 2025 and identified 30 employees who claimed reimbursement for using personal phones for official business.[4] We interviewed 20 of these employees and four supervisors who reviewed the vouchers. Of the 24 individuals interviewed, **23 reported relying on personal devices, with most needing them during nearly every foreign assignment.**
- During interviews, employees who traveled internationally reported using their personal mobile devices as hotspots to provide internet access for GFE laptops. They also described using personal devices to access websites blocked on GFE mobile devices but necessary to support protectee safety. For example, employees needed to research restaurants where a protectee was scheduled to dine.
- Using limited log data,[5] **we identified more than 15,000 instances among 4.8 million calls in which employees sent and received calls from colleagues' personal phones while working protective events.** We also identified approximately 24,000 text messages between colleagues' personal devices and GFE mobile devices among 6.9 million total text messages. Most of the personal device communication occurred within the United States.

[4] This figure does not reflect the total number of employees who used their personal devices for official business; it only includes employees who requested and received reimbursement for charges (i.e., daily international data charges) and explicitly documented in their voucher the use of their personal device during international trips. Employees we interviewed told us that they did not seek reimbursement for personal device use for most of their travel.

[5] We examined call and text logs from Secret Service GFE mobile device records from October 2022 through May 2025, noting that data for some months was not available due to data issues originating from the mobile device service provider. Our analysis captured only personal device communications to or from a GFE mobile device. We did not include personal phone use through messaging apps or any communications made exclusively between personal devices.

- During an interview with DHS OIG,[6] a Secret Service employee described instances in which they used their personal device during a domestic event to share photos with colleagues and local partners.

> Shortly before the July 13, 2024 attempted assassination of then-former President Trump, a Secret Service employee used their personal device to receive a picture message from local law enforcement of the would-be assassin due to reliability concerns with their GFE. The employee described previous issues where they were unable to send text messages with an image using a GFE mobile device.

Policies Prohibit the Use of Personal Mobile Devices for Official Business

DHS policy[7] only allows the use of GFE mobile devices for official business and prohibits the use of personal devices without prior approval. Secret Service policy prohibits employees from carrying personal mobile devices while on duty during a protective or investigative operational assignment.[8] The Secret Service also strongly discourages bringing personal devices on official international travel.[9] However, in practice, **we found the use of personal devices during foreign assignments had become expected and routine among Secret Service employees.**

Employees told us they frequently relied on their personal devices to communicate while abroad, and some provided examples of Secret Service mission planning documents in which colleagues outlined how to communicate effectively overseas using personal devices. One supervisor stated that communicating with foreign stakeholders through personal devices was essential to ensure the safety of the protectee and the public.

Process for Identifying and Implementing New Capabilities Was Not Sufficient

Secret Service employees resorted to using their personal devices because their GFE mobile devices did not have the apps and capabilities needed to perform mission operations across all geographical locations.

---

[6] Interview with Secret Service employee in 2025, as part of DHS Office of Inspector General's (OIG) body of work initiated after the July 13, 2024 attempted assassination of then-former President Trump. This same employee provided similar information to the Committee on Homeland Security and Governmental Affairs.
[7] DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems*, Attachment I *Sensitive Mobile Devices,* Version 1.1, Apr. 3, 2024.
[8] Secret Service Directive CIO-11(26), *Information Technology General Rules of Behavior,* Apr. 2024.
[9] Secret Service Directive CIO-11(20), *Cyber Security Enhancement for OCONUS Operations,* May 2022.

Employees stated that stakeholders and partners outside the United States rely on two commonly used commercial messaging apps — which were not available on their GFE mobile devices — to communicate with:

- foreign police, military, and other foreign stakeholders;
- Department of State personnel;
- other Secret Service employees located overseas; and
- embassy drivers and protectees' staff responsible for transportation and event support.

To a lesser extent, employees identified additional mobile apps they needed during foreign missions that were not available on GFE mobile devices. These included another mobile messaging app and an app required to support employee safety in a high-risk country. Some Secret Service employees reported lacking an essential app to conduct investigations and others to communicate with local law enforcement and protectees domestically.

Device policy restrictions and technical limitations also made GFE mobile devices unusable for certain types of messaging during domestic missions.

- Between March 2023 and May 2025, Secret Service OCIO on multiple occasions changed employees' ability to send text, group, and picture messages on GFE mobile devices. During this period, employees were sometimes unable to share photos (e.g., suspicious individuals) by text or receive certain types of messages, including those originating outside the agency. Employees said they were not always aware of these changes, creating confusion about device capabilities. As of June 2025, employees could receive most types of messages on their GFE mobile devices.
- During an interview with DHS OIG,[10] a Secret Service employee described instances in which they encountered difficulties sharing pictures on their GFE mobile devices.

> After the July 13, 2024 attempted assassination, DHS OIG asked a Secret Service employee to describe how they forwarded a picture of the would-be assassin to multiple colleagues via GFE mobile device. Although the employee received the picture in a text message, they explained how a previously known issue prevented them from simply re-texting the picture, so they took the extra steps to email it instead. The employee described previous issues where they were unable to send text messages with an image using a GFE mobile device.

[10] Interview with Secret Service employee in 2025, as part of DHS OIG's body of work initiated after the July 13, 2024 attempted assassination of then-former President Trump.

- Employees also expressed concerns that GFE mobile devices frequently disconnected from the Secret Service virtual private network (VPN), diminishing the devices' reliability during operations. According to the Secret Service's wireless helpdesk records, roughly 12 percent of all wireless helpdesk tickets concerning GFE mobile devices involved VPN issues.

GFE mobile devices lacked mission-critical capabilities because Secret Service OCIO's process for assessing and approving requests did not always correctly identify operational needs. OCIO is responsible for ensuring its mobile device management capabilities provide both adequate security and operational functionality required for mission needs. OCIO staff explained that devices were heavily restricted by default, and certain messaging apps and functions were blocked due to their inability to incorporate records retention requirements.[11] According to OCIO, when employees identify the need for a new app, they submit requests through the Secret Service OCIO service portal. We reviewed approximately 2.5 years of portal records from October 2022 to March 2025. During this period, employees submitted five requests for the two commercial messaging apps commonly used overseas. This low number of requests[12] did not reflect the frequency with which these apps were already being used.

OCIO management stated that they understood the requested apps would be useful and were aware of only a few employee-generated requests; they did not know that Secret Service employees were already extensively using the apps on personal devices. Consistent with department-wide efforts to improve management of electronic messaging capabilities,[13] OCIO tested a third-party messaging solution[14] that automatically archives communications but did not deploy the app for approximately 1.5 years until March 2025, due to other funding priorities. During this period, OCIO did not provide an interim messaging solution. On May 12, 2025, OCIO made commercial versions of common messaging apps available to employees. We confirmed these apps are now available on GFE mobile devices.

