



United States Government Accountability Office

Report to the Chairman,  
Committee on the Judiciary,  
U.S. Senate

**AUTHORIZED FOR PUBLIC RELEASE BY CHAIRMAN GRASSLEY**

July 2025

# SECRET SERVICE

## Gaps in Policy and Threat Information Sharing Hindered Efforts to Secure 2024 Trump Campaign Rally

FOR OFFICIAL USE ONLY – Releasable Only to Congress and Cognizant Federal Agencies  
LAW ENFORCEMENT SENSITIVE – Further dissemination or disclosure is unauthorized without consent of the source  
Distribution of this Report is Temporarily Restricted Pending Removal of 30-Day Hold.

# GAO Highlights

Highlights of GAO-25-108568SU, a report to the Chairman of the Committee on the Judiciary, U.S. Senate

## Why GAO Did This Study

The Secret Service operates under a “zero-fail” protection mission and is responsible for protecting the President, the Vice President, former Presidents, and others. However, on July 13, 2024, a gunman evaded Secret Service and law enforcement personnel. The gunman fired shots at then-former President Trump, injuring him and two rally participants, and killing a rally participant in the process.

This report addresses the extent to which gaps in Secret Service policy and practices contributed to security failures on July 13, 2024.

GAO conducted site visits to the July 13, 2024, Trump campaign rally site, Secret Service Headquarters, and multiple field offices. GAO reviewed Secret Service policies and investigative reports, extensive body camera footage, radio logs, and emails. GAO also obtained information from the Secret Service, including the protective detail for then-former President Trump, and federal, state, and local law enforcement.

## What GAO Recommends

GAO is making eight recommendations, including that the Secret Service develop a resource to provide agents with readily available information so they know what tasks to complete during protectee events, change policy to require threat information be proactively shared internally to inform security planning, and implement a process that incorporates risk-based decision-making for resource allocation. The Department of Homeland Security concurred with our recommendations.

View GAO-25-108568SU. For more information, contact Triana McNeil at [mcneilt@gao.gov](mailto:mcneilt@gao.gov).

July 2025

## SECRET SERVICE

### Gaps in Policy and Threat Information Sharing Hindered Efforts to Secure 2024 Trump Campaign Rally

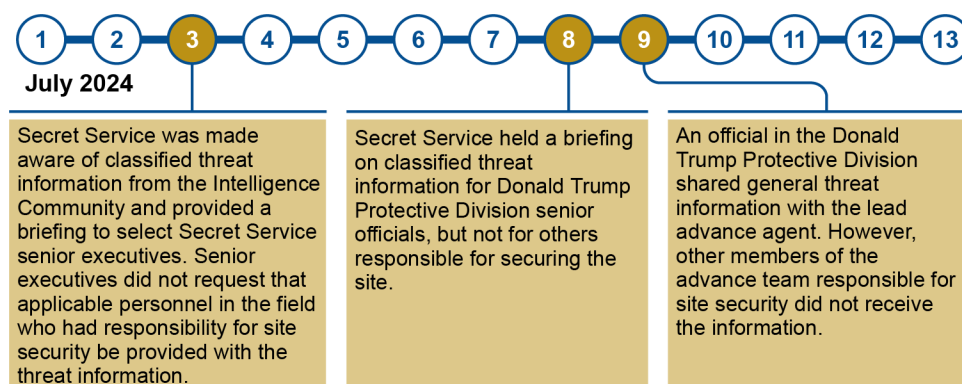
## What GAO Found

The U.S. Secret Service failed to implement security measures that could have prevented the assassination attempt on then-former President Donald J. Trump during a July 13, 2024, campaign rally. At the time, then-former President Trump was not yet the official Republican nominee for President. This presented a unique challenge when Secret Service agents sought to determine what assets to deploy for the rally. The failure was also caused in part by a lack of specific and complete guidance outlining roles and responsibilities for agents assigned to secure the rally. For example, Secret Service guidance did not include details outlining a list of key steps the site agent should take to properly staff the security room, even though the Secret Service provides a checklist for personnel performing other specialized roles. Since the rally, the Secret Service has taken steps to revise its policies, but many of the policies still lack needed details.

Prior to the July 13 rally, senior-level Secret Service officials became aware of a threat to then-former President Trump. This information was not specific to the July 13 rally or gunman. Nonetheless, due to the Secret Service’s siloed practice for sharing classified threat information, Secret Service and local law enforcement personnel central to developing site security plans for the rally were unaware of the threat. According to Secret Service officials, this information was not more broadly shared across the Secret Service because in part, the information was highly classified, and the Intelligence Community did not include information at a lower classification level to share. However, the Secret Service’s siloed information sharing practices, such as requesting that only personnel within an individual’s chain of command be briefed on threat information, contributed to members of the advance team not receiving relevant information. Making changes to Secret Service policies to require it to proactively share threat information internally could help ensure its agents and partners will have information needed to provide effective protection.

Further, sharing threat and risk information could also help ensure resource decisions are based on identified risks. Secret Service’s resource allocation process is not currently set up to comprehensively consider all known risks. Implementing a process that does so can help ensure security asset decisions are based on need and not ad hoc actions outside of a formal process.

#### Timeline of When Secret Service Personnel Obtained but Did Not Share Threat Information with Personnel Responsible for Site Security



Source: GAO review of Secret Service and Intelligence Community information. | GAO-25-108568SU

# Contents

Letter		1
	Background	4
	Policy Gaps, Noncompliance, and Insufficient Threat Sharing Contributed to Security Failures on July 13, 2024	19
	Conclusions	50
	Recommendations for Executive Action	52
	Agency Comments and Our Evaluation	53
Appendix I	Objective, Scope, and Methodology	56
Appendix II	National Special Security Events and Special Event Assessment Rating Events	63
Appendix III	Recommendations Made to the Secret Service in 2024 and 2025 by Other Congressional Investigative Committees	64
Appendix IV	Timeline of Key Events Related to the July 13, 2024 Rally	81
Appendix V	Comments from the Department of Homeland Security	85
Appendix VI	GAO Contact and Staff Acknowledgments	93
Tables		
	Table 1: Secret Service General Roles and Responsibilities for July 13, 2024, Site Security	9
	Table 2: Timeline of Key Actions Taken Related to the July 13, 2024, Campaign Rally	12
	Table 3: Recommendations Included in Senate Homeland Security and Governmental Affairs Report	64
	Table 4: Recommendations Included in DHS Report of the Independent Review Panel	65

---

Table 5: Recommendations Included in Final House Task Force Report	76
--	----

---

Figures

Figure 1: Locations of Secret Service Field Offices in the United States	6
Figure 2: Secret Service Advance Team Members for the July 13, 2024, Rally	11
Figure 3: Secret Service and Other Key Federal, State, Local, and Private Entities That Had Responsibilities for Planning and Securing the July 13, 2024, Rally	13
Figure 4: Timeline of When Secret Service Personnel Obtained and Shared Threat Information Leading Up to the July 13, 2024, Rally	26
Figure 5: Secret Service Process for Fulfilling Asset Requests for Protected Events Through the War Room as of July 13, 2024	35

---

**Abbreviations**

AI	artificial intelligence
CAT	counter assault team
cUAS	counter-unmanned aircraft systems
DHS	Department of Homeland Security
HSGAC	Committee on Homeland Security and Governmental Affairs
HSI	Homeland Security Investigations
FBI	Federal Bureau of Investigation
LES	law enforcement sensitive
NSSE	National Special Security Event
OPO	Office of Protective Operations
SEAR	Special Event Assessment Rating
UAS	unmanned aircraft systems

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.





U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.  
Washington, DC 20548

July 11, 2025

The Honorable Charles E. Grassley  
Chairman  
Committee on the Judiciary  
United States Senate

Dear Mr. Chairman

On July 13, 2024, a gunman opened fire in an attempt to assassinate then-former President Trump during a campaign rally in Butler, Pennsylvania. Then-former President Trump was injured, one attendee was killed, and two other attendees were critically injured.<sup>1</sup> The U.S. Secret Service, a component of the Department of Homeland Security (DHS), is responsible for providing lifetime protection for former Presidents.<sup>2</sup> In addition to protecting former Presidents, the Secret Service also protects the President, the Vice President, and other protectees,<sup>3</sup> but the level of protection provided for each protectee and scenario varies. For example, the Secret Service automatically provides a sitting President with additional protective assets.<sup>4</sup>

The Secret Service relies on its federal, state, and local law enforcement partnerships to carry out its mission and in preparation for the July 13 rally, coordinated with several partners to secure the site. Entities such as U.S. Immigration and Custom Enforcement's Homeland Security Investigations assisted with providing support at posts in and around the site and the Department of Defense assisted with conducting bomb sweeps at the site. The Secret Service also requested assistance from

---

<sup>1</sup>The gunman placed himself on top of the roof of the AGR International, Inc. building located outside of the Secret Service security perimeter for the July 13 rally. The gunman was able to conceal his location from the view of two Beaver County local snipers located inside the AGR building and Secret Service Counter Sniper teams facing the AGR building.

<sup>2</sup>18 U.S.C. § 3056(a)(3). This protection may be declined under 18 U.S.C. § 3056(a).

<sup>3</sup>18 U.S.C. § 3056(a).

<sup>4</sup>Presidential Protection Assistance Act of 1976, Pub. L. No. 94-524, §§ 6, 8, 90 Stat. 2475, 2476 (1976) (as amended) (18 U.S.C. § 3056 note). Assistance provided by executive departments and agencies to assist the Secret Service is otherwise provided on a reimbursable basis.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

---

the Pennsylvania State Police to serve as a liaison for coordinating with state and local law enforcement.

You asked us to review the assassination attempt of then-former President Donald J. Trump during a rally in Butler, Pennsylvania on July 13, 2024. This report examines the extent to which gaps and noncompliance with Secret Service policy may have contributed to security failures at the rally on July 13, 2024.

To determine the extent to which gaps and noncompliance with Secret Service policy contributed to security failures on July 13, 2024, we conducted site visits to the July 13, 2024, Trump campaign rally site in Butler, PA, Secret Service Headquarters, and multiple field offices, such as the Pittsburgh Field Office and the West Palm Beach Field Office. To further inform our assessment of whether established policies were followed given assigned roles and responsibilities, we reviewed available documentation and sought information from third-party sources that observed and contributed to securing the rally, such as other federal entities and state and local officials that supported the rally. Documentation we reviewed included the security plans developed by both Secret Service officials and state and local law enforcement. We further reviewed communication records, including over 1,000 emails, over 4,000 text messages, body camera footage, and over 60 radio logs. We also reviewed documents such as site diagrams and surveys that provide insight into the actions taken by the Secret Service and local law enforcement officials leading up to, and during the rally.

We also analyzed Secret Service policies for securing protected events, including protected events occurring during a presidential campaign, and compared these policies to actions taken on and leading up to July 13, 2024.<sup>5</sup> Our analysis is based on policies Secret Service personnel, including those at Secret Service Headquarters, the Pittsburgh Field Office, the Donald Trump Protective Division, and others that supported the event identified for securing protected events. Specifically, Secret Service personnel identified formal policies, informal documents, and

---

<sup>5</sup>For the purpose of this report, a “protected event” refers to an event where the Secret Service is responsible for providing protection for a protectee, such as a former President, but excludes National Special Security Events (NSSE). We excluded NSSEs from our review of Secret Service policies for securing protected events. See appendix II for more information on NSSEs. Policies we reviewed included, for example, Secret Service, *OPO-03: Protective Advance* (Washington, D.C.: Mar. 11, 2024); *OPO-04: Protective Advance Guidelines* (Washington, D.C.: June 20, 2023); and *OPO-06: Site Security* (Washington, D.C.: May 10, 2022).

---

templates agents utilize when preparing for protected events. Secret Service officials with responsibilities over the identified protective duties confirmed that our list of policies for securing protected events leading up to and on July 13, 2024, was complete and accurate.<sup>6</sup>

In addition, we met with officials and personnel across the Secret Service to gain a factual understanding of what occurred leading up to and on July 13, 2024. This provided us with insights into firsthand accounts of what various personnel experienced in planning for and executing security measures for the rally. It also provided us with an understanding of subsequent retrospective views and assessments of what transpired.

In addition, we interviewed officials from third-party entities at the federal, state, and local levels of government that supported the event, and we visited the site of the July 13, 2024, assassination attempt to better understand the challenges in securing the site. Further detail on the steps we took are described in Appendix I.

We conducted this performance audit from August 2024 to July 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This product has been designated **LAW ENFORCEMENT SENSITIVE / FOR OFFICIAL USE ONLY** because of the sensitive nature of the information it contains. Because the unauthorized disclosure of the sensitive information contained in this product could reasonably be expected to cause a foreseeable harm to the U.S. government or other interest protected by law, recipients may not discuss or release this product to anyone whose official duties do not require access to the information it contains. This product should be safeguarded when not being used and destroyed when no longer needed.

---

<sup>6</sup>We also compared policies for protecting then-former President Donald Trump to other former president protective division policies to determine, how if at all, Donald Trump Protective Division policies differed. We reviewed policies from the following former president protective divisions: Carter Protective Division, George Bush Protective Division, Obama Protective Division, and the Bill Clinton Protective Division.

---

## Background

The Secret Service carries out an integrated mission of protection and investigations. Its protective mission is to provide protection for such persons as the President, Vice President, their immediate families, and visiting foreign dignitaries,<sup>7</sup> as well as facilities such as the White House complex.<sup>8</sup> Its investigative mission is to investigate a wide range of crimes that threaten U.S. financial systems, such as financial and computer-based fraud.<sup>9</sup>

According to Secret Service policy, the agency is authorized to protect other individuals, as directed by the President, through a Presidential Memorandum.<sup>10</sup> For example, senior Secret Service officials noted, at the time of the July 13, 2024, rally, the agency was responsible for the security of 40 full-time protectees and two part-time protectees. The Secret Service reported that in 2024, it secured approximately 5,928 domestic visits and 214 foreign visits—including more than 660 events related to the 2024 presidential campaign.

---

## Secret Service Secures Various Types of Events

**President and Vice President protectee events.** The Presidential Protective Division is responsible for protecting the sitting President of the United States, members of the First Family, and other individuals at the direction of the President. In addition to Secret Service personnel, the President receives support from the White House Military Office, which provides military support to the President of the United States and the First Family to ensure they consistently have secure and reliable communications capabilities. The Vice Presidential Protective Division is responsible for protecting the Vice President of the United States and members of the Second Family.

**Former President protectee events.** A former President may elect to receive lifetime Secret Service protection.<sup>11</sup> Based on our analysis, each former President's protection division (excluding the Donald Trump Protective Division) receives similar levels of base-level protection

---

<sup>7</sup>18 U.S.C. § 3056(a).

<sup>8</sup>18 U.S.C. § 3056A(a).

<sup>9</sup>18 U.S.C. § 3056(b).

<sup>10</sup>Secret Service, OPO-02: Protective Operations – General (Washington, D.C.: Mar. 27, 2024).

<sup>11</sup>Pursuant to 18 U.S.C. § 3056(a)(3), under the direction of the Secretary of Homeland Security, the Secret Service is authorized to protect former Presidents and their spouses for their lifetimes. This protection may be declined.

---

staffing. However, staffing levels may be adjusted up or down at the discretion of the protection division Special Agent in Charge based on the size and scope of a visit.

For example, the Obama, Clinton, and Bush Protective Divisions receive the same base-level Secret Service advance team staffing for domestic trips when they are traveling alone. Prior to July 13, 2024, while then-former President Trump was not a presidential candidate, according to the Secret Service, he received additional assets that a former President's protective division would not typically receive due to his elevated profile and specific threats and intelligence he consistently received during his campaign.

**Candidate and nominee protectee events.** The Secret Service Candidate Nominee Operations Section provides protection for major candidates and nominees for the office of the President and Vice President, as directed by the Secretary of Homeland Security, after consultation with the Congressional Advisory Committee or by Presidential Memorandum.<sup>12</sup> The Candidate Nominee Operations Section also oversees and provides operational support to both the Democratic and Republican National Conventions and all four general election debates.

