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 [redacted] 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 [redacted]

[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 [redacted] 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, [redacted] 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 [redacted] 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 [redacted] 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 [redacted]

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