We also noted that in fiscal years 2023 and 2024, 28 percent and 43 percent, respectively, of Secret Service employees had not completed required cybersecurity awareness training, which may have contributed to the routine use of personal devices. Because OCIO's process for

[11] According to 44 U.S.C. § 3101, *Records Management by Agency Heads, General Duties,* agencies must retain records. 36 Code of Federal Regulations § 1222.22 defines the types of records that must be maintained, including "the persons, places, things, or matters dealt with by the agency."
[12] During interviews, employees told us they did not make service requests for specific messaging apps for various reasons, such as assuming they were already blocked, not having time to make requests, or making their requests outside the OCIO service portal.
[13] Memorandum for Component Chief Information Officers, from Eric Hysen, Chief Information Officer, Subject: Enhanced Retention and Preservation of Electronic Messaging (Oct. 4, 2022).
[14] As discussed later in this report, the third-party solution for messaging and automatic message archiving was removed from GFE devices shortly after deployment when vulnerabilities were made public.

identifying and implementing capabilities on GFE mobile devices did not ensure that employees were prepared — and because the use of personal devices was normalized — there is a risk that OCIO may not properly identify and prioritize other operational needs.

Recommendation 1: We recommend the Secret Service Office of the Chief Information Officer develop and implement a formal policy and process for routinely identifying, evaluating, and implementing mobile device capabilities to ensure all mission functions — foreign and domestic — can be conducted effectively and securely.

Recommendation 2: We recommend the Secret Service Office of the Chief Information Officer ensure employees complete cybersecurity awareness training, as required, and training features clear guidance on the proper use of mobile devices in operational settings domestically and overseas.

Use of Personal Mobile Devices Placed People and Data at Risk

When employees use their personal devices for mission operations, it places at risk the Secret Service's communications, personnel, and protectees. The Secret Service does not secure or manage employees' personal devices and therefore cannot ensure their security. If a personal device is jailbroken,[15] infected with malicious code, or not up to date on security software, an adversary could intercept device communication. Outdated and vulnerable apps[16] could enable malicious actors to conduct surveillance, track locations, or record employees' communications. Connecting to unsecured networks may also allow cybercriminals to access data or install malware. Some employees reported downloading third-party VPN software on their personal devices to reduce these risks. Because personal devices are unmanaged, the Secret Service cannot verify the legitimacy of the third-party VPN software, creating another potential avenue for adversaries to access sensitive information.

The Secret Service is required to preserve records that document the persons, places, things, or matters dealt with by the agency; facilitate actions by agency officials; and make possible proper

[15] Jailbreaking modifies the mobile device and disables some of the built-in security features that keep the operating system safe and protect stored data from exposure or corruption.

[16] We previously reported on risky apps installed on GFE mobile devices at DHS. (See *Management Alert – ICE Management and Oversight of Mobile Applications (REDACTED),* OIG-24-02, Oct. 30, 2023; *ICE Did Not Always Manage and Secure Mobile Devices to Prevent Unauthorized Access to Sensitive Information,* OIG-24-61, Sept. 26, 2024; *CBP's Deficient Mobile Device Management Places Information at Risk (REDACTED)*, OIG-25-42, Sept. 22, 2025; and *Deficiencies in I&A Mobile Device Security Create Vulnerabilities, Place Information at Increased Risk,* OIG-26-06, Apr. 30, 2026.) Similar app risks could also apply to personal devices used for official business at the Secret Service.

scrutiny by Congress.[17] Use of personal phones also creates record retention challenges for the Secret Service, as the agency does not monitor and archive communications on employees' personal devices.[18] Therefore, the Secret Service cannot assure that these communications will be available for future investigative or historical purposes.

Recommendation 3: We recommend the Secret Service Office of the Chief Information Officer enact an outreach strategy to communicate to employees that the use of personal devices is not allowed for official business. In addition, develop and implement guidance outlining steps employees must take to safeguard communications if they need to rely on a personal device (such as during an emergency) and to ensure such usage is reported and information is properly retained as an official record.

Key Finding 2: The Secret Service Did Not Effectively Secure and Manage GFE Mobile Devices Used Internationally

Although Secret Service mostly applied secure settings and configurations on GFE mobile devices, Secret Service OCIO did not adequately secure or manage GFE mobile devices used in the higher threat environment outside the United States. These devices lacked the DHS-required security software for international travel, and they were not consistently wiped of data after employees returned.

Threats Are Greater When Mobile Devices Are Used Outside the United States

Foreign governments can control mobile network infrastructure to monitor all communications to and from devices or use mobile carriers to secretly push malware directly onto them. These risks increase when devices lack Mobile Threat Defense software, potentially allowing adversaries to bypass standard security settings. Additionally, if compromised devices are not wiped after international travel, adversaries could continue to exploit undetected vulnerabilities.

For example, a recent Department of Justice OIG report[19] described how a Federal Bureau of Investigation agent's mobile device information was obtained abroad. Foreign adversaries

[17] 44 U.S.C. § 3101; 36 C.F.R § 1222.22; DHS Instruction 141-01-001, *Records and Information Management*, Sept. 9, 2019; U.S. Secret Service Manual GRS-06(01) *Management of Email and Other Electronic Message Records*, Jan. 24, 2024.

[18] DHS regulations and Secret Service policy make clear that record retention laws apply based on the content of electronic messages, regardless of whether they are text or email, or conveyed via Government or personal devices. DHS Instruction 141-01-001, DHS Policy Directive 141-03, *Electronic Records Management Updates for Chat, Text, and Instant Messaging*, Feb. 23, 2018; Secret Service Manual GRS-06(01).

[19] Department of Justice OIG Report 25-065, *Audit of the Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance*, June 2025 (Redacted).

reportedly used a hacker to exploit device information to identify, intimidate, and, in some cases, kill potential sources or cooperating Federal Bureau of Investigation witnesses. Until the Secret Service improves security controls for mobile devices used overseas, employees' sensitive device information and communication with protectees face similar risks. These risks are even greater when employees rely on personal devices, which also lack Mobile Threat Defense and are not routinely wiped after travel.

GFE Mobile Devices Used Outside the United States Lacked Mobile Threat Defense

Without adequate controls, such as Mobile Threat Defense and routine device data wiping, Secret Service GFE mobile devices faced increased cybersecurity risk when used outside the United States. Despite threats to mobile devices used abroad, Secret Service OCIO did not begin installing Mobile Threat Defense software on any GFE mobile device until August 2025. The software is designed to provide real-time, continuous protection from malicious software, cyberattacks, and other vulnerabilities, even when devices are not connected to a Government network.