The Secret Service provides a standard advance team for major candidates and nominees. However, for more complex visits, the Candidate Nominee Operations Section and Office of Protective Operations (OPO) approve additional specialty assets on a case-by-case basis, including support from the Technical Security Division, Special Operations Division, and Office of Strategic Intelligence and Information, among others.<sup>13</sup>

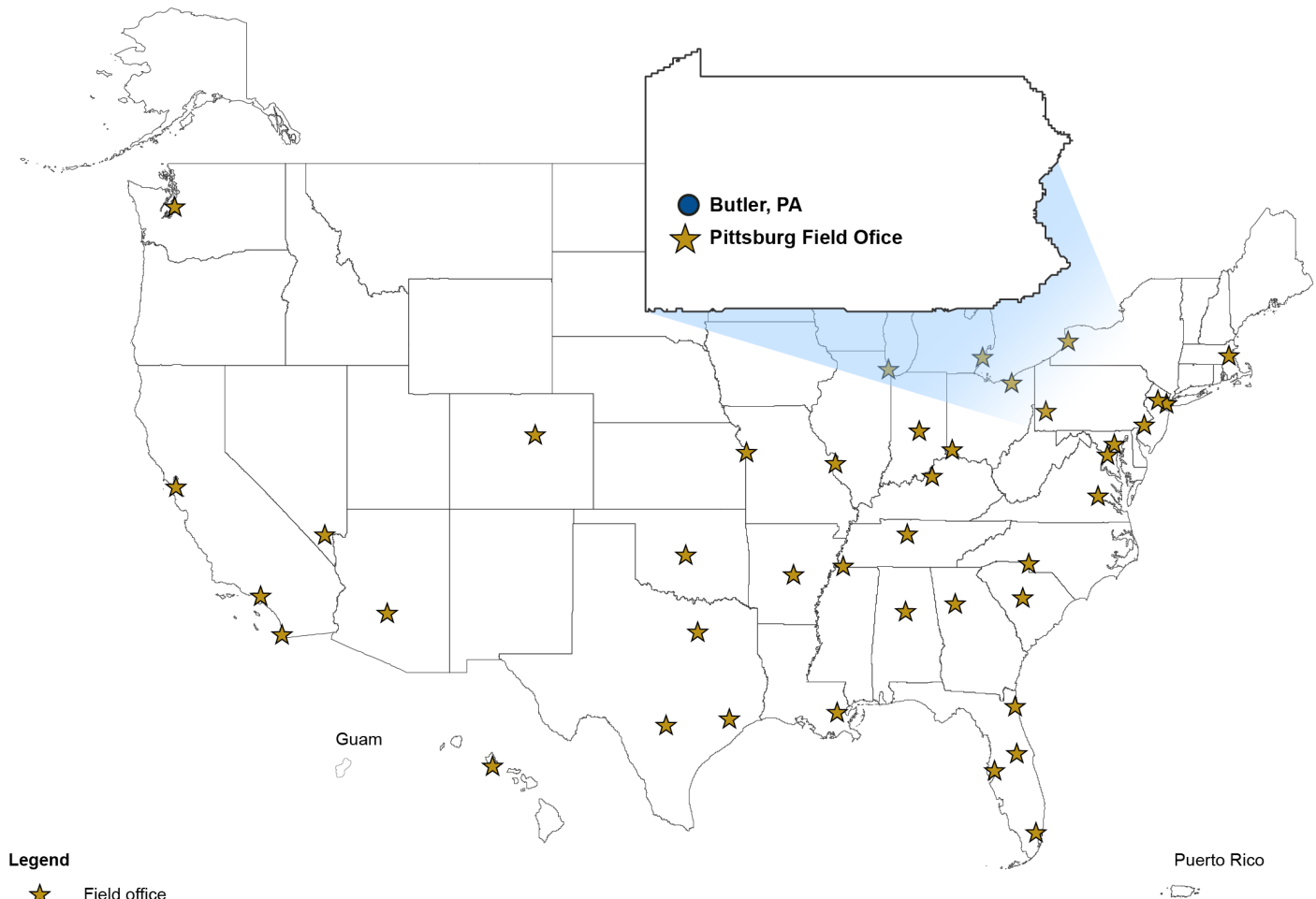
---

<sup>12</sup>The Secret Service is authorized by law 18 U.S.C. § 3056(a)(7) to protect major presidential and vice-presidential candidates and, within 120 days of a general presidential election, the spouses of such candidates. The Secretary of Homeland Security in consultation with an advisory committee consisting of the Speaker of the House, House Minority Whip, Senate Majority Leader, Senate Minority Leader, and one additional member chosen by the committee designate major presidential and vice-presidential candidates and nominees to be protected by Secret Service. Id.

<sup>13</sup>The following pages provide an overview of key Secret Service Divisions. In addition, the Secret Service contributes to NSSE and SEAR events. According to the Secret Service, it contributes to SEAR events when a protectee is scheduled to attend the event, or as part of the Federal Coordination Team, if appointed by DHS. See appendix II for information on these types of events.

See figure 1 for the locations of Secret Service field offices throughout the United States.

**Figure 1: Locations of Secret Service Field Offices in the United States**



Source: GAO analysis of U.S. Secret Service information. | GAO-25-108568SU

## Secret Service Offices Involved in Planning for the July 13, 2024, Rally

Multiple divisions within the Secret Service coordinate to plan and secure a protected event. To secure an event, different representatives from Secret Service divisions and other offices comprise an “advance team,” to include local Secret Service Field Office special agents and agents from other Secret Service divisions. Specifically, these advance team members will request assets, such as specialized personnel and equipment to secure protected events for which they are responsible.

---

**Office of Protective Operations.** OPO is responsible for oversight of Secret Service divisions that plan, direct, coordinate, and implement protective operations. OPO also manages policies and programs that govern and enable protective operations. OPO provides comprehensive protective measures for all persons and events authorized to receive Secret Service protection and coordinates protection for certain facilities, including the White House Complex, foreign diplomatic missions located in the National Capital Region, and residences of former Presidents, among others.

**Donald Trump Protective Division.** The Donald Trump Protective Division, within the operational protective divisions of OPO, provided continuous physical protection for the then-former President Donald Trump, then-former First Lady Melania Trump, and their youngest son. The Donald Trump Protective Division secured and safeguarded several sites in Palm Beach, Florida and New York City. The Donald Trump Protective Division also performed numerous special projects pertinent to the physical protection of the then-former First Family, and the security of related facilities.

**Protective Intelligence and Assessment Division.** The division is responsible for reviewing intelligence, assessing potential threats, and providing relevant information to the appropriate entities within the Secret Service. Personnel in this division work on protective intelligence investigations and conduct interviews with individuals who may pose a threat to a protectee. The Protective Intelligence and Assessment Division, within the Office of Strategic Intelligence and Information, plans, directs, and coordinates efforts involving the evaluation and dissemination of operational intelligence and threat information affecting the Secret Service's protective mission.

Much of this work is conducted by the Protective Intelligence and Assessment Division, which houses the Secret Service Open-Source Intelligence Branch. The Open-Source Intelligence Branch is responsible for providing open-source situational awareness to support protective operations and protective intelligence investigations, and to assist with assessments for protected persons, places, and events.

**Technical Security Division.** The division is responsible for providing secure environments for protectees and providing technical expertise for criminal investigations. Personnel in this division possess specialized skills such as improvised explosive device identification and can help mitigate threats from chemical and other attacks. They also support the



---

agency's criminal investigations with technical expertise and operational support.

**Special Operations Division.** The division is composed of specialized units that directly support the agency's worldwide protective mission. Each unit has a specific function that enhances the secure environment for protectees. The Special Operations Division managed assets such as counter sniper personnel, and prior to 2024, managed the Counter-Unmanned Aircraft Systems (cUAS) Branch.<sup>14</sup> This branch develops and implements unmanned aircraft systems (UAS) detection and mitigation plans for sites visited by the President and Vice President of the United States, including National Special Security Events (NSSE) and other designated major events.

**Secret Service Field Offices.** Within the Secret Service Office of Investigations, Secret Service Field Offices oversee and execute investigative and other priorities set by the Office of Investigations. They also liaise with state, local, tribal, territorial, and federal law enforcement agencies in support of both protective and investigative missions. Within their respective geographic districts, such as Pittsburgh and West Palm Beach, Field Offices support all protective operations and investigations in their assigned district.

Prior to all Secret Service protectee events, the Secret Service deploys a Secret Service advance team to the site. The advance team develops the security plan for the event and determines the resources and personnel needed to secure the event. Table 1 highlights general roles and responsibilities for the Secret Service advance team in place for the July 13, 2024, rally.

---

<sup>14</sup>According to the Secret Service, the Secret Service Office of Technical Development and Mission support began managing cUAS assets in January 2024.

**Table 1: Secret Service General Roles and Responsibilities for July 13, 2024, Site Security**

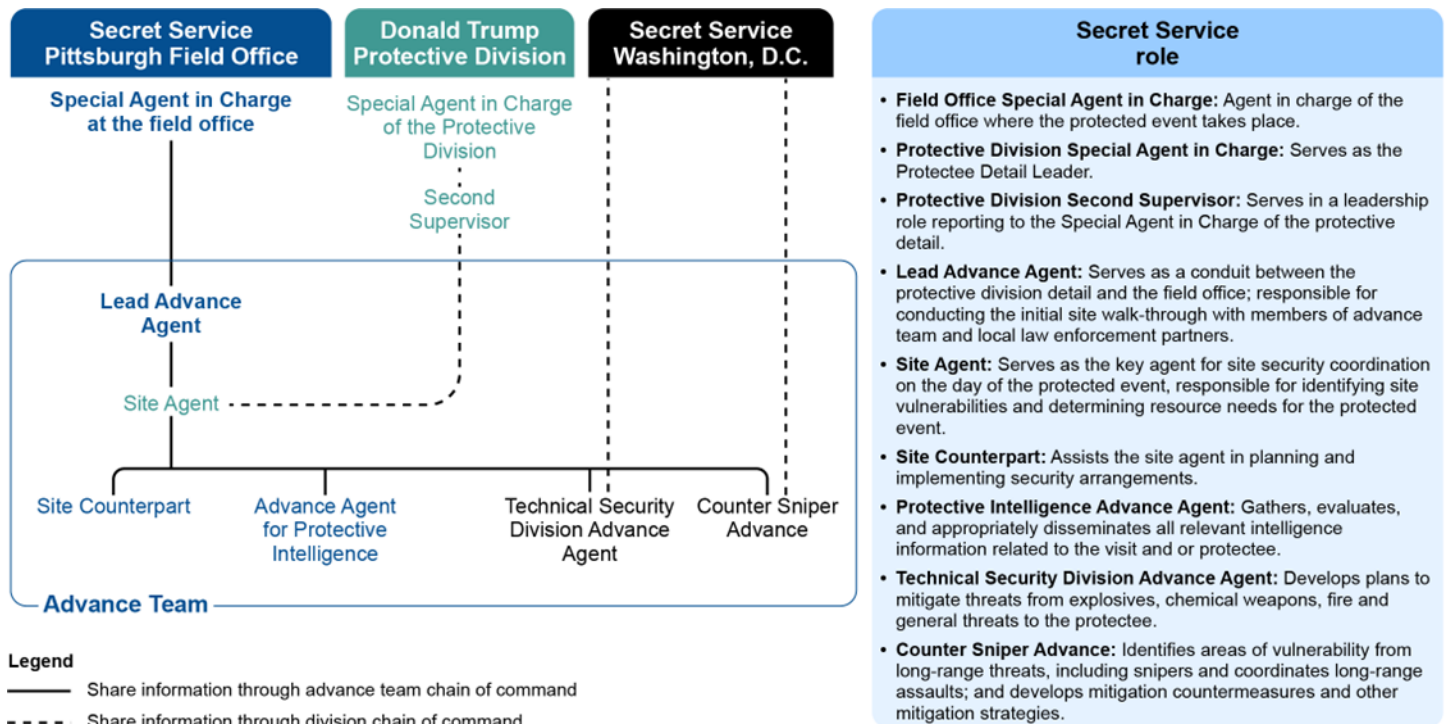
<b>Site Security Advance Team</b>	<b>Description of Advance Team responsibilities</b>
Field Office Special Agent in Charge	Coordinates decisions related to the operational security environment, in conjunction with the lead advance agent, including evaluating all equipment and personnel requirements prior to making the formal requests to the respective protective detail operations section. This Special Agent in Charge also notifies the Federal Bureau of Investigation (FBI) and local law enforcement/emergency services of pending events and communicates with the lead advance agent regarding any schedule changes, police meetings, intelligence concerns, support requests, and any other pertinent information regarding the event, among other responsibilities. The field office Special Agent in Charge is in charge of the Secret Service field office in the district where the protected event is held, which was the Pittsburgh field office during the July 13 rally.
Field Office Assistant to the Special Agent in Charge	Helps prepare protection and case work, approves timecards and travel vouchers, completes purchase orders, and on July 13, 2024, served as the Site Supervisor. The Site Supervisor is responsible for responding to critical incidents at the site and mitigating issues with advance personnel, detail personnel, campaign staff, and state and local law enforcement entities. The field office assistant to the Special Agent in Charge is assigned to the Secret Service field office in the district where the protected event is held and was from the Pittsburgh field office during the July 13 rally.
Lead Advance Agent	Can be a member of the field office or the protective division, and serves as a conduit between both entities, completes "preliminary site survey" and submits it to the Special Agent in Charge of the protective division, conducts site walk-throughs with relevant members of advance team and local law enforcement partners, and addresses all logistical considerations of Technical Security Division personnel and others working on the advance. During the July 13 rally, the lead advance agent was assigned to the Pittsburgh field office.
Site Agent	Identifies site-specific vulnerabilities, determines what resources and countermeasures are needed, in conjunction with special team(s), makes any necessary site adjustments, coordinates additional support—if required—through the lead advance agent, and creates a site security plan that identifies needed resources and personnel to mitigate site vulnerabilities. The site agent is also responsible for ensuring (1) all security personnel have been briefed on current threat intelligence, communication procedures, and emergency response measures; (2) personnel such as magnetometer officers, counter sniper technicians are briefed; and (3) detailed post instructions are provided to personnel assigned to various posts within and around the site. The site agent for the July 13 rally was assigned to the Donald Trump Protective Division. The site agent can be a member of the field office or the protective division.
Site Counterpart	Assists the site agent in planning and implementing security arrangements. During the July 13 rally, the site counterpart was assigned to the Pittsburgh field office.
Protective Intelligence Advance Agent	Gathers, evaluates, and appropriately disseminates all relevant intelligence information related to the visit and/or protectee; maintains communication with Protective Intelligence and Assessment Division, other federal agencies, and local law enforcement partners; coordinates use of protective intelligence teams consisting of Secret Service and local law enforcement personnel; and ensures all intelligence information has been disseminated to post-standers, the command post/security room, and the working detail. During the July 13 rally, the protective intelligence advance agent was assigned to the Pittsburgh field office. However, in some cases, the protective intelligence advance agent may be assigned to the Secret Service's Protective Intelligence and Assessment Division, which is a Secret Service headquarters-based division.
Counter-Unmanned Aircraft System (cUAS) Advance Agent	Coordinates cUAS requirements prior to departure including determining type(s) of equipment required, and location of deployment site(s). Prior to July 13, this responsibility was typically performed by personnel from the Technical Security Division. However, due to limited personnel, the Donald Trump Division assigned an agent from their own division to this role. The cUAS advance agent is deployed on an as-needed basis, and during the July 13 rally, this agent was assigned to the Donald Trump Protective Division.
Counter Sniper Advance	Identifies areas of vulnerability from long-range threats, including snipers and coordinated long-range assaults; and develops mitigation countermeasures (i.e., counter snipers) and other mitigation strategies (e.g., coordination with local tactical assets) to address identified vulnerabilities. The counter sniper advance is assigned to the Special Operations Division, which is a Secret Service Washington, D.C. based division.