In interviews, OCIO staff confirmed that they did not install this software on GFE mobile devices, yet DHS policy[20] requires Mobile Threat Defense software on any device used outside the United States, regardless of the location's threat level. This deficiency occurred because OCIO did not have a policy to ensure compliance with DHS' requirement to use Mobile Threat Defense software during international travel. OCIO staff responsible for managing mobile devices stated they believed the limitations on the available apps, the connection to the Secret Service VPN, and existing device configurations provided sufficient protection. However, these controls are intended to be used in conjunction with Mobile Threat Defense software. The Secret Service had installed Mobile Threat Defense on most GFE mobile devices as of December 2025.

GFE Mobile Devices Were Not Routinely Wiped after International Travel

Secret Service OCIO did not consistently wipe data from GFE mobile devices after employees returned from international missions despite Secret Service policy requiring employees to manually wipe their GFE mobile devices within 24 hours of returning to the United States.[21] Wiping ensures the secure deletion of all content on a device, including threats that may have been introduced during foreign travel. If employees do not complete this step, OCIO policy requires that the device be wiped remotely.

[20] DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems,* Attachment Q *International Travel with Mobile Devices,* Version 1.1, Mar. 21, 2024.
[21] Secret Service Directive CIO-11(20) required device wiping (Secret Service has since rescinded this requirement) and requires employees to identify and preserve records as outlined in GRS-06(01).

Of the 24 employees we interviewed, 20 reported that mobile device wiping either did not occur or was performed inconsistently. One employee stated that their phone had never been wiped over 8 years and 20 international trips, including travel to high-risk countries. Another employee reported 15 trips over 8 years and estimated that their phone had been wiped only four times.

These deficiencies occurred because OCIO's process for monitoring devices used internationally was focused on high-risk countries and therefore did not account for all travel. Further, OCIO management explained that devices were not wiped because of prior and ongoing Department of Justice and DHS OIG oversight reviews dating back to January 2021. During this timeframe, OCIO did not develop an alternative process to ensure phones used on international travel were secure.

Recommendation 4: We recommend the Secret Service Office of the Chief Information Officer develop and implement controls to ensure that all mobile devices returning from international missions are wiped and develop and implement contingency plans for situations when devices cannot be wiped.

Key Finding 3: The Secret Service Did Not Properly Assess and Ensure the Security of Apps before They Were Used for Official Business

Secret Service OCIO did not properly assess and ensure the security of apps or prevent the deployment of vulnerable apps to GFE mobile devices. **OCIO deployed to GFE mobile devices a third-party messaging solution, along with custom-made mobile apps, containing vulnerabilities.** As noted earlier, in March 2025 OCIO deployed a third-party messaging solution with automatic message archiving that provided the same capabilities as other well-known commercial messaging apps on over 600 GFE mobile devices. According to OCIO, a DHS assessment determined that a limited number of Secret Service messages were compromised when the messaging solution improperly stored them on unsecured third-party servers. The Secret Service's internal assessment[22] of the compromised messages found they contained employees' Personally Identifiable Information but no operationally sensitive data. OCIO decommissioned the third-party messaging solution in May 2025 after vulnerabilities were publicly disclosed. In place of the third-party messaging solution, OCIO allowed the use of commercial messaging apps and required Secret Service personnel to manually retain records by saving logs and taking screen shots.

Separately, OCIO deployed four custom-made mobile apps to Secret Service GFE mobile devices. During our testing, all but one app had enough compensating controls and functionality restrictions to minimize risks from vulnerabilities we identified. The one app with remaining

[22] We did not review the accuracy of Secret Service's assessment of compromised messages.

risks was installed on fewer than 10 devices managed by the Secret Service Mobile Device Management system. Although the vulnerabilities we identified were not critical, they increased the risk that malicious actors could access information to facilitate more sophisticated attacks. Secret Service OCIO staff maintained the risk was limited because these devices did not have access to Secret Service systems or data.

Vulnerabilities existed on GFE mobile devices because OCIO's testing policy[23] did not include the National Institute of Standards and Technology's (NIST) recommended process for testing mobile app source code. NIST recommends[24] using an app assessment process to ensure software is free from vulnerabilities. This process should include testing the app's source code or performing binary code analysis when source code is not available. For custom-made apps, agencies should[25] perform static application security testing of the app's source code. Additionally, the Secret Service requires testing of computer software and open-source software for vulnerabilities.

OCIO staff explained that their testing of the third-party messaging solution was limited to records retention compliance, privacy policies, and network communication reviews, which did not detect vulnerabilities in the code. Notably, the third-party messaging solution was already being used across DHS and may have provided a false sense of security. Plus, OCIO did not perform static application security testing on custom-made apps until we began our review.

Recommendation 5: We recommend the Secret Service Office of the Chief Information Officer update its vulnerability testing policy to incorporate the National Institute of Standards and Technology's process for testing mobile app code.

[23] Secret Service Directive CIO-11(34), *Secure Software Development and Acquisition,* Sept. 21, 2023.
[24] NIST Special Publication 800-163 Revision 1, *Vetting the Security of Mobile Applications*, Apr. 2019.
[25] NIST Special Publication 800-218, *Secure Software Development Framework V1.1,* Feb. 2022.

Appendix A:
Objective, Scope, and Methodology

We conducted this review to determine whether the Secret Service effectively manages and secures mobile devices used to conduct official Government business, including its protective mission.

Our audit publication was significantly delayed by three Government shutdowns in fiscal year 2026. Even though some of our staff continued working during portions of the shutdowns, delays covered 48 percent of the fiscal year through May 1, 2026.

We reviewed DHS information technology system security program policies and applicable attachments, such as those related to mobile device use policy, vulnerability management policy, incident response, and international travel for mobile devices. In addition, we reviewed Secret Service information technology policy on the management of mobile services and devices, enhanced cybersecurity for operations outside the continental United States, incident reporting, software development and acquisition, configuration management, and vulnerability mitigation. We interviewed Secret Service OCIO staff responsible for mobile device management, security, and mobile services. These interviews were conducted over video conference calls, and we used screen sharing to observe the capabilities of the Secret Service's Mobile Device Management system. We also obtained read-only access to the Mobile Device Management system for the purpose of generating reports.

We reviewed prior and ongoing audits, investigations, inspections, and testimony of Secret Service employees to identify mentions of personal device use and systemic issues with GFE mobile device usability. Throughout the review, we monitored OIG hotline complaints that could indicate issues with Secret Service mobile devices. We analyzed all employee training records between October 2022 and April 2025 to identify cybersecurity course completion dates. We excluded the results from fiscal year 2025 because the data did not cover the entire fiscal year.

To identify potential personal mobile device use, we reviewed the Secret Service's help desk requests, travel reimbursement records, employee profiles, and phone records. Using read-only access to the Secret Service's voucher reimbursement system, we obtained travel records identifying employee expenses between October 2022 and April 2025. We then filtered these records to focus on 782 employees who traveled internationally and used miscellaneous travel expenditure codes during that period. Using keyword searches, we identified vouchers that indicated employees had used their personal devices during international travel and requested and received reimbursement for the expenses. We found 30 employees with clear signs of personal device use expenses in their vouchers; for example, some of these employees directly stated in their vouchers that they used a personal mobile device to complete their assigned

mission. Other employees' reimbursement requests may have included personal device expenses, but we focused only on clear and explicit personal device use.

We interviewed 20 of the employees who had clear signs of personal device use in their vouchers as well as 4 supervisors who approved the vouchers. These individuals described the common practice of using personal mobile devices and explained how most employees who use personal devices do not seek reimbursement. We conducted these interviews to identify potential issues with GFE mobile devices, as well as to gain an understanding of the circumstances, frequency, and reasons why employees used personal mobile devices. We also used these interviews to determine if employee devices were being wiped after foreign travel and confirmed details with Secret Service OCIO staff. We conducted the interviews both in person and over video conference calls.

We also requested internal planning documents from Secret Service employees coordinating foreign site visits and reviewed them for evidence of personal device use, such as listing employee personal numbers and providing written guidance for using personal devices while abroad.

We reviewed Secret Service GFE mobile device records from October 2022 through May 2025 to determine if employees used personal devices to communicate with other employees while assigned to protective events. These records included the phone numbers employees communicated with (using voice or standard text message) as well as the time and place of the communications. We noted approximately 10 months of missing data and worked with the Secret Service to obtain additional records, but those records were not available due to data issues originating from the mobile device service provider. We identified employees' personal phone numbers by reviewing Secret Service personnel system records. We also obtained all office phone numbers within the Secret Service and compared them to the listing of personal phone numbers to remove false positives. To determine if personal devices were used, we compared GFE mobile device communications to the listing of employees' personal phone numbers. If we found a match, we determined if the employees were working protective events by comparing the date from GFE mobile device communications to dates employees worked events as recorded in Secret Service's Events Management system. According to a Secret Service official, when employees work protective events, the assignment may include periods of personal/downtime, such as what employees might encounter during lengthy trips.

Our call and text analysis was limited to communication that involved a GFE mobile device; we did not review employees' personal device records. Therefore, our analysis does not include any calls or texts between employees using only personal devices. Our results also did not include calls and texts between a Secret Service employee's assigned GFE mobile device number and their own personal number because employees are allowed limited personal communication with their families, and the communication would not have been with other Secret Service

employees. Additionally, we could not analyze communication that occurred via messaging apps.

As part of our assessment, we reviewed the configuration settings of four profiles used on Secret Service mobile devices. We manually checked these configuration settings against applicable Defense Information System Agency Security Technical Implementation Guides. We also performed static application security testing on four Secret Service custom-developed mobile apps. Our code analysis followed DHS Sensitive Systems Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems*, Version 13.4, which requires components to employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within DHS. We analyzed scan results only for high, medium, and low severity vulnerabilities and did not include issues related to code quality or coding practices in our analysis. We conducted both tests between February and March 2025.

We conducted this review under the authority of the *Inspector General Act of 1978, as amended*, 5 U.S.C. §§ 401–424, and according to the *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency.

DHS OIG's Access to DHS Information

During this review, the Secret Service delayed our requests for read-only access to the TOPS Sunflower Enterprise Property Management System database and the Concur Government Edition Reporting Tool. These delays, both of which lasted for more than 130 calendar days, significantly impacted our ability to meet project milestones and prevented us from independently validating the Secret Service's property information and performing targeted interviews related to mobile device use. Additionally, the Secret Service delayed our request for documentation related to site post log assignments and the Special Operations Division Joint Tactical Survey. These delays limited the extent of our planned analysis and negatively impacted the review timeline.

Appendix B:
Recommendations, Management Comments, and OIG Analysis

The Secret Service provided management comments on a draft of this report. We included the comments in their entirety in Appendix C. We also received technical comments from the Secret Service on the draft report; we revised the report as appropriate. The Secret Service concurred with all five recommendations. We consider recommendation 4 closed and resolved. We consider recommendations 2 and 5 open and resolved. We consider recommendations 1 and 3 open and unresolved. A summary of the Secret Service's response and our analysis follows.

In its comments, the Secret Service disputed that it delayed our request for read-only access to its databases and other documentation. However, lasting more than 130 calendar days, these delays significantly impacted our ability to meet project milestones and prevented us from independently validating the Secret Service's property information and performing targeted interviews related to mobile device use, limited the extent of our planned analysis, and negatively impacted the review timeline.

Recommendation 1: We recommend the Secret Service Office of the Chief Information Officer develop and implement a formal policy and process for routinely identifying, evaluating, and implementing mobile device capabilities to ensure all mission functions — foreign and domestic — can be conducted effectively and securely.

Secret Service Response to Recommendation 1: Concur. On May 12, 2025, Secret Service OCIO updated CIO-05(02), *Management of Mobile Services and* Devices, with the "Directives Control Point" CIO 2025-113. This control point, which is a tool to rapidly incorporate directives into Secret Service policy and guidance, made commercial versions of commonly used messaging apps available for Secret Service users to support foreign and domestic requirements. Additionally, Secret Service OCIO identifies and evaluates emerging capabilities on an ongoing basis, including those for mobile devices, through the formal intake process. The Secret Service requested that we consider this recommendation closed and resolved, as implemented.

OIG Analysis: During our review, the Secret Service addressed the immediate need for the specific messaging apps. However, Secret Service has not demonstrated how the formal intake process ensures mobile device capabilities meet mission needs. Therefore, additional and future needs may not be identified without improvements to the existing evaluation process.

This recommendation will remain open and unresolved until we receive evidence of policy changes to strengthen how mobile device needs are identified.

Recommendation 2: We recommend the Secret Service Office of the Chief Information Officer ensure employees complete cybersecurity awareness training, as required, and training features

clear guidance on the proper use of mobile devices in operational settings domestically and overseas.

Secret Service Response to Recommendation 2: Concur. On January 15, 2026, Secret Service OCIO modified CIO-11(04), *Information Security Training and Awareness,* to require personnel to complete required cybersecurity awareness training within 30 days after entry on duty, or by September 30 of each fiscal year, as appropriate. In addition, OCIO monitors and enforces training completion. The Secret Service requested that we consider this recommendation closed and resolved, as implemented.

OIG Analysis: The corrective actions are responsive to the recommendation. This recommendation will remain open and resolved until we receive evidence of enforcement actions on training completion requirement.