Site Security Advance Team	Description of Advance Team responsibilities
Counter Assault Team Advance Agent	Coordinates the overall tactical plan and assets (local, state, and federal partners) that may be deployed and utilized during a protected event in conjunction with other Secret Service and supporting advance partners. The counter assault team advance agent is assigned to the Special Operations Division, which is a Secret Service Washington, D.C. based division. The counter assault team advance agent position could also be filled by a former counter assault team agent now assigned to a field office.
Technical Security Lead Coordinator	Develops plans to mitigate threats from explosives, chemical weapons, fire, and general threats to the protectee; and coordinates bomb sweeps prior to a protected event. The technical security lead coordinator is assigned to the Technical Security Division, which is a Washington, D.C. based division.
<b>Protective detail</b>	
Special Agent in Charge of the Donald Trump Division	Serves as the Protectee Detail Leader; in conjunction with the field office Special Agent in Charge, develops contingency plans as the situation warrants to ensure the safety of the protectee.
Second Supervisor of the Donald Trump Division	Serves in a leadership role reporting to the Special Agent in Charge of the protective detail and conducts a walk-through of the site. The overall responsibility of the Second Supervisor is to review all facets of the visit security plan to include the site security plan and make any necessary adjustments. For the July 13, 2024, rally, the Second Supervisor signed off and approved the site security plan after having been briefed by the lead advance agent and site agent.

Source: Analysis of U.S. Secret Service Information. | GAO-25-108568SU

Figure 2 conveys the structure of the Secret Service advance team for the July 13 rally along with what divisions each position was sourced from.

Figure 2: Secret Service Advance Team Members for the July 13, 2024, Rally



Source: GAO analysis of Secret Service policies and July 13, 2024, planning documents. | GAO-25-108568SU

## Timeline of Key Actions During the July 13, 2024, Rally

We identified a timeline of key events, based on our review of pertinent communication records such as email, text messages, local law enforcement body camera footage, radio logs, and other documents such as site diagrams and surveys. These records provide insight into the actions the Secret Service and local law enforcement officials took leading up to and during the rally. Table 2 conveys a timeline of key events. For additional information on the key actions of the July 13, 2024, rally, see appendix IV.

**Table 2: Timeline of Key Actions Taken Related to the July 13, 2024, Campaign Rally**

Date	Description
July 2, 2024	The Secret Service reported that the Pittsburgh Field Office Special Agent in Charge was notified by phone of a potential visit by then-former President Donald Trump on July 13, 2024.
July 3, 2024	The Intelligence Community identified threat-related information about former President Trump and notified a Secret Service Federal Bureau of Investigation (FBI) Counterterrorism Division Liaison of the information. In addition, the Secret Service Protective Intelligence and Assessment Division provided a classified briefing on the threat-related information to senior Office of Protective Operations officials.
July 5, 2024	The Secret Service Pittsburgh Field Office invited local law enforcement partners to a police meeting on July 8, 2024.
July 8, 2024	Secret Service advance team held a walkthrough at the Butler site, which included a Trump campaign staffer. The Secret Service also held a police briefing with state and local law enforcement.
July 9, 2024	Members of the advance team, including the lead advance agent, site agent, and site counterpart conducted an initial police walkthrough with the Pennsylvania State Police, and further discussed post assignments at the Butler Pennsylvania State Police location. The Donald Trump Protective Division Second Supervisor called lead advance agent regarding threat information concerning Trump, and the Office of Protective Operations' request for counter sniper assets was approved.
July 11, 2024	The Secret Service conducted another walkthrough with state and local law enforcement. The Secret Service advised the Intelligence Community that the counter sniper asset was "turned on" (i.e., approved and provided) for former President Trump.
July 12, 2024	The site agent, including the site counterpart, led a walkthrough with the Donald Trump Protective Division Second Supervisor.
July 13, 2024	<p>Trump campaign rally on July 13, 2024:</p> <ul style="list-style-type: none"> <li>11:21 a.m.: Butler Emergency Management Services shared a social media post about threats to Donald Trump with the protective intelligence advance agent, who then shared it with members of the Advance Team.</li> <li>3:51 p.m.: According to the FBI, the gunman, Thomas Matthew Crooks, flew his drone for approximately 11 minutes in the vicinity of the site.</li> <li>4:26 p.m.: Beaver County Snipers noted that they observed an individual, sitting on a picnic table, who parked in a restricted area, and observed Beaver County Snipers move into the AGR International, Inc. building.</li> <li>5:14 p.m.: Beaver County snipers located inside the AGR building noticed Crooks sitting on a small concrete wall.</li> <li>5:38 p.m.: Beaver County snipers observed Crooks with a rangefinder and were asked to call it into the command post.</li> <li>5:45 p.m.: Beaver County snipers and Butler Emergency Services Unit personnel sent photos of the gunman to the local mobile command post and to Secret Service Counter Snipers.</li> <li>5:56 p.m.: Local law enforcement observed Crooks with a backpack.</li> <li>6:00 p.m.: Local law enforcement observed Crooks entering an alcove between the AGR buildings.</li> <li>6:08 p.m.: A person, later identified as Crooks, was observed on the roof of the AGR building.</li> <li>6:11 p.m.: The gunman was observed with a long gun by local law enforcement and fired shots.</li> </ul>

Source: GAO analysis of U.S. Secret Service, FBI, Pennsylvania State Police, and local law enforcement information, which includes emails, texts, radio logs, and body camera footage. | GAO-25-108568SU

In preparation for protected events, the Secret Service partners with other federal, state, local, and private entities to provide security for an event. Figure 3 lists the federal, state, and local law enforcement personnel who supported the Secret Service in securing the July 13 rally.

**Figure 3: Secret Service and Other Key Federal, State, Local, and Private Entities That Had Responsibilities for Planning and Securing the July 13, 2024, Rally**

U.S. Secret Service	Other federal agencies	State and local law enforcement	External entities
 <b>Office of Protective Operations</b> <ul style="list-style-type: none"> <li>• Donald Trump Protective Division</li> <li>• Dignitary Protective Division                             <ul style="list-style-type: none"> <li>◦ Candidate Nominee Operations Section</li> </ul> </li> <li>• Special Operations Division</li> </ul>	 <b>Department of Defense</b>   <b>Department of Homeland Security</b> Homeland Security Investigations	 <b>Pennsylvania State Police</b>   <b>Beaver County</b>   <b>Butler County</b>   <b>Butler Township</b>   <b>Washington County</b>	 <b>Donald Trump Campaign Staff</b>   <b>Butler Farm Show Venue Personnel</b>
 <b>Pittsburgh Field Office</b>			

Source: GAO review of agency information; agency logos courtesy of respective agencies; Christos Georghiou/stock.adobe.com (badge icon); 123levit/stock.adobe.com (flag icon); arabel0305/stock.adobe.com (stage icon). | GAO-25-108568SU

## DHS and Congressional Investigations

Three investigative entities that reviewed the actions and failures of the July 13, 2024, rally identified a number of challenges that contributed to shortfalls during the rally.<sup>15</sup>

**Poorly defined policies for protecting former Presidents.** The Senate Committee on Homeland Security and Governmental Affairs (HSGAC) and DHS Independent Review Panel investigating the July 13 assassination attempt concluded that Secret Service policies are ill-

<sup>15</sup>Department of Homeland Security, *Report of the Independent Review Panel on the July 13, 2024, Assassination Attempt in Butler, Pennsylvania*, (Washington, D.C.: Oct. 15, 2024). United States Senate Committee on Homeland Security and Governmental Affairs, *Interim Joint Report: Examination of U.S. Secret Service Planning and Security Failures Related to the July 13, 2024, Assassination Attempt*, (Washington, D.C.: Sept. 2024). United States House of Representatives, *Task Force on the Attempted Assassination of Donald J. Trump: Final Report of Findings and Recommendations*, (Washington, D.C.: Dec. 5, 2024). For the purpose of this report, we use the term "House Task Force" to refer to the House of Representatives Task Force on the Attempted Assassination of Donald J. Trump.



defined and outlined recommendations to address these issues.<sup>16</sup> For example, the DHS Independent Review Panel recommended that the Secret Service update its policies concerning site advance planning and site security to document overall responsibility for site advance planning, a detailed chain of command process, and how Secret Service personnel should interact with federal and local law enforcement partners.<sup>17</sup> Secret Service personnel noted that agents conducting advances for former presidential details rely on the overarching OPO policies to provide protection and secure environments.

**Heavy use of external partners.** The investigative entities also found that the Secret Service relies heavily on its partnerships with federal and local law enforcement partners to ensure the security and safety of the protectees under their charge. However, relying on partners presents some challenges due to the limited training partners receive specific to the event. For example, some U.S. Immigration and Custom Enforcement's Homeland Security Investigations (HSI) personnel assigned to the rally had limited experience working with the Secret Service and were not familiar with Secret Service protocols or the site they were assigned to.<sup>18</sup> The Secret Service utilizes "jump teams" during campaigns to fill various security posts and other protective support

---

<sup>16</sup>Department of Homeland Security, *Report of the Independent Review Panel on the July 13, 2024, Assassination Attempt in Butler, Pennsylvania*, (Washington, D.C.: Oct. 15, 2024). United States Senate Committee on Homeland Security and Governmental Affairs, *Interim Joint Report: Examination of U.S. Secret Service Planning and Security Failures Related to the July 13, 2024, Assassination Attempt*, (Washington, D.C.: Sept. 2024).

<sup>17</sup>Department of Homeland Security, *Report of the Independent Review Panel on the July 13, 2024, Assassination Attempt in Butler, Pennsylvania*, (Washington, D.C.: Oct. 15, 2024).

<sup>18</sup>Department of Homeland Security, *Report of the Independent Review Panel on the July 13, 2024, Assassination Attempt in Butler, Pennsylvania*, (Washington, D.C.: Oct. 15, 2024). United States Senate Committee on Homeland Security and Governmental Affairs, *Interim Joint Report: Examination of U.S. Secret Service Planning and Security Failures Related to the July 13, 2024, Assassination Attempt*, (Washington, D.C.: Sept. 2024). United States House of Representatives, *Task Force on the Attempted Assassination of Donald J. Trump: Final Report of Findings and Recommendations*, (Washington, D.C.: Dec. 5, 2024).



---

assignments within and around the site. These jump teams typically consist of six agents, at least one being a Secret Service special agent.<sup>19</sup>

The House Task Force recommended that the Secret Service work with U.S. Immigration and Custom Enforcement's HSI to ensure agents participating in Secret Service-led protective operations receive appropriate training.<sup>20</sup>

During the Secret Service's review of the incidents that took place on July 13, 2024, it found that while some U.S. Immigrations and Customs Enforcement HSI special agents stated that they had a clear understanding of their duties following the security briefing, others conveyed that they were inadequately prepared due to insufficient training. Secret Service Office of Training officials stated that while virtual training provides a flexible option to help prepare partner agencies for protectee events, in-person training is usually a more effective option. Secret Service officials also stated that the Office of Training offers training to all supporting law enforcement partners upon request. Training officials noted that the Secret Service offers in-person and virtual training upon request.

**Insufficient training and experience.** In addition, the investigative entities found that key individuals such as the site agent, the counter-unmanned aircraft system (cUAS) agent, and the protective intelligence advance agent filled roles that could have been filled by other, more

---

<sup>19</sup>Federal partners that commonly work with the Secret Service include the Department of Homeland Security HSI and the Department of Defense. The Secret Service also coordinates with additional federal partners like the FBI to process and disseminate threat intelligence regarding protectees and protected events. In addition to federal partners, Secret Service also relies on local law enforcement partners to secure protected events as well. During our discussion with OPO officials, they stated that as of October 9, 2024, HSI provided Secret Service over 520 special agents, the Transportation Security Administration provided 90 federal Air Marshalls, and the Department of Defense approved air support for over 37 missions to support Secret Service protective operations across the country.

<sup>20</sup>United States House of Representatives, *Task Force on the Attempted Assassination of Donald J. Trump: Final Report of Findings and Recommendations*, (Washington, D.C.: Dec. 5, 2024).

experienced personnel from more specialized divisions.<sup>21</sup> For the July 13 rally, the assigned site agent was new to the role, with the event being her first time planning and securing a large outdoor event as the site agent. In addition, the cUAS agent had very limited experience in his role as well. Further, the protective intelligence advance agent was not deployed from the Protective Intelligence and Assessment Division. Rather, he was deployed from the Secret Service Pittsburgh Field Office and had limited experience in this role.<sup>22</sup> Secret Service officials noted that they planned to take additional steps in the future to conduct a more thorough review of an agent's experience prior to making a protective advance assignment.<sup>23</sup>

The House Task Force recommended that the Secret Service allow less-experienced personnel to participate in advance planning for low-risk events, and instead rely on more experienced agents for high-risk protection events like the July 13 rally.<sup>24</sup> In addition, the DHS Independent Review Panel recommended that the Secret Service require all former presidential, candidate, and nominee details, along with all field offices, to

---

<sup>21</sup>Department of Homeland Security, *Report of the Independent Review Panel on the July 13, 2024, Assassination Attempt in Butler, Pennsylvania*, (Washington, D.C.: Oct. 15, 2024). United States Senate Committee on Homeland Security and Governmental Affairs, *Interim Joint Report: Examination of U.S. Secret Service Planning and Security Failures Related to the July 13, 2024, Assassination Attempt*, (Washington, D.C.: Sept. 2024). United States House of Representatives, *Task Force on the Attempted Assassination of Donald J. Trump: Final Report of Findings and Recommendations*, (Washington, D.C.: Dec. 5, 2024).

<sup>22</sup>Secret Service officials noted that deploying a protective intelligence advance agent from the field is routine.

<sup>23</sup>Secret Service officials from the Office of Training told us that each Secret Service agent receives extensive training on how to conduct protection operations, specifically for performing site security duties in advance of an event (i.e., site advance). During Secret Service basic training, trainees receive a comprehensive overview of general protection tactics, maneuvers, and coordination. This training teaches recruits how to identify line-of-sight concerns, suspicious activity/individuals, and how to set up a security room. Secret Service Training Officials stated that trainees receive a 2-week intensive training on advance planning and procedures.

<sup>24</sup>United States House of Representatives, *Task Force on the Attempted Assassination of Donald J. Trump: Final Report of Findings and Recommendations*, (Washington, D.C.: Dec. 5, 2024).

adopt a policy requiring the use of experience-based methods for the selection of site and advance agents.<sup>25</sup>

**Siloed communication among Secret Service, state, and local law enforcement.** The investigative entities identified challenges and a lack of coordination between local law enforcement partners, such as establishing separate communication centers.<sup>26</sup> For example, Secret Service personnel did not ensure that the security room was properly staffed with representatives from all law enforcement agencies supporting the event. The Senate HSGAC recommended that DHS and the Secret Service ensure communications plans between federal, state, and local law enforcement agencies and first responders are properly executed and should ensure records retention capabilities.<sup>27</sup> Further, the DHS Independent Review Panel recommended that the Secret Service ensure that one or more representatives from the Secret Service and each supporting law enforcement agency operating at the event be physically collocated with one another in the space which is serving as the central communications hub for the event, for the purpose of facilitating centralized communications.<sup>28</sup>

Further, the investigative entities found that Secret Service agents did not request or review all law enforcement partner operational plans which contributed to a breakdown in understanding roles and responsibilities. Specifically, the Secret Service advance team did not request law enforcement partner plans, and OPO policies did not instruct Secret Service personnel to integrate law enforcement partner plans or assess

---

<sup>25</sup>Department of Homeland Security, *Report of the Independent Review Panel on the July 13, 2024, Assassination Attempt in Butler, Pennsylvania*, (Washington, D.C.: Oct. 15, 2024).

<sup>26</sup>Department of Homeland Security, *Report of the Independent Review Panel on the July 13, 2024, Assassination Attempt in Butler, Pennsylvania*, (Washington, D.C.: Oct. 15, 2024). United States Senate Committee on Homeland Security and Governmental Affairs, *Interim Joint Report: Examination of U.S. Secret Service Planning and Security Failures Related to the July 13, 2024, Assassination Attempt*, (Washington, D.C.: Sept. 2024). United States House of Representatives, *Task Force on the Attempted Assassination of Donald J. Trump: Final Report of Findings and Recommendations*, (Washington, D.C.: Dec. 5, 2024).

<sup>27</sup>United States Senate Committee on Homeland Security and Governmental Affairs, *Interim Joint Report: Examination of U.S. Secret Service Planning and Security Failures Related to the July 13, 2024, Assassination Attempt*, (Washington, D.C.: Sept. 2024).

<sup>28</sup>Department of Homeland Security, *Report of the Independent Review Panel on the July 13, 2024, Assassination Attempt in Butler, Pennsylvania*, (Washington, D.C.: Oct. 15, 2024).

---

their capabilities when planning for a protected event. The Senate HSGAC noted that while such plans were not requested, some advance team members, such as the site agent, reviewed one of the operational plans from the Pennsylvania State Police. The Senate HSGAC recommended that Secret Service policies require advance planning leads to request and review state and local operational plans in advance of any protected event to ensure a shared understanding of security responsibilities and vulnerabilities as well as other critical planning and security components.<sup>29</sup> Further, the House Task Force recommended that the Secret Service consolidate all partner operational plans when planning for a protected event.<sup>30</sup>

---

### **Steps the Secret Service Has Taken to Address Identified Shortfalls**

Since the July 13 rally, the Secret Service has taken several steps to address the failures and shortfalls identified above. For example, it updated its policy to ensure Secret Service advance teams request and review site security plans developed by local law enforcement partners prior to a protected event.<sup>31</sup> This new policy also requires that the advance team coordinate to ensure redundant communications by establishing primary, alternate, contingency, and emergency communications plans.<sup>32</sup> In addition, the Secret Service has begun developing a handbook to be provided to state and local law enforcement partners, to help provide these partners with a better understanding of Secret Service protective operations, and Secret Service expectations when partnering with local law enforcement during protected events. At the time of our review, the Secret Service was working toward addressing the more than 50 recommendations made by the investigative entities. According to the Secret Service, it will need additional time to address the recommendations. See appendix III for a list of recommendation made to the Secret Service in 2024 and 2025 by DHS and other congressional investigative committees.

---

<sup>29</sup>United States Senate Committee on Homeland Security and Governmental Affairs, *Interim Joint Report: Examination of U.S. Secret Service Planning and Security Failures Related to the July 13, 2024, Assassination Attempt*, (Washington, D.C.: Sept. 2024).

<sup>30</sup>United States House of Representatives, *Task Force on the Attempted Assassination of Donald J. Trump: Final Report of Findings and Recommendations*, (Washington, D.C.: Dec. 5, 2024).

<sup>31</sup>Secret Service, *OPO-03(01): Protective Advance Overview* (Washington, D.C.: April 10, 2025).

<sup>32</sup>Secret Service, *OPO-08: Communications* (Washington, D.C.: Sept. 11, 2024).

---

## Policy Gaps, Noncompliance, and Insufficient Threat Sharing Contributed to Security Failures on July 13, 2024

---

### Secret Service's Roles and Responsibilities Are Not Fully Documented in Policy

We found that leading up to the July 13 rally, Secret Service policies for securing protected events were overly broad, did not clearly assign specific protective responsibilities, and omitted some key roles and responsibilities. Other investigative entities also found that prior to the July 13 rally, Secret Service policies lacked specific and complete guidance outlining roles and responsibilities for agents assigned to secure the rally, which resulted in agents being left to define their own responsibilities. For example, the Senate HSGAC reported that Secret Service advance personnel roles and responsibilities were unclear and lacked accountability.<sup>33</sup> As a result, that committee recommended that the Secret Service update its guidance to ensure Secret Service guidance includes defined roles and responsibilities for personnel responsible for advance planning.

*Standards for Internal Control in the Federal Government* emphasize that policies should be documented at the appropriate level of detail to allow management to effectively monitor control activities.<sup>34</sup> In addition, these standards state that management should internally communicate the necessary quality information to achieve the entity's objectives. This can include identifying the appropriate method of communication.

Further, selected *Leading Practices for Interagency Collaboration* identified in our prior work calls for agencies to collaborate and work together to define and agree on their respective roles and responsibilities,

---

<sup>33</sup>United States Senate Committee on Homeland Security and Governmental Affairs, *Interim Joint Report: Examination of U.S. Secret Service Planning and Security Failures Related to the July 13, 2024, Assassination Attempt*, (Washington, D.C.: Sept. 2024).

<sup>34</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014).

including how the collaborative effort will be led.<sup>35</sup> In this scenario, by defining and documenting roles and responsibilities, the Secret Service and supporting agencies can clarify who will do what, organize their joint and individual efforts, and facilitate decision-making.

Prior to the July 13, 2024 rally, the Office of Protective Operations (OPO) developed and issued numerous policy documents covering the roles and responsibilities for properly securing a protected event that Secret Service agents could review to refamiliarize themselves with protective operation procedures.<sup>36</sup> The policies covered a wide range of topics and scenarios regarding general procedures for conducting a site advance.<sup>37</sup> However, roles and responsibilities outlined in these policy documents lacked appropriate detail to ensure required tasks were completed prior to the arrival of the protectee.

Further, during our discussions with Secret Service advance team personnel, at least five of the 14 agents that performed key roles on July 13 noted that the policy documents that OPO provided were broad and spread over numerous policies. Therefore, instead of using them for guidance in planning for the rally they relied on their overall protection experience.

Based on our interviews with members of the site advance team and our review of Secret Service policies, there were several contributing factors that led to the security failures during the July 13 rally, including a lack of clear roles and responsibilities documented in policy for all advance team members, confusion on how to properly set up the security room, and the failure to review local law enforcement operational plans, among others. Specifically:

---

<sup>35</sup>GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, [GAO-23-105520](#), (Washington, D.C.: May 24, 2023). Using this list of leading interagency collaboration practices, we selected the practices most relevant and applicable to the actions and processes used by the Secret Service to prepare for the July 13, 2024, campaign rally.

<sup>36</sup>In addition to OPO, other Secret Service divisions (e.g., Protective Intelligence and Assessment Division, Special Operations Division, Technical Security Division.) and branches have created similar guidance documents outlining roles and responsibilities that pertain to their mission and personnel responsibilities. However, for the purposes of our analysis we focused mainly on OPO guidance since they provide a general overview of site advance.

<sup>37</sup>For the purposes of this review, we identified a set of key OPO policies that apply to securing protected events similar to the July 13 campaign rally.

- Three out of 14 key protective roles did not have any responsibilities defined in OPO policies. These roles are the site counterpart, protective detail second supervisor, and the site supervisor.<sup>38</sup> Each of these agents played a significant part in planning and securing the July 13 rally but did not have responsibilities like reviewing site diagrams, conducting site walk-throughs with advance team personnel and local law enforcement, and ensuring the site build met the needs of the protective detail documented in policy.
- OPO policies did not provide clarity on who is responsible for overseeing the setup of the Secret Service security room. For example, policy states that “the determination for use of a security room may depend on the advance conducted for the visit or the individual protective division guidelines.”<sup>39</sup> However, during our discussions with the site agent and site counterpart there was confusion on who was responsible for setting up the Secret Service security room on July 13.
- OPO policies did not require the advance team to request and review local law enforcement operational plans or ensure all law enforcement representatives were present in the Secret Service security room. This led to a breakdown in communication and coordination between the Secret Service and law enforcement partners, which contributed to the gunman’s ability to evade law enforcement personnel on July 13.

General roles and responsibilities for conducting site advances are dispersed over more than 20 OPO policy documents, not including separate division-specific (e.g., Special Operations Division, Technical Security Division, and the Protective Intelligence and Assessment Division) guidance as well. As a result, it is difficult for agents, especially inexperienced agents, to have a comprehensive understanding of their required roles and responsibilities. For example, the lead advance and site agent roles and responsibilities have responsibilities identified in

---

<sup>38</sup>Secret Service OPO policies (OPO-03 and OPO-06) mention different types of counterparts (e.g., Field Counterpart, Protectee’s Staff Counterpart, and Police Counterpart). However, there is no clear distinction between these roles written in policy. Further, OPO-03 does mention that the advance team, field counterparts, and local law enforcement are responsible for conducting a site security survey. However, OPO policy does not delegate a specific task regarding the site security survey to the Site Counterpart.

<sup>39</sup>Secret Service, *OPO-08: Communication*, (Washington, D.C.: Nov. 23, 2023).



---

multiple policies including OPO-03, OPO-06, OPO-08, and OPO-13, among others.<sup>40</sup>

Because Secret Service policies in place at the time of the rally were broad and did not consistently clarify which agent was supposed to complete a specific task, and some tasks lacked detail, it was difficult for us to determine with certainty whether a majority of the roles and responsibilities delegated to multiple advance team personnel for the July 13 campaign rally were technically satisfied or completed. However, the outcome of the July 13 rally showed that the Secret Service advance team did not ensure proper mitigation, communication, and coordination efforts had been effectively carried out.

Since the July 13 rally, the Secret Service has taken steps to revise its policies to further clarify roles and responsibilities. OPO, in particular, has created additional guidance providing further detail to Secret Service personnel regarding the roles and responsibilities for conducting an advance. For example, the updated policies convey the following:

- Additional roles and responsibilities for the site counterpart, field office site supervisor, and the protective detail second supervisor are outlined in policy;<sup>41</sup>
- The advance team is now required to request and review all operational plans from law enforcement partners prior to the protective visit to ensure there is a shared understanding of areas of concern and roles and responsibilities;<sup>42</sup> and
- The lead advance agent is in charge of setting up the command post, ensuring that all relevant documentation (e.g., surveys, post

---

<sup>40</sup>In addition, Secret Service has updated and issued additional policies since July 13 including *OPO-03(01): Protective Advance Overview*, (Washington, D.C.: Apr. 10, 2025), *OPO-03(02): Advance Team Components*, (Washington, D.C.: Apr. 10, 2025), *OPO-03(03): Protective Advance Meetings and Briefings*, (Washington, D.C.: Apr. 10, 2025), *OPO-03(04): Situation Reports*, (Washington, D.C.: Apr. 10, 2025), *OPO-24: Protective Operations Staffing and Logistics*, (Washington, D.C.: Nov. 7, 2024), and *OPO-25: Protective Operations Accountability*, (Washington, D.C.: Apr. 4, 2025).

<sup>41</sup>Secret Service, *OPO-25: Protective Operations Accountability*, (Washington, D.C.: Apr. 4, 2025), and Secret Service, *OPO-03(01): Protective Advance Overview*, (Washington, D.C.: Apr. 10, 2025).

<sup>42</sup>Secret Service, *OPO-03(01): Protective Advance Overview*, (Washington, D.C.: Apr. 10, 2025).

---

assignments log, law enforcement partner operational plans, etc.) and personnel are present.<sup>43</sup>

These additions are positive and demonstrate that the Secret Service has taken steps to address the overarching failures that occurred on July 13. However, while the Secret Service has taken steps to address gaps in its policies, requirements for roles and responsibilities remain widely dispersed across multiple policies, making it difficult for Secret Service personnel to have a full understanding of what their roles and responsibilities are when conducting an advance.

In reviewing the roles and responsibilities outlined in the new OPO policies, we found that the policies do not provide Secret Service personnel with readily available information (e.g., a checklist or other readily available quick guides) delineating specific tasks that need to be completed when conducting a site advance.

Due to the policies being widely dispersed, developing and providing readily available information, such as a checklist or some other related resource such as an app-based resource guide accessible through agency issued cell phones, could be a valuable tool for personnel, especially those who may have less protection experience—like the site agent, cUAS agent, and protective intelligence advance agent assigned to the July 13 rally.<sup>44</sup>

During our review, we also found that the Secret Service has operationalized the use of checklists for personnel performing specialized roles.<sup>45</sup> However, OPO has not created such a tool for roles like the lead advance agent, site agent, or site counterpart agent responsible for securing a protected event. OPO has updated its policies to include a single document with bulleted general responsibilities for each advance

---

<sup>43</sup>Secret Service, *OPO-08: Communications*, (Washington, D.C.: Sept. 11, 2024), and Secret Service, *OPO-03(02): Advance Team Components* (Washington, D.C.: Apr. 10, 2025).

<sup>44</sup>Further, it would be optimal for Secret Service to assign experienced agents to these site advance roles, however, due to periods of increased operational tempo that the Secret Service experiences during campaign years, this is not always feasible and agents with little experience may need to be relied upon to complete the mission.

<sup>45</sup>The Special Operations Division and Protective Intelligence and Assessment Division have created a resource/checklist for personnel including the Counter Sniper Advance, Counter Assault Team Advance, and Protective Intelligence Advance to use and refer to when conducting a site advance.

---

team role.<sup>46</sup> However, this document does not capture key responsibilities that are dispersed throughout the other policies.

At the beginning of our review, Secret Service officials told us that their policies are not meant to be overly prescriptive because each protected event is different. Therefore, policies are broad to address various situations that Secret Service agents may encounter while conducting a site advance for a protectee. Secret Service officials also stated that in addition to the OPO policy documents, the Secret Service maintains resources such as training manuals and PowerPoints to provide refreshers on advance team roles and responsibilities for agents performing protective operations.

While it would be impractical to create a checklist that includes every security consideration for every site and situation, agents would benefit from a readily available resource identifying the actions and responsibilities they would likely perform during most, if not all, protectee events. For example, a resource that outlines the tasks for collecting and reviewing state and local operational plans, ensuring line-of-sight mitigation equipment is in place, and ensuring representatives from all supporting agencies are present in the Secret Service command post/security room could help ensure agents adequately secure protected events.

As previously noted, the Secret Service has many policies and training manuals available for review. However, agents that we interviewed did not report referring to these documents in preparation for the event. Instead, they reported relying on their experience, which in some cases they self-reported to be limited. Further, specialized divisions of the Secret Service have created resource guides such as a checklist for select positions, including the counter sniper and counter assault advance teams, but not for other positions such as the lead advance or site counterpart agent.

Creating a resource that outlines the requisite forms and paperwork to complete during an advance, or specifying how to properly equip a security room may better prepare agents who are responsible for conducting site security advances. Therefore, creating a tool that captures key responsibilities and tasks in one comprehensive source, at

---

<sup>46</sup>Secret Service, *OPO-03(02): Advance Team Components*, (Washington, D.C.: Apr. 10, 2025).

---

least by role, could better ensure Secret Service agents perform the fundamental baseline set tasks for securing a site, and help them determine whether additional security measures are needed.

---

**Policy Barriers Contributed  
to Ineffective Sharing of  
Threat Information Within  
the Secret Service and  
with Local Law  
Enforcement Partners**

As reported in public media and conveyed during Congressional hearings, prior to the July 13 rally, the Secret Service became aware of a general threat regarding then-former President Trump, at some point in the future.<sup>47</sup> However, due to the Secret Service's siloed process for sharing classified threat information, Secret Service and local law enforcement personnel were unaware of the general threat. Although some senior level Secret Service personnel were aware of this threat information, other senior personnel who had responsibilities for providing protective equipment for the rally, report to have been unaware of the threat information.

According to Secret Service officials, this information was not more broadly shared across the Secret Service partly because the information was highly classified, which involved constraints from the Intelligence Community on sharing information. In addition, the Intelligence Community did not include tear line information at a lower classification level to share.<sup>48</sup> Another reason, however, was that the information was general in nature and not specific to the Butler, Pennsylvania event. The Secret Service had no process to share classified threat information with partners when the information is deemed highly classified and a significant threat to security operations, but not considered an imminent threat to life.<sup>49</sup>

In the days leading up to the rally, senior Secret Service officials across multiple divisions either had access to or received one-time "read-ins" regarding classified threat intelligence information related to then-former President Donald Trump.<sup>50</sup> Figure 4 displays a timeline of when various

---

<sup>47</sup>According to Secret Service officials, the general threat information provided to some Secret Service officials prior to the rally was not related to the Butler rally, or to the July 13 gunman.