Recommendation 3: We recommend the Secret Service Office of the Chief Information Officer enact an outreach strategy to communicate to employees that the use of personal devices is not allowed for official business. In addition, develop and implement guidance outlining steps employees must take to safeguard communications if they need to rely on a personal device (such as during an emergency) and to ensure such usage is reported and information is properly retained as an official record.

Secret Service Response to Recommendation 3: Concur. Secret Service policy CIO-11(26) prohibits the use of personally owned equipment, including cell phones. Further, ITG-03(05), *Miscellaneous Standards (U.S. Secret Services),* prohibits the use of personal mobile devices while on duty. Additional guidance is regularly provided before trips, including any available guidance regarding foreign travel information security, which frequently also prohibits personally owned devices. The Secret Service requested that we consider this recommendation closed and resolved, as implemented.

OIG Analysis: We acknowledge that the Secret Service had existing policies relevant to this recommendation. The Secret Service made enhancements to policies prohibiting use of personal devices, and policy for Federal records retention when automatic archiving is not possible, including when personal devices are used for official business due to an emergency. However, we reported personal device use was normalized, and we obtained examples of Secret Service mission planning documents outlining personal devices were needed while overseas. Given the normalization, we recommend the Secret Service implement a robust outreach strategy emphasizing the risks of using personal devices for official business and provide clear guidance on the Secret Service's policy.

This recommendation will remain open and unresolved until we receive evidence of an outreach strategy to communicate that personal device use is not allowed for official business.

Recommendation 4: We recommend the Secret Service Office of the Chief Information Officer develop and implement controls to ensure that all mobile devices returning from international missions are wiped and develop and implement contingency plans for situations when devices cannot be wiped.

Secret Service Response to Recommendation 4: Concur. As part of the Secret Service's ongoing commitment to data security, and to comply with ongoing data preservation requirements, Secret Service OCIO rescinded the requirement to wipe mobile devices after travel outside of the continental United States in January 2026. In alignment with DHS Policy Directive 4300A, Attachment Q, Secret Service OCIO also implemented the requirement that all Secret Service–issued devices shall have Mobile Threat Defense software installed prior to and for the duration of all travel and office assignments outside of the continental United States. The Secret Service Security Operations Center proactively monitors for signs of compromised devices. This policy change rescinding the prior requirement is documented in CIO-11(20). The Secret Service requested that we consider this recommendation closed and resolved, as implemented.

OIG Analysis: During our review, we received documentation of the Secret Service's corrective actions. The change in policy and the implementation of Mobile Threat Defense as a mitigating control met the intent of our recommendation. This recommendation is closed and resolved.

Recommendation 5: We recommend the Secret Service Office of the Chief Information Officer update its vulnerability testing policy to incorporate the National Institute of Standards and Technology's process for testing mobile app code.

Secret Service Response to Recommendation 5: Concur. In 2025, Secret Service OCIO initiated a process to comply with the NIST process for testing mobile app code and is currently developing an update to its vulnerability testing policy addressing these processes. Estimated Completion Date: October 31, 2026.

OIG Analysis: The corrective actions are responsive to the recommendation. During our review, the Secret Service partially addressed this recommendation by implementing source code analysis of custom mobile apps. However, the process should include testing of both custom app and third-party app source code or binary code if source code is not available.

This recommendation will remain open and resolved until we receive evidence OCIO updated its vulnerability testing policy for vetting the security of mobile apps per NIST Special Publication 800-163.

Appendix C:
Secret Service Comments on the Draft Report

The Secret Service's formal management response begins on the next page.

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE
Washington, D.C. 20223

BY ELECTRONIC SUBMISSION

May 13, 2026

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Sean M. Curran
Director
United States Secret Service

SUBJECT: Management Response to Draft Report: "Secret Service's Deficient Mobile Device Management Increased the Risk to Protectees and Sensitive Information"
(Project No. 25-008-AUD-USSS)

Thank you for the opportunity to comment on this draft report. The U.S. Secret Service (Secret Service) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

Secret Service leadership is pleased to note OIG's recognition of the importance of Secret Service identifying and implementing measures to protect the President and other protectees as part of the agency's mission. We take seriously the OIG's work in this report, and consequently made several comprehensive enhancements to Secret Service communications policies and protocols to both mitigate the potential for adversaries to intercept and exploit Secret Service information, as well as further strengthen the protective environment. For example, the Secret Service Office of the Chief Information Officer modified CIO-11(04)[1] to require personnel complete cybersecurity training within 30 days after entry on duty and by September 30 each fiscal year. The Secret Service remains committed to ensuring a safe protective environment for all protectees by strengthening protocols, processes, and policies regarding mobile device capabilities.

However, the Secret Service disagrees with the OIG's allegation that the Secret Service delayed OIG requests for read-only access to the "TOPS Sunflower Enterprise Property Management System" database and the "Concur Government Edition Reporting Tool," as well as the allegation that Secret Service delayed documentation related to site post log assignments and the Special Operations Division Joint Tactical Survey.

[1] CIO-11(04), "Information Security Training and Awareness," dated January 15, 2026.

OIG requests for data, including requests for direct access to agency IT databases, should be evaluated on a case-by-case basis. DHS fully supports providing the OIG timely access to information "which relate[s] to the programs and operations with respect to which [the] Inspector General [IG] has responsibilities . . .." 5 U.S.C. § 406(a)(1)(A). The law, however, does not state *how* the Department should provide access to the information or require the Department to provide OIG the data in the manner OIG requests. Accordingly, DHS is not required to provide the information to the OIG via direct access to agency systems, especially where the agency, as the steward of the data, assesses that the system may include a significant amount of data that is beyond the scope of the OIG's stated objectives, including sensitive, classified, and otherwise confidential information. In order to ensure the appropriate handling and safeguarding of the information, DHS may seek information on the relevance of a data request to the scope and objectives of OIG's work, especially in light of the types of sensitive data held by DHS. In addition, the law does not prohibit DHS from providing the requested information via alternative means to satisfy auditors' need for "appropriate, sufficient evidence to provide a reasonable basis for addressing the audit objectives and supporting their findings and conclusions." GAO-24-106786, *Government Auditing Standards*, § 8.90.

The draft report contained five recommendations with which the Secret Service concurs. Attached find our detailed response to each recommendation. The Secret Service previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: Management Response to Recommendations Contained in OIG 25-008-AUD-USSS

OIG recommended the Secret Service Office of the Chief Information Officer:

Recommendation 1: Develop and implement a formal policy and process for routinely identifying, evaluating, and implementing mobile device capabilities to ensure all mission functions – foreign and domestic – can be conducted effectively and securely.

Response: Concur. On May 12, 2025, the Secret Service Office of the Chief Information Officer updated CIO-05(02)[2] with the "Directives Control Point" CIO 2025-11[3]. This control point, which is a tool to rapidly incorporate directives into Secret Service policy and guidance, made commercial versions of Signal and WhatsApp available for Secret Service users to support foreign and domestic requirements. In addition, the Secret Service Office of the Chief Information Officer routinely identifies and evaluates emerging capabilities on an ongoing basis, including those for mobile devices, through the formal intake process.

On May 11, 2026, Secret Service personnel provided the OIG with documentation of efforts to address this recommendation. We request that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 2: Ensure employees complete cybersecurity awareness training, as required, and training features clear guidance on the proper use of mobile devices in operational settings domestically and overseas.

Response: Concur. On January 15, 2026, the Secret Service Office of the Chief Information Officer modified CIO-11(04),[4] to require personnel to complete required cybersecurity awareness training within 30 days after entry on duty, or by September 30 of each fiscal year, as appropriate. In addition, training completion is monitored and enforced by the Office of the Chief Information Officer.

On May 11, 2026, Secret Service personnel provided the OIG with documentation of efforts to address this recommendation. We request that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 3: Enact an outreach strategy to communicate to employees that the use of personal devices is not allowed for official business. In addition, develop and

---

[2] CIO-05(02), "Management of Cellular Services and Devices," dated May 12, 2025.
[3] Directives Control Point CIO 2025-11, "Smartphone Messaging and Record Retention Requirements," dated May 12, 2025.
[4] CIO-11(04), "Information Security Training and Awareness," dated January 15, 2026.

implement guidance outlining steps employees must take to safeguard communications if they need to rely on a personal device (such as during an emergency) and to ensure such usage is reported and information is properly retained as an official record.

Response: Concur. Secret Service policy CIO-11(26)[5] prohibits the use of personally owned equipment, including cell phones. Furthermore, ITG-03(05)[6] prohibits the use of personal mobile devices while on duty. Additional guidance is regularly provided before trips, including any available guidance regarding foreign travel information security, which frequently also prohibits personally owned devices.

On May 11, 2026, Secret Service personnel provided the OIG with documentation of efforts to address this recommendation. We request that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 4: Develop and implement controls to ensure that all mobile devices returning from international missions are wiped and develop and implement contingency plans for situations when devices cannot be wiped.

Response: Concur. As an alternative approach to address the intent of this recommendation as part of the Secret Service's ongoing commitment to data security, and to comply with ongoing data preservation requirements, the Secret Service Office of the Chief Information Officer rescinded the requirement to wipe mobile devices after travel outside of the continental United States in January 2026. In alignment with DHS Policy Directive 4300A, Attachment Q,[7] the Secret Service Office of the Chief Information Officer also implemented the requirement that all Secret Service-issued devices shall have mobile threat defense software installed prior to—and for the duration of—all travel and office assignments outside of the continental United States. The Secret Service Security Operations Center proactively monitors for signs of compromised devices. This policy change is documented in CIO-11(20),[8] which incorporates Directives Control Point CIO 2026-02,[9] and removes the prior requirement to wipe devices returning from international missions.

On May 11, 2026, Secret Service personnel provided the OIG with documentation of efforts to address this recommendation. We request that the OIG consider this recommendation resolved and closed, as implemented.

---

[5] CIO-11(26), "Information Technology General Rules of Behavior," dated January 21, 2026.
[6] ITG-03(05), "Miscellaneous Standards (U.S. Secret Service)," dated January 31, 2025.
[7] DHS Policy Directive 4300A, "International Travel with Mobile Devices," Attachment Q, "International Travel with Mobile Devices," dated April 25, 2022; See: https://share.google/rgp8DS8ul8ffeYxhM.
[8] CIO-11(20), "Cyber Security Enhancements for Outside of the Continental United States (OCONUS) Operations," dated January 6, 2026.
[9] Directives Control Point CIO 2026-02, "Rescinding of Requirement to Wipe Mobile Devices," dated January 6, 2026"

Recommendation 5: Update vulnerability testing policy to incorporate the National Institute of Standards and Technology's process for testing mobile app code.

Response: Concur. In 2025, the Secret Service Office of the Chief Information Officer initiated processes to comply with the National Institute Standards of Technology process for testing mobile app code, and is currently developing an update to vulnerability testing policy addressing these processes. Estimated Completion Date: October 31, 2026.

Appendix D:
7-Day Letter

Our October 24, 2024 letter to the Department begins on the next page.

OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

October 24, 2024

BY ELECTRONIC TRANSMISSION

The Honorable Alejandro Mayorkas
Secretary
Department of Homeland Security
Washington, D.C.

Re: OIG Project Nos. 24-038-ISP-USSS, *Secret Service's Process for Securing Former President Trump's July 13, 2024 Event;* 24-039-AUD-USSS, *U.S. Secret Service Counter Sniper Preparedness and Operations;* and 24-040-AUD-USSS, *U.S. Secret Service Planning and Implementation Activities for Protective Operations*

Dear Secretary Mayorkas:

In accordance with 5 U.S.C. § 405(e), I am writing to report "particularly serious or flagrant problems, abuses, or deficiencies relating to the administration of programs and operations" of the U.S. Secret Service. As detailed below, the Department of Homeland Security (DHS) Office of Inspector General (OIG) has received credible and detailed information indicating that Secret Service personnel routinely conduct official communications on their personally-owned cell phones while working on protective missions.[1]

Background

According to public statements of the Federal Bureau of Investigation, at a July 13, 2024 rally in Butler, Pennsylvania, an individual named Matthew Crooks ascended to the roof of a building adjacent to the rally site and fired a high-powered rifle in the direction of the stage, striking and wounding former President Donald J. Trump, killing an attendee, and wounding several other attendees.[2] Within days, DHS OIG opened the three projects referenced above.

[1] The information available to DHS OIG indicates that despite multiple Secret Service personnel raising concerns to Secret Service management at the highest levels about the use of personal phones for official business, Secret Service management has created the conditions that have left Secret Service personnel no choice but to use personal phones to accomplish their mission, has permitted this practice to persist, and has not taken action to remediate it.

[2] *See* https://www.fbi.gov/news/speeches/investigative-updates-on-the-butler-pennsylvania-assassination-attempt (last visited October 22, 2024).

One area of DHS OIG's focus in these projects is examining any challenges encountered by the Secret Service in communicating among their own personnel and with law enforcement partners, both in general and during the July 13 rally.