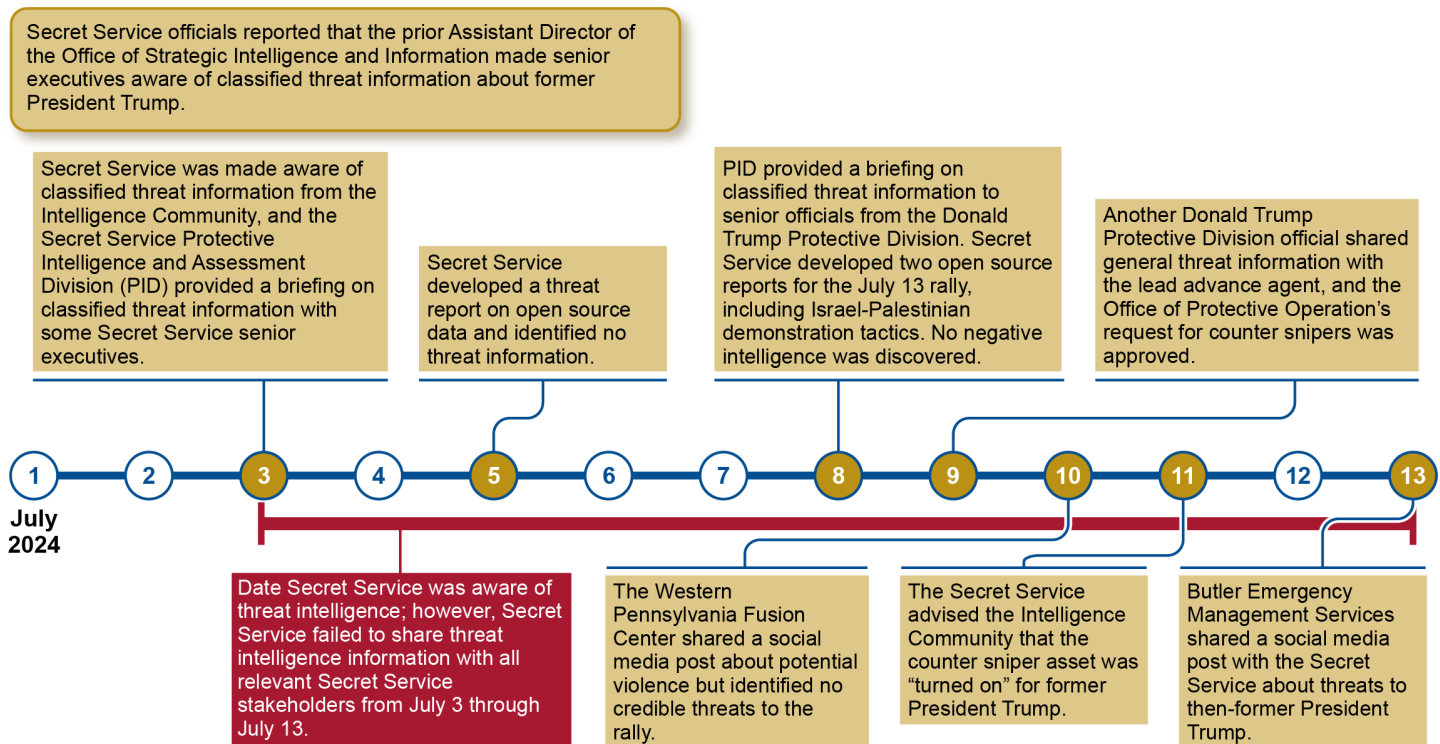
<sup>48</sup>A "tear line" in an intelligence document indicates the point at which a sanitized, less classified version begins.

<sup>49</sup>Secret Service officials noted that processes exist for sharing information when partners have the appropriate clearance. Sharing of classified information would also be dependent on having access to appropriate facilities for sharing the information.

<sup>50</sup>The term "read-in" refers to the process of requesting approval for an individual to have access to highly classified information.

entities and officials received classified threat intelligence and other threat information.

**Figure 4: Timeline of When Secret Service Personnel Obtained and Shared Threat Information Leading Up to the July 13, 2024, Rally**



Source: GAO review of Secret Service and Intelligence Community information. | GAO-25-108568SU

According to Department of Homeland Security guidance, the need to share actionable, timely, and relevant classified information among federal, state, local, tribal, and private sector partners in support of homeland security is self-evident. To the extent practicable and consistent with governing executive orders and regulations, agencies should prepare information for dissemination to partners at the lowest sensitivity level possible while still retaining the information's value and relevance to the consumer.<sup>51</sup>

<sup>51</sup>Department of Homeland Security, Office of the Chief Security Officer, *Implementing Directive: Classified National Security Information Program for State, Local, Tribal and Private Sector Entities* (Washington, D.C.: Feb. 2012).

---

Further, *Standards for Internal Control in the Federal Government* calls for the agency to design a process that uses the entity's objectives and related risks to identify requirements needed to achieve the objectives and address the risks while considering the expectations of both internal and external users.<sup>52</sup>

When the Secret Service receives highly classified information from its partners, it is common practice to share that classified information with senior executives first.<sup>53</sup> Once officials review the classified intelligence, they can request that personnel within their chain of command be briefed on the specific information with a one-time "read-in" or request a tear line from the Intelligence Community.

Officials within the Office of Strategic Intelligence and Information told us that the Assistant Director of that office at the time of the rally ensured senior officials from OPO were made aware of classified threat information regarding then-former President Donald Trump. Consequently, prior to the rally, senior executives within OPO read classified threat information about then-former President Donald Trump, took steps to ensure the information was shared, and identified mitigation strategies to address related risks. Specifically, OPO officials requested that senior personnel from the Donald Trump Protective Division receive a one-time "read-in." In addition, OPO officials requested that then-former President Donald Trump receive counter sniper assets for all campaign events moving forward. Absent OPO senior executives' use of general threat information to inform its assessment of security needs, then-former President Donald Trump would likely not have received the counter sniper assets that ultimately eliminated the gunman. Consequently, although the threat information was general in nature and not specific to the Butler rally, according to Secret Service officials, the decision to provide an extra layer of protection based on information provided to OPO officials proved to be necessary.

---

<sup>52</sup>Management designs a process that uses the entity's objectives and related risks to identify the information requirements needed to achieve the objectives and address the risks. Information requirements consider the expectations of both internal and external users. [GAO-14-704G](#).

<sup>53</sup>Secret Service has policies for handling and safeguarding information once Secret Service personnel receive it. See, for example Secret Service, Human Resources, *SMD-03(01): Handling and Safeguarding Classified National Security Information and Controlled Unclassified Information (CUI)* (Washington, D.C.: June 2, 2018). Secret Service, Human Resources, *SMD-06: United States Secret Service Operations Security (OPSEC) Program* (Washington, D.C.: May 19, 2023).

According to officials within the Office of Strategic Intelligence and Information, senior officials from the Office of Investigations and the Office of Technical Development and Applied Research were also made aware of classified threat information regarding then-former President Donald Trump. However, there is disagreement within the Secret Service about how the threat information was shared across various Secret Service offices. For example, officials from the Office of Investigations and the Office of Technical Development and Applied Research told us that the senior executives within their offices were not informed that the classified threat information was available to review. According to Secret Service officials, since the prior Office of Strategic Intelligence and Information Assistant Director left the Secret Service, they cannot confirm whether he provided this information to the senior executives. At the time of the rally, Secret Service had no process to document when senior executives were notified of such threat information and when senior executives reviewed such information. Office of Strategic Intelligence and Information officials told us that they now have a documented process to log when senior executives are notified to review classified threat information.

The net effect, however, is that officials from the Office of Investigations—who oversee Secret Service Field Office personnel—and the Office of Technical Development and Applied Research did not make a similar request to have their subordinates receive a similar read-in. As a result, Field Office personnel assigned to the rally and responsible for designing and implementing the site security plan, such as the Pittsburgh Field Office Special Agent in Charge, the lead advance agent, and the protective intelligence advance agent were unaware of classified threat information. Therefore, they did not make additional requests to secure additional resources and assets to protect then-former President Trump to mitigate the threats. Notably, the protective intelligence advance agent's responsibilities include gathering, evaluating, and appropriately disseminating all relevant intelligence information related to the visit and/or protectee.

The site agent for the July 13 rally was from the Donald Trump Protective Division. She stated that she did not receive the threat information. In addition, the lead advance agent reported that she received some general threat information about then-former President Trump from the Donald Trump Protective Division Second Supervisor. However, according to the lead advance agent, the information she received was general in nature and did not outline the specific threat. The lead advance agent did not share the general threat information with all Secret Service advance team



members responsible for securing the rally, such as the Pittsburgh Field Office Special Agent in Charge, site agent, or local law enforcement partners, because she believed the information might have been classified. The Pittsburgh Special Agent in Charge did not receive the threat information. He reported that if he had received the threat information, he would have requested additional assets, such as ballistic glass, additional drone mitigation, and a full counter sniper advance team, among other assets.

Siloed information sharing practices, such as requesting that only personnel within an individual's chain of command be briefed on threat information contributed in part to individuals such as the Pittsburgh Field Office Special Agent in Charge not receiving relevant information. Had Secret Service's threat sharing practice encouraged executives to identify others outside of their chain of command who should be briefed on the information based on their role, key individuals would have received the threat information even if their superiors did not.

Another siloed information sharing practice that inhibited sharing threat information with relevant Secret Service personnel is that threat information received regarding then-former President Trump was considered general and not specific to the Butler, Pennsylvania rally. Secret Service officials noted that it follows procedures for sharing classified threat information regarding when there is an imminent threat-to-life.<sup>54</sup> In these cases, originating agencies are to provide tear line information at a sanitized, lower classification level to share with partners.

In cases where classified threat information is not considered an imminent threat, such as the classified information shared prior to the rally, the Secret Service's information sharing practices are limited to dissemination controls from the originating agency. Secret Service officials we met with told us that they are limited in what and with whom they can share classified threat information.

Regardless of whether the information is considered general or specific to an event or protectee, the Secret Service is able to request that agencies

---

<sup>54</sup>Office of the Director of National Intelligence, *ICD-191: Duty to Warn* (Washington, D.C.: July 21, 2015). Secret Service officials told us that in accordance with *Intelligence Community Directive 191*, when a U.S. intelligence agency learns of an impending threat to an individual's life, the originating agency provides the information to Secret Service with tear lines, at a sanitized, lower-classification level. This allows for the wider dissemination of information while protecting sensitive sources and methods.

providing classified information provide the information with tear lines so that the Secret Service can be informed of what information can be more broadly shared. However, according to Secret Service officials we spoke to, because threat information they received about then-former President Trump was general and not specific to the Butler, Pennsylvania rally, they did not pursue acquiring the information at a lower classification level.<sup>55</sup>

It is common practice for personnel from across the Secret Service to plan for and support security for protected events. It is also common practice for the Secret Service to rely on other federal, state, and local law enforcement officials during protected events. These non-Secret Service law enforcement personnel are often charged with providing important aspects of security. For the July 13 rally, state and local law enforcement personnel planned for and provided perimeter security and snipers to protect the event, among other things.

In particular, state and local law enforcement had significant responsibilities for protecting the area around the AGR International, Inc. building, where the gunman ultimately climbed on a roof and took his shots from. However, the state and local law enforcement officials who helped plan for and execute security for the July 13 rally were not aware of threats to then-former President Trump.

Again, siloed information-sharing practices prevented officials with significant security responsibilities from having access to threat information that could have changed how they secured the area. State and local law enforcement officials we met with told us that had they known of threat information, they would have taken different steps to secure the area.

Maintaining highly classified information security is of the utmost importance. Strict rules must be followed to keep the information from

---

<sup>55</sup>Secret Service officials further told us that if they had received classified information specific to the Butler rally and it did not have tear line information, the Secret Service would have requested tear line information from the Intelligence Community. That information then has to be approved by the Intelligence Community partner and possibly other partners, and ultimately disseminated back to Secret Service. According to Secret Service officials, each agency has its own way of submitting the request. Once submitted, there is no standard time frame for the originating agency to provide the information back to the Secret Service. Secret Service officials told us that there can be great variation on how quickly the information is provided to the Secret Service, and sometimes they receive the information within a few hours, and other times it takes a week. According to Secret Service officials that handle making such requests, the Secret Service has no agreement in place for originating agencies to produce unclassified information when needed.

---

being improperly disclosed. At the same time, successful execution of the Secret Service's protective mission requires that it rely extensively on people from across the agency and external to the agency. Consequently, these individuals and organizations can better support the Secret Service if threat information, or at least relevant information on what to look out for, is shared with them.

To do so, the Secret Service could make policy changes that require its senior executives to proactively share threat information internally with key individuals on a protective advance. For example, senior officials could ask that the protective intelligence advance agent be read-in to the information and use that knowledge when coordinating security between the advance team and state and local officers.

Further, whether informed by general or specific threats to an event or protectee, the Secret Service should identify methods for, as a common practice, sharing potential trends and tactics adversaries may use against a protectee.

Making changes to Secret Service policies to (1) proactively share threat information internally, and (2) establish methods for sharing potential trends and tactics adversaries may use against a protectee with those responsible for designing site security could help ensure Secret Service agents and its partners will have information needed to provide effective protection.

---

**Assets Were Not  
Requested Due to  
Common Practices and  
Unclear Policy**

Secret Service personnel requesting assets were not aware of all assets they could request for the rally because Secret Service policy does not include a readily available, documented list of what assets could be requested. As a result, Secret Service personnel relied on their understanding of what assets were typically provided to protectees based on their status.<sup>56</sup>

Two entities (the House Task Force and Senate HSGAC) investigating the July 13 assassination attempt identified a number of assets that could have been helpful in securing the rally. However, some were not requested because, based on prior experiences and common practices,

---

<sup>56</sup>Two entities (Senate HSGAC and House Task Force) investigating the July 13 assassination attempt also identified these issues. Both entities developed recommendations that addressed request determinations. We discuss these recommendations in greater detail later in this report and in appendix III.

---

members of the Secret Service advance team believed the assets would not be provided for a former President.

The lead advance agent noted that some of the assets she would have requested were typical for a President and not typical for a former President at the time. For example, in her statement before the House Task Force, the lead advance agent stated that she did not request a Counter Surveillance Unit for the rally even though this asset could have helped mitigate the known risk. The site counterpart also noted that she believed this asset could have been helpful, but the lead advance agent told her that this asset was not available for a former President and the lead advance agent assumed that the request would be denied. However, based on our analysis, the Counter Surveillance Unit could have been requested for a former President.

In her statement before the House Task Force, the lead advance agent noted that, based on past precedent, certain assets are requested and approved for certain protectees and sometimes not for others. She said her assessment of what assets to request were based on her experience conducting protection efforts over time. The lead advance agent further noted that certain assets would have been great to have, but requests were not made because it was not typical to have those assets.

Identifying which assets could be requested and would likely be approved was made more difficult by then-former President Trump being a former President who was also close to being officially recognized as a nominee. For example, the lead advance agent told us that the scope of assets requested for then-former President Donald Trump was higher than that of other former Presidents, but not up to the level of what a major Presidential candidate would receive.

However, it was unclear what would be approved. Further, several Secret Service advance team members told us that even when they know they need a resource based on known risks, they are unlikely to make the request if they do not believe the request will be approved.

In addition, the Donald Trump Protective Division Second Supervisor noted in his statement before the House Task Force that he was not aware of policies that documented what assets could be requested for then-former President Donald Trump. Based on our analysis, Secret Service policy does not include a readily available, documented list of assets that could be requested for protected events.

Based on our review of OPO, Donald Trump Protective Division, and Candidate Nominee Operations Section policies, we found that the policies recorded 41 assets that could be employed for protection.<sup>57</sup> Of those assets, as documented across the numerous policies, we found the following could be made available, depending on whether then-former President Trump was considered a former President or an official candidate or nominee for President at the time.

- **Former President.** Thirty of the 41 assets could have been requested for then-former President Donald Trump, as a former President, with six identified as routinely provided. However, according to our analysis, of the remaining 11 assets, two could not be requested since they were designated to be used for the President and Vice President, and existing policy did not identify whether the remaining nine assets could be requested.
- **Candidate or nominee for President.** In addition, as a candidate or nominee for President, the policies identified that 29 of the 41 assets could be requested. Of the 29 assets, eight were identified as routinely provided. However, one of the remaining 12 assets could not have been requested because the asset only supports the President and the Vice President, and existing policy did not identify whether 11 assets could be requested.

In accordance with *Standards for Internal Control in the Federal Government*, management should design control activities to achieve objectives and respond to risks.<sup>58</sup> In addition, management is to use quality information to make informed decisions. Quality information is information that is appropriate, current, complete, accurate, accessible, and provided on a timely basis.<sup>59</sup>

While the advance team and others planning protection for events are responsible for identifying, analyzing, assessing, and mitigating risks, their ability and proclivity to request certain assets may be hampered by

---

<sup>57</sup>The 41 assets we identified are unlikely to be a comprehensive count of all available assets; there may be more assets that could be used that we did not identify in policy. The assets we identified are specific to technological assets and resources available to be requested for certain Secret Service protectees. We selected technological assets and resources relevant to the July 13 rally and protectees with a status of former President, candidate, or nominee.

<sup>58</sup>[GAO-14-704G](#).

<sup>59</sup>[GAO-14-704G](#).