The problem

A whistleblower credibly alleges that in 2021, the Secret Service imposed functional limitations on government phones issued to Secret Service personnel that eliminated the ability of a user to: (i) Initiate or participate in a group text limited to users of Secret Service phones; and (ii) send or receive a photo attached to a text message. The whistleblower further alleges that in most instances the only way to communicate with foreign law enforcement partners when working on protective missions overseas is to use a messaging application such as Signal or WhatsApp, which cannot be installed on a Secret Service phone.[3] The whistleblower alleges that as a result of these functional limitations and prohibitions, Secret Service personnel on protective missions routinely resort to using their personal cell phones to communicate with other Secret Service personnel, as well as with law enforcement partners, during protective missions. In addition, the whistleblower alleges that Secret Service personnel sometimes incur charges on their monthly personal cell phone bills amounting to several hundred dollars or more resulting from using their personal cell phones overseas, and that such charges are not always reimbursed by the Secret Service.

According to the *Report of the Independent Review Panel on the July 13, 2024 Assassination Attempt in Butler, Pennsylvania* (10/15/24),[4] in the critical moments leading up to the assassination attempt, Secret Service personnel on duty at the July 13 rally exchanged information among themselves and with state and local law enforcement partners -- including a photo of an individual acting suspiciously, who turned out to be Crooks –- via telephone call,[5]

[3] A user of a Secret Service-issued phone lacks the capability to download an application from a public site. Instead, according to the whistleblower, the only applications that can be installed on a Secret Service phone are found in a "library" of approved applications made available by the Secret Service, and the library does not include WhatsApp and Signal.

[4] The independent review panel report is available at https://www.dhs.gov/publication/independent-review-panel-report (last visited October 23, 2024).

[5] *Report of the Independent Review Panel* at 9 ("the agent from the Trump detail with CUAS responsibilities passed that information [concerning Crooks] on by phone to the Countersniper Response agent"); *Report*, Appendix A at vii ("5:50 PM: "Hercules 1 receives a call from Protective Intelligence Agent inquiring if he has seen [the individual acting suspiciously] and informing him of their attempt to locate [him]"); *id.* at vii – viii ("5:52 PM: DTD CUAS Agent calls Secret Service Countersniper Response Agent . . . describing . . . a suspicious person with a range finder and asking the Countersniper Response Agent to locate him"); *id.* at ix ("5:57 PM: Countersniper Response Agent calls Local CS Team Lead to obtain additional details"); *id.* at x ("6:10 PM: DTD CUAS Agent in the Security Room calls Countersniper Response Agent to tell him the suspicious person with the range finder is now on the roof of the AGR building").

text message,[6] and e-mail.[7] Particularly noteworthy is the fact that Secret Service personnel sent and received a text message to which a photo was attached, something the whistleblower says they could not have accomplished using Secret Service-issued phones.

A Special Agent who was on duty at the July 13 rally corroborated the whistleblower's allegations. This Special Agent stated in a transcribed interview, given as part of a Senate investigation, that when he learned that a local law enforcement officer had obtained a photo of an individual acting suspiciously, "I asked him to send it to my personal phone because our phones have issues with sending out picture[s]." The Special Agent explained that photos cannot be sent or received via text on a Secret Service phone because of "inherent issues with security systems that are built into the phones," and he agreed with a Senate staff member who characterized the issue as a "general capability problem . . . rather than a problem with cell service at that particular site, on that particular day."[8]

Additionally, a Secret Service Officer Technician who was on duty at the July 13 rally stated in a transcribed interview, given as part of the Senate investigation, that if in the course of a protective mission he cannot reach another agent on his or her Secret Service phone, he calls them on their personal phone, and that in fact he did exactly that at the July 13 rally.[9]

The Secret Service Officer Technician also corroborated the whistleblower's allegation that Secret Service personnel communicate using the Signal messaging application when they

---

[6] *Report of the Independent Review Panel*, Appendix A at ix ("6:04 PM: Protective Intelligence Agent receives text from Countersniper Response Agent conveying . . . [a] photo [of] a suspicious person with a range finder"); *id.* at ix ("6:07 PM: Protective Intelligence Agent sends two texts to Secret Service Protective Intelligence Advance Agent informing him about [the individual] and providing a photo; the Protective Intelligence Advance Agent receives the texts and takes note of their contents").

[7] *Report of the Independent Review Panel*, Appendix A at vii-viii ("5:52 PM: . . . Hercules 1 sends e-mail to the other three Hercules team members nearby him, conveying the text description and photos regarding [the suspicious person]").

[8] Interview of [REDACTED], Special Agent, Secret Service, Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations (8/20/24), at 102 – 103, 123. The interview transcript is available at https://www.hsgac.senate.gov/library (last visited October 22, 2024).

[9] Interview of [REDACTED], Officer Technician, Secret Service, Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations (8/28/24), at 156 – 157. The interview transcript is available at https://www.hsgac.senate.gov/library (last visited October 22, 2024). The Acting Director of the Secret Service told the House Task Force on the Attempted Assassination of Donald J. Trump that the Secret Service's "internal review . . . found an over-reliance on cell phones" at the July 13 rally. *See Interim Staff Report: Investigating the Stunning Security Failures on July 13, 2024 in Butler, Pennsylvania* (October 21, 2024), at 23, available at https://taskforce.house.gov/sites/evo-subsites/july13taskforce.house.gov/files/evo-media-document/task-force-interim-staff-report-10.21.2024.pdf (last visited October 24, 2024).

are overseas.[10] If, as stated above, Signal cannot be used on a Secret Service-issued phone, it may be inferred that the Officer Technician was describing the use of personal phones to communicate when overseas. Furthermore, and regardless of whether the Secret Service allows applications such as Signal on Secret Service phones, on July 22, 2024, Kimberly Cheatle, who at the time was the Director the Secret Service, admitted in sworn testimony before the House Committee on Oversight and Accountability that Secret Service personnel use "personal device[s]" to communicate with "partners" when "work[ing] internationally."[11] It is well-known that other agencies, including DHS components, provide special phones to employees traveling overseas on official government business. It is unclear why the Secret Service does not follow this practice.

The consequences

The apparently routine practice of Secret Service personnel using their personal cell phones for official communications while serving on protective missions, both domestically and overseas, creates a host of concerns, including but not limited to the following:

- The Secret Service cannot ensure that personally-owned phones have been updated with the most recent version of the relevant operating system, which often has security patches aimed at countering the latest malware, thereby leaving sensitive non-public information vulnerable to hacking;[12]

- The Secret Service cannot ensure that applications which create security vulnerabilities, such as applications controlled by foreign adversaries, are excluded from personally-owned phones, thereby leaving sensitive non-public information vulnerable to hacking;

[10] Interview of [REDACTED], Officer Technician, Secret Service, Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations (8/28/24), at 217 - 218. The interview transcript is available at https://www.hsgac.senate.gov/library (last visited October 22, 2024).

[11] The Government Publishing Office has yet to release the official transcript of then- Director Cheatle's testimony. A video of the hearing is available at https://oversight.house.gov/hearing/oversight-of-the-u-s-secret-service-and-the-attempted-assassination-of-president-donald-j-trump (last visited October 23, 2024). The testimony quoted above is at 4:29:45 – 4:30:15.

[12] Many types of sensitive non-public information are likely to reside on agents' personal phones, such as records of protectees' movements, evidence in active law enforcement matters, and names and contact information of Secret Service agents and personnel in other law enforcement agencies. In addition, depending on the settings and permissions chosen by a Secret Service agent on his or her personal phone, real-time location data of an agent on a protective mission may be visible to the agent's friends and family and may be collected and stored on other applications.

- Family members and friends of Secret Service personnel may have access to sensitive non-public information on the personal phones of Secret Service agents;

- Depending on the settings chosen by the individual user on his or her personal phone, official Secret Service records that include sensitive non-public information could end up being stored in personal accounts on servers that are owned and controlled by private entities (e.g., cell phone carrier, internet service provider, device manufacturer);

- The Secret Service cannot passively collect data that the Secret Service is required by law to retain, such as federal records, evidence sought by a party in litigation, evidence relevant to a criminal investigation, and information sought by DHS OIG. Instead, the Secret Service shifts the burden to each individual user to identify data that is subject to a retention requirement, and then to somehow transfer that data to the Secret Service information network and properly catalog it so that it can be retrieved consistent with the law;

- Congress might be deprived of information it needs, and to which it is entitled, to conduct oversight, because the information is not in the custody and control of the Secret Service but instead resides on agents' personal phones;[13]

- Under 36 C.F.R. § 1230.14, an agency must "promptly" report the "unlawful or accidental . . . alteration or destruction" of federal records to the National Archives and Records Administration, an obligation that the Secret Service is unlikely to meet with respect to records of Secret Service business on the personally-owned phones of Secret Service employees;

---

[13] This concern is not hypothetical. For example, the Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations, which conducted an investigation into the events at the July 13 rally, did not receive all of the materials it requested from the Secret Service with respect to at least three witnesses who appeared before subcommittee staff for transcribed interviews. *See* Interview of [REDACTED], Special Agent, Secret Service, Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations (8/29/24), at 64-65 (the Special Agent indicated in his interview that he was asked to provide "call logs and texts" from his "work phone," but not his "personal phone," for the Secret Service to produce to the Senate); Interview of [REDACTED], Special Agent in Charge, Secret Service, Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations (8/30/24), at 166 – 167 (a Special Agent in Charge stated that he was told to make information available for production to the Senate from his "work devices" but not his "personal devices"); Interview of [REDACTED], Officer Technician, Secret Service, Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations (8/28/24), at 218-219 (an Officer Technician stated that he did not provide the Secret Service with records of group chats among Secret Service personnel on Signal while the security measures for the rally were being planned, leading committee staff to pause the interview and ask that the witness provide the records directly to the Senate). The interview transcripts are available at https://www.hsgac.senate.gov/library (last visited October 22, 2024).

- The Secret Service's alleged practice of not always reimbursing agents who incur significant charges on their monthly cell phone bills stemming from use of their personal phones on overseas protective missions raises potential equity and fairness issues; and

- Literally leaving agents to their own devices while on overseas protective missions, with the associated expenses borne by the agents personally, raises the question of whether the Secret Service is accepting unauthorized gifts and/or violating the prohibition against an agency augmenting its appropriation.

Under 5 U.S.C. § 405(e), the Department must "transmit [this] report to the appropriate committees or subcommittees of Congress within 7 calendar days, together with a report by the head of the [Department] containing any comments the [Department] deems appropriate." Should you have any questions, you may call me, or a member of your staff may call Chief Counsel James Read at 202-981-6000.

Sincerely,

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2024.10.24 09:22:14 -07'00'

Joseph V. Cuffari, Ph.D.
Inspector General

cc: Acting General Counsel, DHS
Director, Departmental GAO-OIG Liaison Office
Chief Information Officer, DHS
Acting Director, Secret Service

Appendix E:
7-Day Letter Response

The Department's October 31, 2024 transmittal letter and comments to the Senate Committee on Homeland Security and Government Affairs begins on the next page.

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 31, 2024

BY ELECTRONIC TRANSMISSION

The Honorable Gary Peters, Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Peters:

On October 24, 2024, the U.S. Department of Homeland Security (DHS or "the Department") Office of the Inspector General (OIG) issued a letter under 5 U.S.C. § 405(e) regarding communications practices at the U.S. Secret Service (Secret Service or "the Agency"). Secretary Mayorkas has asked me to transmit the OIG letter and the following comments on his behalf.

DHS and the Secret Service acknowledge concerns raised by the Inspector General involving challenges encountered by the Secret Service in communicating among its own personnel and with law enforcement partners. Investigations into the July 13, 2024, assassination attempt—including the Mission Assurance Review (MAR) conducted by the Secret Service, the Independent Review Panel (IRP) directed by the President and empaneled by DHS, and interim reports by the U.S. Senate Committee on Homeland Security & Governmental Affairs and the House Task Force—have identified significant communications failures. DHS and the Secret Service have and continue to cooperate fully with those investigations, as well as with an audit by the Government Accountability Office and various investigations initiated by the Office of the Inspector General.

The conclusions and recommendations in these reports are informing critical changes that the Secret Service has begun and will continue to make. The Agency has also conducted its own comprehensive review of internal policies and systems to address communications reliability, interoperability, and coverage challenges observed at the Butler rally.

Similarly, following the events of January 6, 2021, the Secret Service participated in a Department-wide working group commissioned by the Secretary, to develop and implement recommendations that ensure retention and preservation of Agency text messages and related communications.

We will thoroughly review and, where appropriate, address the concerns raised by the OIG letter. For clarity, we offer the following information.

The Secret Service has pursued multiple strategies to equip its employees with a suite of effective and secure electronic messaging solutions, to include instant messaging solutions, to perform their mission. This includes instant messaging technologies that allow users to send group messages and transmit photos to multiple recipients.

To help avoid the need for non-agency device use, the Agency has provided specialized phones to certain operational personnel for use overseas—particularly when those personnel are engaged in undercover investigations. In exceptional or exigent situations when employees must rely on a non-Agency devices or messaging accounts, employees must incorporate those communications into a Secret Service IT system within 20 business days—a requirement that aligns with National Records and Archives Administration's records retention standards.

DHS and the Secret Service are committed to addressing the failures that led to the events of July 13, 2024, and making fundamental changes to how the Secret Service executes its protective operations moving forward.

Sincerely,

Kara Lynum
Acting General Counsel
U.S. Department of Homeland Security

Enclosure

CC: The Honorable Rand Paul
Ranking Member, Committee on Homeland Security and Governmental Affairs

Appendix F:
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, please visit our website: www.oig.dhs.gov.

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline.

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

U.S. Mail:
Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive SW
Washington, DC 20528-0305