---

common practice and incomplete information on what assets can be requested and would be likely provided. By developing a readily available list that specifies what assets may be requested, along with circumstances under which they are likely to be provided, the Secret Service could better ensure that personnel request needed resources. Moreover, this could provide the Secret Service with greater assurance that asset requests appropriately address security needs for protected events.

---

**Policy Not Structured to Ensure Resource Decisions Are Based on Identified Risks**

The Secret Service did not make all resource and asset allocation decisions for the July 13, 2024, rally based on identified risks.<sup>60</sup> Further, the process, as documented, is not set up to comprehensively consider and make resource allocation decisions based on risk.

DHS Risk Management Fundamentals state that to improve decision-making, leaders in DHS and their partners in the homeland security enterprise must practice foresight and work to understand known and uncertain risks, as best they can, in order to make sound management decisions. These leaders need to consider the risks facing the homeland to make appropriate resource tradeoffs and align management approaches.<sup>61</sup>

In addition, most homeland security measures involve representatives of different organizations, and it is important that there is a unity of effort among those charged with managing risks to ensure consistent approaches are taken and that there is a shared perspective of security challenges. Further, in accordance with *Standards for Internal Control in the Federal Government*, management should design control activities to achieve objectives and respond to risks.<sup>62</sup>

In general, each protective advance team and the protectee's protective detail or division is responsible for identifying assets and resources needed for a protective event. Officials from the OPO Office of Staffing and Logistics, also known as the War Room, told us, for example, that the advance team is responsible for identifying, analyzing, assessing, and

---

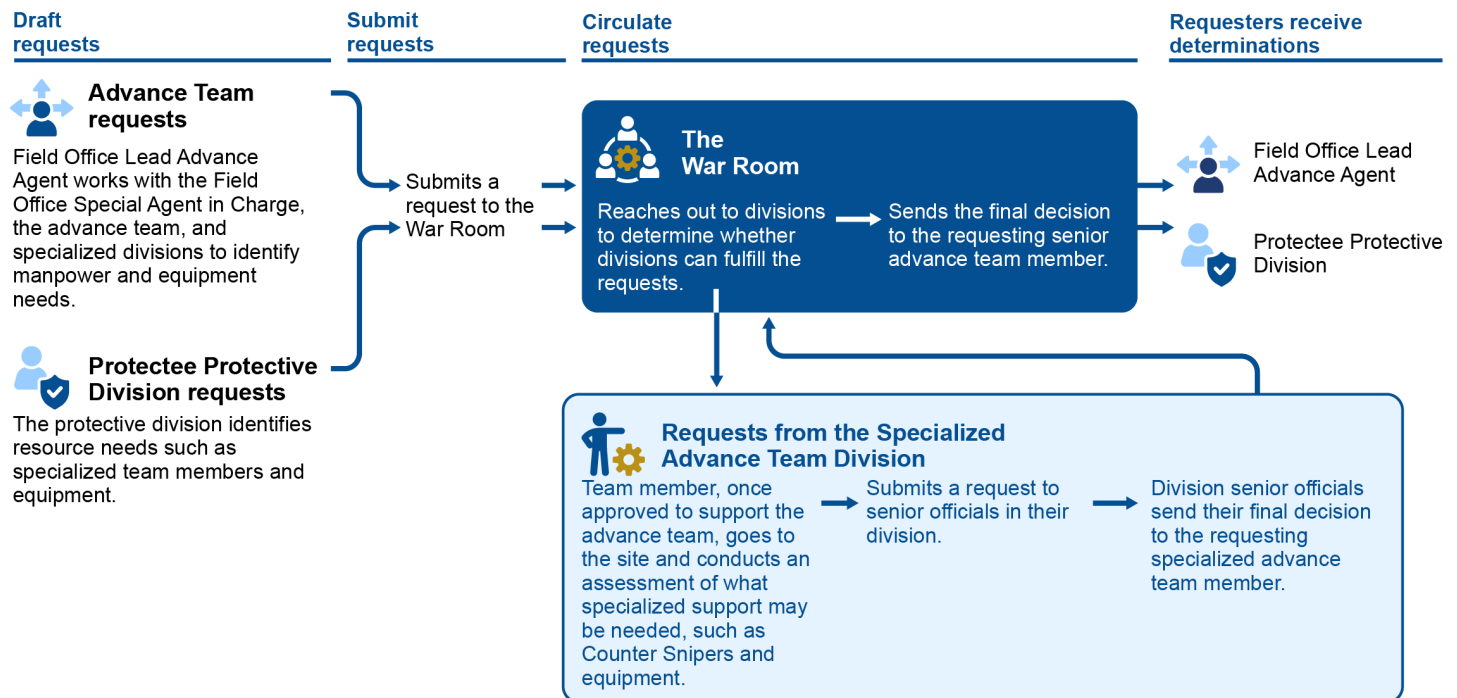
<sup>60</sup>For the purpose of this report, we define "risk" in the resource decision-making process to include threat information that could contribute to security risks at a protected event.

<sup>61</sup>Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*. (Washington, D.C.: Apr. 2011).

<sup>62</sup>[GAO-14-704G](#).

mitigating risks.<sup>63</sup> Based on its assessment, the advance team and the protectee’s detail or division submits asset and resource requests to the War Room. See figure 5 for additional information on this process.

**Figure 5: Secret Service Process for Fulfilling Asset Requests for Protected Events Through the War Room as of July 13, 2024**



Source: GAO analysis of Secret Service July 13 documents; Icons-Studio/stock.adobe.com (illustrations). | GAO-25-108568SU

<sup>63</sup>The “War Room” is comprised of personnel from OPO, Office of Field Operations, Office of Technical Development and Applied Research, Office of the Chief Financial Officer, and Uniformed Division who help facilitate asset requests for Secret Service protected events.



---

Multiple entities within the Secret Service play a role in determining the type and amount of resources provided for a protectee event.<sup>64</sup> These entities include the War Room, senior officials within specialized divisions, and OPO senior officials.<sup>65</sup>

**War Room.** According to War Room officials, the War Room ingests requests and coordinates internally and with other divisions for needed resources. As a matter of practice, internal to the War Room, information on risks is not requested or known unless documented in a manpower request or other document reviewed by the War Room. As a result, War Room decisions on, for example, personnel available to fill posts within and around the site, are primarily based on availability and efficiency assessments.

**Specialized division senior officials.** Coordination on resources by the War Room and other divisions occur, but that too is not necessarily based on known risk. These divisions also make decisions based on factors such as the availability of resources. Based on our analysis, some Secret Service division-level policies require Secret Service divisions to consider available intelligence, risks, and threats related to the protectee or the protected event when resource requests are made.<sup>66</sup>

However, threats and risks, for example, will not necessarily be reported to division officials coordinating with the War Room. Consequently, these divisions may not have access to all known threat and risk information when making their decisions. In addition, while information on risks may be known, decisions on providing specialized assets, such as a full Counter Sniper Advance, are primarily based on availability. There is no requirement, for example,

---

<sup>64</sup>For the purposes of this assessment, an entity can be an individual position, division, office, or component within the Secret Service.

<sup>65</sup>While the process was not documented, a senior OPO official noted that the Office of Staffing and Logistics, referred to as the War Room, is an entity where OPO and Office of Field Operations staff facilitate asset requests. The official noted that the advance team members on the ground responsible for the visit initiate staffing requests, such as identifying the number of post-standers needed for an event, which will be sent to the protective detail operations section. The respective protective detail operations section contacts the War Room, which coordinates specific staffing requests with the respective protective divisions and the Secret Service Field Offices.

<sup>66</sup>For example, the Counter Sniper member of the advance team is to make recommendations and suggest measures to mitigate threats when assessing a site for a protected event, such as blocking vehicles, banners, change to arrival locations, among other recommendations based on a threat assessment. Secret Service, UDS-02(05): Counter Sniper Team Operational Procedures, (June 12, 2023).

---

that resources and assets be allocated among the various protectees based on the relative risks to their event, in addition to other factors.

**OPO senior officials.** Separate from the coordination of requests with the War Room, senior OPO officials may receive risk information on a protectee, and make related decisions based on threats and risks. However, OPO officials noted that when such decisions are made, they do not typically involve the War Room, and they work directly with the division that can provide the asset. Further a senior War Room official noted that this process is not standard and is atypical.

While it is common for various entities within Secret Service to make resource decisions, not all are provided with the known threat and risk information to inform their decisions. Further, the Secret Service's approach to making resource decisions does not require that there be one entity that is comprehensively aware of the known threats and risks, and that it inform resource decisions.

In preparation for the July 13 rally, numerous resource and asset decisions were made. However, resource decisions were not consistently based on risk. Specifically, the War Room and divisions it coordinated with did not consider risks when approving requests, such as requests for enhanced cUAS capabilities and the Counter Assault Team. The Donald Trump Protective Division requested enhanced cUAS equipment for detection and mitigation, since then-former President Donald Trump would be exposed to a large crowd for over 75 minutes and vulnerable to UAS threats.

However, the specialized division personnel from the Technical Security Division did not provide these enhanced cUAS capabilities. A Secret Service division official reported to us that these resources had already been allocated for the Republican and Democratic National Conventions.<sup>67</sup> In addition, the War Room and the divisions it was coordinating with were not privy to threat information associated with then-former President Trump, so the asset was not made available.

---

<sup>67</sup>There is no documentation of the War Room responding to the Donald Trump Protective Division's request. According to a senior War Room official, this is because prior to the July 13 rally, such requests from the Donald Trump Protective Division and Candidate Nominee Operations Section were not consistently documented. However, the official noted that the request and documentation process has since been corrected.

However, senior OPO officials considered risks to then-former President Trump, when they approved counter sniper assets for the July 13 rally. This decision was inconsistent with and separate from War Room practices for making resource decisions.<sup>68</sup> Specifically, prior to the rally, senior OPO officials received a briefing from the Protective Intelligence and Assessment Division, on classified threat information involving a threat related to then-former President Trump and used that information to justify providing counter sniper assets for the July 13 rally. However, this resource allocation decision process was independent from the standard War Room resource allocation process. Specifically, although the Donald Trump Protective Division and the lead advance agent submitted a request to the War Room for counter sniper assets for the July 13 rally, OPO senior officials independently approved counter sniper assets. Senior OPO officials told us that at that time, since senior level OPO officials were privy to, and reviewed classified threat information, they proactively approved counter snipers for the July 13 rally.

Following the rally, in November 2024, the Secret Service developed a policy to document the resource decision-making process for reviewing requests, since no policy was previously in place. According to the new policy, when assessing staffing and resource needs, the War Room will consider the totality of circumstances pertaining to the event and work with the responsible protective division and others to ensure the balance between efficiency and effectiveness. However, if resources are not available, the policy notes that it is the responsibility of the lead advance agent to find other solutions to mitigate the identified risk for which they requested support.<sup>69</sup>

Documenting the resource decision-making process is a step in the right direction. However, we identified several shortfalls regarding how risk is considered by divisions and the lack of details on how the Secret Service will conduct a comprehensive review to determine risks. Lacking such details may hinder the Secret Service from making asset and resource decisions based on comprehensive knowledge of risks to a site or protectee. For example, the new policy does not identify if or how the War

---

<sup>68</sup>We and two entities (House Task Force and Senate HSGAC) investigating the July 13 assassination attempt found that the OPO senior officials, not within the War Room, proactively approved counter sniper assets separate from the July 13 requests.

<sup>69</sup>Secret Service, *OPO-24: Protective Operations Staffing and Logistics* (Washington, D.C.: Nov. 7, 2024).

---

Room or Secret Service divisions will consider information about known risks prior to making resource decisions.

Further, the policy does not identify or require an entity within the Secret Service to receive comprehensive threat and risk information for a site or protectee and use that information to inform, and if needed correct, resource decisions. Lastly, the process for making resource decisions remains decentralized across the Secret Service, with no alternative for ensuring available resources are comprehensively considered and assigned based on identified risks.

Taking steps to provide resource decision-makers with information related to all known risks prior to an event can help ensure Secret Service personnel responsible for securing protectee events have the information needed to effectively secure protectees. Moreover, taking these steps can help ensure asset allocations across the agency are informed by known risk, rather than protectee status, asset availability, or by ad hoc input. By implementing a process that incorporates risk-based decision-making for determining resource allocations, the Secret Service can help ensure security asset decisions are based on need and not based on ad hoc actions outside of a formal process.

---

**Secret Service Did  
not Adhere to Policy  
Governing Counter-  
Unmanned Aircraft  
System Operations  
and Training**

The counter-unmanned aircraft system (cUAS) equipment used by the Donald Trump Protective Division on July 13 did not operate as intended. Importantly, the cUAS was not operational before the gunman flew his drone over the event site. The agent charged with operating the cUAS attempted to fix the issue. However, the agent took hours to correct the issue, as he lacked the training, knowledge, and support to quickly fix the issue and operate the cUAS. Consequently, the Secret Service missed an opportunity to detect the UAS the gunman used to scan the area in advance of the event.

We and three entities (Senate HSGAC, House Task Force, and the DHS Independent Panel) investigating the July 13 assassination attempt found that the Secret Service agent assigned to operate the cUAS did not have the proper training to operate the equipment. Based on our review of available documentation, this occurred because the Secret Service did not adhere to requirements that personnel complete training before undertaking cUAS activities, set forth by the Secret Service for operating cUAS. Secret Service officials told us that no such requirements for the equipment used that day were needed. According to the Secret Service, the cUAS used at the rally did not have the capability to mitigate a UAS system and only had detection capability. Secret

Service officials also said that they do not believe a policy is necessary for operating cUAS equipment used for detection purposes only, and likened it to “turning on a flashlight,” meaning that it is simple to use.

The Secret Service’s stance that it did not have to follow its operator and training requirements to operate the cUAS during the July 13 rally is inconsistent with statute and its policies. Under the statute, authorized actions include detection, identification, monitoring, and tracking of UAS, and seizing and disrupting control of UAS, among other things.<sup>70</sup> The statute further provides that prior to the use for any of these authorized actions, training is to be conducted.<sup>71</sup>

Consistent with this statute, in its policies, Secret Service defines who within the Secret Service is authorized to conduct cUAS actions—which are those actions authorized to detect and mitigate a credible UAS threat—and identifies initial and refresher training requirements.<sup>72</sup> In addition, the Secret Service has a companion concept of operations document that provides additional information on authorized personnel and topics to be included in initial operator training for both cUAS systems.<sup>73</sup> Its current cUAS policies cover requirements, including training and knowledge, for operators of both cUAS systems. Moreover, these policies are consistent with the statute that provides authority for Secret Service to conduct cUAS actions and that is referenced in these policies. In addition, the policies are consistent with the *Standards for Internal Control in the Federal Government*, where management is to establish expectations of competence for key roles to help achieve its objectives to include identifying relevant knowledge, skills, and abilities to be gained from professional experience, training, and certifications.<sup>74</sup> Based on our analysis, Secret Service did not follow its policies in a number of ways.

**Authorized users.** Secret Service policy states that only Secret Service agents, officers and employees who are authorized by the DHS Secretary

---

<sup>70</sup>6 U.S.C. § 124n(b)(1).

<sup>71</sup>6 U.S.C. § 124n(b)(3).

<sup>72</sup>See 6 U.S.C. § 124n(a). United States Secret Service, *Component Policy for Counter-Unmanned Aircraft Systems* (Washington, D.C.: July 26, 2021).

<sup>73</sup>United States Secret Service, *Concept of Operations: Component Counter-Unmanned Aircraft Systems* (Washington, D.C.: July 26, 2021).

<sup>74</sup>[GAO-14-704G](#).

---

and approved by the designated Secret Service authority may operate counter-UAS systems and take counter-UAS authorized actions.<sup>75</sup> Further, the concept of operations document states that Secret Service employees are deemed “authorized personnel” only after they are authorized by the DHS Secretary to conduct cUAS actions and have received appropriate training in a number of topics, including the relevant laws and policies, incident reporting, civil rights and civil liberties, and general operation of cUAS systems.<sup>76</sup>

It is unclear whether the cUAS advance agent was authorized by the DHS Secretary or its designee to operate the cUAS. At the time of the rally, the Office of Technical Development and Applied Research overseeing the deployment of the cUAS equipment to former presidential protective details was not documenting who was responsible for operating cUAS in former presidential protective details, such as the Donald Trump Protective Division. As a result, there was no control in place to ensure agents operating the cUAS were authorized in accordance with stated requirements.

**Initial operator training.** Secret Service policy directs that the Secret Service is to institute operator training and system qualification standards.<sup>77</sup> Further, the concept of operations document states that newly authorized personnel will receive a training manual and accompany cUAS systems operators on a series of training trips.<sup>78</sup> On these training trips, newly authorized personnel must demonstrate working knowledge of DHS and Secret Service policies, technical skill in operating the equipment, and the capacity to make appropriate decisions under stressful conditions.

In deploying the cUAS in 2022, OPO assigned a designated Special Operations Division official to execute training trips to former presidential protective details, such as the Donald Trump Protective Division, to

---

<sup>75</sup>United States Secret Service, *Component Policy for Counter-Unmanned Aircraft Systems* (Washington, D.C.: July 26, 2021).

<sup>76</sup>United States Secret Service, *Concept of Operations: Component Counter-Unmanned Aircraft Systems* (Washington, D.C.: July 26, 2021).

<sup>77</sup>United States Secret Service, *Component Policy for Counter-Unmanned Aircraft Systems* (Washington, D.C.: July 26, 2021).

<sup>78</sup>The concept of operations further requires that the training manual be developed by the Secret Service’s Airspace Security Branch, which was housed within the Office of Technical Development and Applied Research at the time the policy was developed.

---

ensure personnel were trained to operate the equipment. Documentation we reviewed indicates that they conducted a few hours of training in May 2022, including how to set up the system, deployment in the field, and troubleshooting after hours. However, the Special Operations Division did not maintain documentation of who within the Donald Trump Protective Division attended the training. Further, there is no indication that the cUAS advance agent assigned to the July 13 rally participated in the training. The cUAS advance agent told us that he received 1 hour of training from another member of the Donald Trump Protective Division, not a technical expert. He further told us that he did not have the training or expertise to troubleshoot the cUAS equipment during the rally, and in retrospect, did not have enough training to confidently operate the equipment. As a result, there was no control in place to ensure Donald Trump Protective Division personnel operating the equipment received the training required by policy.

**Training handbook.** The Secret Service concept of operations document states that, in addition to participating in training trips, newly authorized personnel are to receive a training manual.<sup>79</sup> However, no manual, as described by the concept of operations document, was developed and shared. Consequently, the Donald Trump Protective Division developed their own handbook for handling and using this equipment, as former presidential divisions were encouraged to do, according to Secret Service officials. Because the handbook was developed without documented training curriculum requirements, the Secret Service lacked effective controls for ensuring the handbook provided comprehensive information on operating the system and deploying it in the field.

**Refresher training.** Secret Service policy states that cUAS training is to include both standard initial training requirements and periodic requalification training requirements.<sup>80</sup> However, the Secret Service has not identified requirements for requalification training, as required by policy. For example, the Secret Service has not defined what requalification training is to entail, a specific time frame for periodic requalification, or records showing that requalification training was

---

<sup>79</sup>United States Secret Service, *Concept of Operations: Component Counter-Unmanned Aircraft Systems* (Washington, D.C.: July 26, 2021).

<sup>80</sup>United States Secret Service, *Component Policy for Counter-Unmanned Aircraft Systems* (Washington, D.C.: July 26, 2021).



---

conducted. As a result, there was no control in place to ensure operators participated in periodic requalification training.

According to Secret Service officials, they believed the efforts they took to train agents in former presidential protection details on cUAS were appropriate. However, challenges and shortfalls experienced in operating the cUAS device prior to the rally suggest more could have been done.

To address the above noted shortfalls and subsequent operational failures that took place during the July 13 rally, in November 2024 the Secret Service established a new division, the Aviation and Air Security Division. According to Secret Service officials, moving forward, this division is to manage all requests for UAS equipment, including cUAS equipment. It is also to ensure all operators complete training requirements and are certified to operate the equipment.<sup>81</sup>

The Secret Service's new Aviation and Air Security Division, as conveyed, could positively address shortfalls that contributed to the cUAS issues on July 13, 2024. However, much remains unknown about how the new division will ensure training and other cUAS requirements are met and expanded on, for example, to provide initial and refresher training. As noted above, additional work is needed to fully convey how training requirements such as refresher training is to be deployed. Further, Secret Service has not documented in policy how the new division is to operate or how it will ensure agents adhere to existing training requirements and operational protocols for using cUAS, or whether they will develop training requirements and operational protocols for the use of detection-only cUAS, including while employing separate mitigation devices. Secret Service officials noted that they plan to finalize policies for the new division by January 2026.

In accordance with *Standards for Internal Control in the Federal Government*, management is to develop and maintain documentation of its internal control system and identify requirements for knowledge, skills, and abilities to be gained from professional experience, training, and certifications.<sup>82</sup> Furthermore, Secret Service should determine whether

---

<sup>81</sup>Secret Service plans to allow non-technical personnel in former presidential divisions to continue operating cUAS equipment, and the Aviation and Air Security Division is in the process of selecting these individuals and inventorying all of the cUAS equipment these details operate.

<sup>82</sup>[GAO-14-704G](#).

---

they should adhere to existing guidance for cUAS operators to receive initial and periodic training or develop guidance outlining such requirements for the use of detection-only cUAS, including while employing separate mitigation devices. As such, documenting in policy (1) initial and periodic refresher training requirements for authorized Secret Service cUAS operators and (2) requirements for how the Secret Service's new Aviation and Air Security Division is to oversee and ensure cUAS use and training policies are adhered to can help ensure new cUAS requirements are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated. Importantly, taking these steps could help ensure cUAS technologies are appropriately deployed and supported during future protectee events.

---

**Secret Service and Its Partners Experienced Cell Phone Service and Bandwidth Issues, and Policy Did Not Require Cellular Assessment at the Site**

Secret Service agents used cell phones to send images of the gunman during the rally since radios do not have this capability. In addition, Secret Service officials noted that department-issued cell phones may be utilized as secondary or back-up communications for radios during a protected event. During the July 13 Trump campaign rally, multiple Secret Service personnel and local law enforcement partners responsible for securing the rally experienced challenges sending and receiving text messages on their cell phone, and some personnel had poor cellular service due to limited cellular bandwidth during the rally. As a result, these personnel did not receive real-time messages and updates on their cell phone while the Secret Service and local law enforcement partners were searching for the gunman.

According to the Secret Service site agent assigned to the rally, her cell phone was working normally on the morning of the rally, but after a few hours, as the crowd size of the rally began to grow, she noticed some of her text messages were not delivered. The site agent said she sent several text messages to the Second Supervisor of the Donald Trump Protective Division and to other agents assigned to the rally, but those messages were not delivered due to poor cellular service. During an interview with members of the House Task Force in October 2024, the site agent also reported that she experienced cell phone reception challenges during the rally.

In addition, one of the Secret Service Counter Snipers assigned to the rally also reported that he experienced challenges receiving messages on his cell phone during the rally. In August 2024, during an interview with the Senate HSGAC team investigating the assassination attempt during the July 13 rally, this counter sniper told Senate HSGAC investigators that

---

his personally owned cell phone—the phone he used to communicate during the rally—“was getting kind of sketchy getting text messages.” According to this Counter Sniper, messages sent to his cell phone were delayed, and at one point during the rally, some of the delayed messages suddenly appeared all at once.

Additionally, one of the Pennsylvania State Police officers we met with, who was also providing security during the rally, told us his cell phone, and the cell phones of some of his troopers were also experiencing connectivity issues. As a result, the officer told us he and his troopers experienced spotty cellular reception at different times throughout the day.

While the radio is the primary means of communication for Secret Service personnel during protective visits, it cannot be used to share images. According to Secret Service personnel we spoke to that were assigned to the rally, Secret Service agents assigned to protectee events, like the July 13 rally, used cell phones as their primary method for sharing images and text messages. Since cell phones play such a vital role for providing agents with the ability to communicate during a protectee event, including providing them with the ability to share real-time photos of persons of interest, it is important that cell phones, and the respective cellular service used by Secret Service personnel assigned to protectee events, are reliable and work effectively.

National Institute of Standards and Technology security guidance encourages agencies, like the Secret Service, to identify essential mission and business functions and associated contingency requirements. This guidance also calls for agencies to conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.<sup>83</sup> Further, *Standards for Internal Control in the Federal Government* emphasize that management should design the entity’s information system and related control activities to achieve objectives and respond to risks.<sup>84</sup>

---

<sup>83</sup>National Institute of Standards and Technology, *NIST Special Publication 800-53, Revision 5*, Security and Privacy Controls for Information Systems and Organizations (Washington, D.C.: Dec. 10, 2020).

<sup>84</sup> [GAO-14-704G](#).

---

Although the Secret Service anticipated hundreds of rally participants on July 13, it did not conduct a capacity or capability assessment in advance of the rally to determine if the existing cellular bandwidth capacity at the location could adequately support the cell phones used by the team of Secret Service agents and local law enforcement partners that day. The Secret Service policy in place at the time stated that the lead advance agent may request Chief Information Officer support through the Detail Operations Center for telephone lines and radio support if the site is unusually large or complex.<sup>85</sup>

This support could entail providing technical troubleshooting assistance or providing backup communication equipment. However, this policy only applies to events involving official presidential candidates or nominees. Leading up to the July 13 rally, the protectee was a former President and, while in some instances, was being treated as a candidate, his nomination was not yet official. Consequently, there was confusion on whether the resource could be requested, and we found no evidence that it was requested.

Further, according to Secret Service personnel we spoke to, leading up to the July 13 rally, there was no requirement to conduct an assessment of cellular bandwidth or cell phone service prior to a protected event for a former President. As such, the Secret Service team assigned to the rally did not conduct cell phone checks to determine whether cell phones would operate properly, or if local cellular bandwidth coverage was adequate for the rally.

To address the challenges noted above, in November 2024 the Secret Service created a new Division, the Operational Communications and Integration Division. According to Secret Service guidance issued in February 2025, the Operational Communications and Integration Division is responsible for establishing capabilities for the Secret Service mission through research, development, and implementation of interoperable communications platforms between federal, state, and local interagency partners.<sup>86</sup>

The Division is also responsible for establishing Secret Service policy to support operational communication mission needs. For example, the

---

<sup>85</sup>Secret Service, *CNOS-03: Communications*, (Washington, D.C.: May 31, 2023).

<sup>86</sup>Secret Service, *OCI-01: Operational Communications and Integration Division Functions* (Washington, D.C: Feb. 11, 2025).

---

Division is to develop, coordinate, and implement interagency coordination for all communications for sites visited by the President, the Vice President, major presidential and vice-presidential candidates, and other Secret Service protectees. It is also to develop communication platforms for all NSSEs not supported by the White House Communications Agency.<sup>87</sup>

The steps taken by the Secret Service to create a new Division to address communication challenges, to include ensuring future protectee events receive adequate cellular bandwidth support, is encouraging. However, to date, the Secret Service has not established a policy that requires agents to conduct a capability assessment to identify potential audio and data communication challenges, along with mitigation measures, prior to all large or complex protectee events. The Secret Service's Operational Communications and Integration Division is a new Division and still in the process of hiring staff to fulfill its mission.

In addition, although the Secret Service created this Division to address communication challenges during protectee events, the Division has not developed concepts-of-operations and other related operational policies that outline how the Division will operate or ensure it will identify potential communication challenges along with mitigating measures prior to events. According to the Division Chief, these policies will not be developed and finalized until early 2026. Achieving the early 2026 date will be difficult, however, as according to the Division Chief, the current federal hiring freeze delayed his ability to move forward with all of his plans to fully staff the Division and accomplish other related objectives. Given observed challenges sending images and text messages during protected events, and the Secret Service's role in providing protectee security on a daily basis, it is imperative that the Secret Service prioritize implementing the policy related to how it will assess audio and data challenges along with mitigating measures prior to events as soon as possible, but certainly before early 2026.

---

<sup>87</sup>The White House Communications Agency provides assured global information services to the President, Vice President, and others as directed, ensuring the White House is able to communicate with anyone, under any condition. The White House Communications Agency is a joint service organization dedicated to providing premier information services and communications support to the President.

---

**Policy Did Not Dictate  
How Changes to the  
Secret Service’s Site  
Security Planning Based  
on Protectee Staff Input  
Should Be Documented  
and Escalated**

While the Secret Service was developing its plan to secure the July 13 rally, according to members of the Secret Service advance team, a Trump campaign staffer asked members of the Secret Service advance team not to use large farm equipment to address line-of-sight concerns near one of the buildings—the AGR building—located near the rally presentation stage.<sup>88</sup> The Secret Service advance team originally planned to use the farm equipment to block line-of-sight vulnerabilities created by the AGR rooftop, but according to members of the Secret Service advance team, the campaign staffer said the equipment would interfere with campaign press photos.

As such, according to Secret Service advance team members, the staffer expressed significant concerns and pressed the Secret Service advance team to develop another solution to address the line-of-sight concerns. Based on input from the staffer, the advance team deviated from its original plan to use the farm equipment, and used other obstacles, such as a jumbotron and a large flag to address the line-of-sight vulnerability.<sup>89</sup>

Members of the Secret Service advance team who participated in the back-and-forth discussion with the staffer about the farm equipment did not share the staffer’s input with senior level Secret Service officials overseeing the rally. Consequently, the Special Agent in Charge of the Pittsburgh Field Office, the Special Agent in Charge of the Trump Protective Detail, and Secret Service leadership within the Office of Protection Operations were unaware the Advance team chose not to use the farm equipment to address the line-of-sight vulnerability based on input from the campaign staffer.

If the Secret Service advance team would have informed someone in a leadership position, Secret Service leadership could have played a role in ensuring a suitable alternative line-of-sight mitigation solution was implemented. At the time of the rally, there were no Secret Service policies or processes in place that required the advance team to

---

<sup>88</sup>During Secret Service site security advances, protectee staff usually participate in site walk-throughs with the Secret Service prior to an event. During these site walk-throughs, protectee staff typically provide input to the Secret Service on site security options and other campaign preferences. Providing input to the Secret Service is not unique to the Trump campaign, or to the July 13, 2024, rally. According to Secret Service personnel we met with, the Secret Service often adjusts site security plans based on input from protectee staff, but nevertheless works to ensure the event is properly secured.

<sup>89</sup>According to members of the Secret Service advance team, Secret Service counter snipers and local law enforcement partners were placed in and around the AGR building to address possible vulnerabilities.

document changes made to Secret Service site security plans, based on recommendations received from non-Secret Service personnel.

The Secret Service cannot definitively determine whether the farm equipment it originally planned to use to address the line-of-sight vulnerability would have completely blocked or prevented the gunman from using the AGR building to carry out his assassination attempt. However, not using the farm equipment possibly created an opportunity for the gunman to use the AGR's elevated rooftop to fire several shots at then-former President Trump and kill and injure other rally participants.

To address this issue and other conflicts that may arise between a Secret Service advance team and a protectee's staff during a site advance, in April 2025, the Secret Service issued a new policy.<sup>90</sup> This new policy adheres to federal government internal control standards by documenting and establishing a formal process for members of a Secret Service advance team to elevate conflicts between its team and a protectee's staff, if the conflict cannot be resolved without elevating the issue.<sup>91</sup> For example, the new policy states:

*“during the entirety of the advance process and ensuing visit, Secret Service personnel will work with their protectee staff counterparts to identify any conflicts between protectee staff requests and protective needs to ensure protective needs are met. Secret Service personnel will work diligently with protectee staff counterparts to resolve conflicts regarding protective needs. In the event Secret Service personnel are not able to reach consensus with their protectee staff counterparts to resolve conflicts involving protective needs, the matter(s) requiring resolution will be elevated through the advance chain-of-command, i.e., through lead or supervisory personnel, and as a last resort, through executive-level personnel. When conflicts with protectee staff counterparts require resolution through the advance chain-of-command, the lead advance agent shall ensure that details pertaining to the conflict and ultimate resolution are appropriately documented, e.g., via email.”*

---

<sup>90</sup>Secret Service, OPO-03(01): Protective Advance Overview (Washington, D.C.: Apr. 10, 2024).

<sup>91</sup>[GAO-14-704G](#).



---

By developing this new policy that requires the Secret Service advance team to evaluate conflicts related to site security decisions, and document the final resolution of these decisions, the Secret Service will increase transparency in developing its site security plan. This policy should also help ensure Secret Service leadership who have site security oversight are aware of possible changes to site security plans and the possible risks created if changes are made based on input from non-Secret Service personnel.

---

## Conclusions

The Secret Service operates under a “zero-fail” protection mission and is responsible for protecting the President, the Vice President, former Presidents, and others. However, due to policy gaps, a failure to effectively share information across the Secret Service and with local law enforcement partners during the July 13, 2024, Trump campaign rally, a gunman evaded the Secret Service and law enforcement and fired shots at then-former President Trump. The gunman injured then-former President Trump and two campaign participants and killed a rally participant in the process.

The three investigative entities that reviewed the actions and failures of the July 13 rally identified a number of challenges that contributed to shortfalls securing the rally. These entities made over 50 total recommendations aimed at improving Secret Service protective operations. The recommendations were constructive and in-line with many of the issues we observed during our review. Since the July 13 rally, the Secret Service has taken steps to address the identified failures and has implemented some of the recommendations. However, our work identified additional shortfalls that played a role in the failures of July 13, and we found that the actions the Secret Service has taken to address the beforementioned recommendations were not sufficient in some cases. As a result, the Secret Service must take additional steps to ensure the operational failures of July 13 are not repeated in the future.

Multiple Secret Service personnel responsible for securing the July 13 rally told us that they did not refer to Secret Service policies prior to the rally because the policies were broad and did not provide specific details regarding roles and responsibilities. Instead, some Secret Service personnel relied on their experience and other agents. Based on our analysis, we determined available policies documenting roles and responsibilities were overly broad. In addition, the policies did not outline all of the key roles, responsibilities, and tasks agents should complete during a protected event.

Additionally, roles and responsibilities that were documented were spread across multiple policies. Since the July 13 rally, the Secret Service has updated several of its policies to include additional detail on the roles and responsibilities for agents assigned to protected events. However, it has not created a readily available resource tool to help agents better understand the key tasks to complete during a protected event. Until the Secret Service takes additional action to ensure agents have such a resource, it continues to risk the possibility of agents failing to implement all necessary security procedures during future protected events.

In addition, prior to the rally, Secret Service personnel and local law enforcement personnel central to securing the rally were unaware of threat information pertaining to then-former President Donald Trump. According to Secret Service officials, this information was not more broadly shared across the Secret Service, partly because the information was highly classified. Further, the Secret Service had no process to share classified threat information with partners when the information was not considered an imminent threat to life. Secret Service protected events require agents to coordinate with multiple Secret Service divisions and local law enforcement partners to ensure the event is adequately secured. As such, it is important that all relevant partners receive relevant threat information in a timely manner. It is vital for the Secret Service to proactively share threat information internally and with local law enforcement partners, including potential trends and tactics adversaries may use. Doing so could help ensure the Secret Service is better prepared to address any known threats during protected events.

Further, the advance team and other Secret Service entities responsible for planning the security for the July 13 rally did not request all available assets to help secure the rally. According to Secret Service personnel we spoke to, some assets were not requested because, based on prior experiences and common Secret Service practices, agents believed the assets would not be provided for a former President. These personnel also were not aware of all the assets that they could have requested because Secret Service policy does not include a readily available, documented list of assets.

Until the Secret Service develops a readily available list that specifies what assets may be requested for protected events, agents may continue missing opportunities to request assets needed to adequately secure future protected events. In addition, Secret Service personnel responsible for making resource decisions for protected events did not consistently make risk-based decisions to determine the type and amount of assets

---

needed. Also, the process, as documented, is not set up to comprehensively consider risks. Providing personnel with such information prior to a protected event can help ensure the Secret Service makes resource decisions based on risks, and not based on ad hoc actions outside of a formal process.

The Secret Service also utilized specialized equipment, such as cUAS, radios, and cell phones to maintain operational awareness and coordination with one another. However, their cell phones and cUAS equipment failed at various times during the rally, and the agent operating the cUAS equipment was not properly trained to use or troubleshoot challenges with the system. Since the July 13 rally, the Secret Service has established multiple divisions (e.g., the Operational Communications and Integration Division and the Aviation and Air Security Division) to address these technology gaps. However, policies that outline how these new divisions will govern cUAS operations and cell phone capability assessments had not been developed as of July 2025. Until the Secret Service develops and finalizes this guidance, it is unclear how the Secret Service will ensure this technology will be effectively deployed during future protected events.

---

## **Recommendations for Executive Action**

We are making eight recommendations to the Secret Service:

The Director of the Secret Service should develop a resource (e.g., a checklist or other readily available quick guide or tool) that provides agents, by role, with readily available information needed to have a clear understanding of the tasks they need to complete to properly secure a protected event. (Recommendation 1)

The Director of the Secret Service should make changes to Secret Service policies to (1) proactively share threat information internally and (2) establish methods for sharing potential trends and tactics adversaries may use against a protectee with those responsible for designing site security. (Recommendation 2)

The Director of the Secret Service should develop a process to ensure actionable threat information is shared with individuals developing the site security plan, including Secret Service stakeholders and law enforcement partners. (Recommendation 3)

The Director of the Secret Service should develop a list of assets that may be requested to secure protectees, along with circumstances under which they are likely to be provided, and ensure the list is readily

---

available to Secret Service personnel responsible for securing protected events. (Recommendation 4)

The Director of the Secret Service should develop and implement a process that manages risks by consistently sharing known risk information when making resource allocation decisions for a protected event. (Recommendation 5)

The Director of the Secret Service should adhere to existing policy or document, in policy, initial and periodic refresher training requirements for authorized Secret Service cUAS operators. (Recommendation 6)

The Director of the Secret Service should document, in policy, requirements for the new Aviation and Air Security Division, including outlining the oversight and internal control mechanisms it will employ to ensure that cUAS use and training policies are adhered to. (Recommendation 7)

The Director of the Secret Service should develop a policy as soon as possible, but before 2026, to require Secret Service personnel to conduct a capability assessment to identify potential audio and data communication challenges along with mitigation measures prior to a large or complex protectee event. (Recommendation 8)

---

## **Agency Comments and Our Evaluation**

We provided a draft of this report to Secret Service and the FBI. In the draft report, we made eight recommendations to the Secret Service. DHS concurred with all eight recommendations and reported actions the Secret Service plans to take to implement them. DHS provided a comment letter which is reproduced in appendix V. Secret Service and the FBI provided technical comments, which we incorporated, as appropriate.

Regarding our first recommendation, DHS reported that Secret Service will conduct a review to determine the appropriate resource, such as but not limited to a checklist, quick guide, or similar tool, to provide agents with readily available information needed to have a clear understanding of the tasks they must complete to secure a protected event. Once complete, the Secret Service plans to promulgate this resource, as appropriate, to agents and partners. The Secret Service will also consider how best to make this tool readily available from issued equipment (e.g. smart phone or computer). We agree that these are positive steps and look forward to evaluating Secret Service's actions when completed.

In response to our second and third recommendations, DHS reported that Secret Service's Office of Strategic Intelligence and Information initiated a comprehensive policy review to ensure guidance is updated as appropriate to reflect new procedures to document threat reporting notifications. DHS further noted that the Secret Service is limited in its ability to broadly distribute classified information by classification controls and other constraints by the U.S. Intelligence Community. We recognize the unique challenges Secret Service faces when securing its protectees. However, the shortfalls we identified were structural, at times focused on sharing information using a self-imposed chain-of-command approach rather than the need to know. Given its zero-fail mission, ensuring key decision-makers responsible for developing and implementing security plans are provided with fulsome information is vital to its success. We look forward to evaluating the additional changes Secret Service proposes for breaking down existing siloed information sharing practices and ensuring key decision-makers are provided with complete and actionable information.

Regarding our fourth recommendation, DHS reported that Secret Service's Office of Protective Operations will develop a list of assets that may be requested to secure protectees, as well as guidance on the circumstances under which these assets are likely to be provided. It plans to further share this list with personnel responsible for securing protected events. We believe this is a positive step that can help those with protective responsibilities have a consistent understanding of assets that can be deployed.

In response to our fifth recommendation, DHS reported that Secret Service's Office of Protective Operations will develop and implement a process that manages risks by consistently sharing known risk information when making resource allocation decisions for a protected event. As previously noted, in November 2024, the Secret Service developed a policy to document the resource decision-making process for reviewing requests, since no policy was previously in place. This was a step in the right direction. Taking steps to inform resource decision-makers of all known risks, especially those deciding whether to allocate a resource to a particular event or protectee, can help ensure appropriate tradeoffs are made when allocating resources among protectees. We look forward to evaluating Secret Service's actions when completed.

Regarding recommendations six and seven, DHS reported that Secret Service would take steps to document cUAS training requirements for authorized Secret Service cUAS operators, as well as guidance on the

---

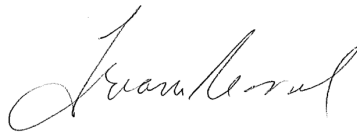
oversight and internal control mechanisms that will be employed to ensure that cUAS personnel are in compliance with use and training policies. We look forward to reviewing Secret Service's new training and guidance when developed.

In response to recommendation eight, DHS conveyed that Secret Service would initiate a review to determine how best to establish a requirement that Secret Service personnel conduct a capability assessment to identify potential audio and data communication challenges, as well as mitigation measures prior to a large or complex protectee event. It intends to complete this assessment and develop a policy, or other guidance as appropriate, by December 31, 2025. We agree that these are positive steps and look forward to evaluating Secret Service's actions when completed.

---

As agreed with your office, we plan no further distribution of this report until 30 days from the report date. At that time, and because of the sensitive nature of the information contained in this product, we are only providing copies to the appropriate congressional committees with a need-to-know, and the Attorney General, the Secretary of the Department of Homeland Security, and the Director of the Secret Service. On request, this product will also be made available to others with the appropriate need-to-know.

If you or your staff have any questions about this report, please contact me at [mcneilt@gao.gov](mailto:mcneilt@gao.gov). GAO staff who made key contributions to this report are listed in appendix VI.



Sincerely,  
Triana McNeil  
Director, Homeland Security and Justice

# Appendix I: Objective, Scope, and Methodology

---

This report examines the extent to which gaps and noncompliance with Secret Service policy may have contributed to security failures on July 13, 2024. To do so, we analyzed Secret Service policies for securing protected events, including protected events occurring during a presidential campaign, and compared these policies to actions taken on and leading up to July 13, 2024.<sup>1</sup>

Our analysis is based on policies Secret Service personnel, including those at Secret Service Headquarters, the Pittsburgh Field Office, the Donald Trump Protective Division, and others that supported the event identified for securing protected events. Specifically, Secret Service personnel identified formal policies, informal documents, and templates agents utilize when preparing for protected events. We also had Secret Service officials with responsibilities over the identified protective duties confirm that our list of policies for securing protected events leading up to and on July 13, 2024, were complete and accurate.<sup>2</sup>

In addition, we met with officials and personnel across the Secret Service to gain a factual understanding of what occurred leading up to and on July 13, 2024. This provided us with insights into firsthand accounts of what various personnel experienced in planning for and executing security measures for the rally. It also provided us with an understanding of subsequent retrospective views and assessments of what transpired.

In addition, we interviewed officials from third-party entities at the federal, state, and local levels of government that supported the event, and we visited the site of the July 13, 2024, assassination attempt to better understand the challenges in securing the site. Further detail on the steps we took are described below.

---

<sup>1</sup>For the purpose of this report, a “protected event” refers to an event where the Secret Service is responsible for providing protection for a protectee, such as a former President, but excludes National Special Security Events (NSSE). We excluded NSSEs from our review of Secret Service policies for securing protected events. Policies we reviewed included Secret Service, *OPO-03: Protective Advance – Overview* (Washington, D.C.: Mar. 11, 2024); *OPO-04: Protective Advance Guidelines* (Washington, D.C.: June 20, 2023); and *OPO-06: Site Security* (Washington, D.C.: May 10, 2022).

<sup>2</sup>We also compared policies for protecting then-former President Donald Trump to other former president protective division policies to determine, how if at all, Donald Trump Protective Division policies differed. We reviewed policies from the following former president protective divisions: Carter Protective Division, George Bush Protective Division, Obama Protective Division, and the Bill Clinton Protective Division.



Appendix I: Objective, Scope, and  
Methodology

---

## Roles and Responsibilities

To determine the extent to which Secret Service personnel responsible for securing the July 13 rally followed established policies given assigned roles and responsibilities, we first identified policies in place prior to the rally. We assessed these policies to identify the extent to which roles and responsibilities were defined. We then proceeded to interview personnel from across the Secret Service with responsibilities for executing key responsibilities for the rally. Our interviews with these individuals focused in part on understanding what they believed to be their roles and responsibilities for the July 13 rally and understanding what experience and resources were available to them for executing their roles. We interviewed key officials from the following:

- **The Pittsburgh Field Office**, which the Secret Service identified as the lead for securing the site. This included meetings with the Pittsburgh Special Agent in Charge, who leads the Pittsburgh office; the lead advance agent, who had responsibility for overseeing much of the security planning and coordinating for resources internal and external to the Secret Service; and the site counterpart agent, who primarily supported the site agent and lead advance agent in efforts to plan security for the rally and help ensure security measures were in place on the day of the rally.
- **The Donald Trump Protective Division**, which provided the site agent that had day-to-day responsibility for defining site security and coordinating with the Donald Trump campaign staff on security matters, among other things. This also included the Donald Trump Protective Division Second Supervisor, who supervised security planning for the July 13 rally on behalf of the Donald Trump Protective Division, and the counter unmanned aircraft system (cUAS) advance agent, who operated the cUAS on the day of the rally.

We also met with additional Secret Service personnel who had operational responsibilities at the site on the day of the rally. For instance, we met with the security room agent, who had responsibility for managing communications from the Secret Service security room; the site protective intelligence agent, who served as the counterpart to the protective intelligence advance agent during the July 13 rally; the Technical Security Division Coordinator, who provided technical assets and

**Appendix I: Objective, Scope, and  
Methodology**

---

countermeasures to enhance site security; and the Secret Service counter snipers assigned to the rally.<sup>3</sup>

To further inform our assessment of whether established policies were followed given assigned roles and responsibilities, we reviewed available documentation and sought information from third-party sources that observed and contributed to securing the rally, such as other federal entities and state and local officials that supported the rally. Documentation we reviewed included the security plans developed by both Secret Service officials and state and local law enforcement. We further reviewed communication records including over 1,000 emails, over 4,000 text messages, body camera footage, over 60 radio logs, and other documents such as site diagrams and surveys that provide insight into the actions taken by Secret Service and local law enforcement officials leading up to and during the rally. We also reviewed records of resources available to Secret Service agents, such as training guides and resource guides called “go bys” that could be used by Secret Service agents to inform how they perform their roles and responsibilities when securing an event. In addition, we reviewed the sworn testimony of Secret Service personnel provided in support of congressional and internal investigations into the July 13, 2024, assassination attempt.<sup>4</sup>

Additionally, we met with third party sources that observed and contributed to securing the rally. For example, we met with Department of Homeland Security (DHS) officials to learn how Homeland Security Investigations agents were trained and supported the rally. We also met with state and local law enforcement officials to understand how they

---

<sup>3</sup>We did not speak to the protective intelligence advance agent or the counter assault team advance agent, because both individuals separated from Secret Service after the July 13, 2024, rally. We obtained their contact information and attempted to make contact but deemed the efforts unsuccessful after multiple attempts with no response.

<sup>4</sup>We reviewed sworn testimony conducted by two congressional entities investigating the July 13 assassination attempt. United States Senate Committee on Homeland Security and Governmental Affairs, *Interim Joint Report: Examination of U.S. Secret Service Planning and Security Failures Related to the July 13, 2024, Assassination Attempt*, (Washington, D.C.: Sept. 2024). United States House of Representatives, *Task Force on the Attempted Assassination of Donald J. Trump: Final Report of Findings and Recommendations*, (Washington, D.C.: Dec. 5, 2024). We also reviewed congressional testimony of other officials, including state and local law enforcement, Secret Service, and FBI officials. We also reviewed sworn testimony provided in support of the Secret Service Mission Assurance Report.

Appendix I: Objective, Scope, and  
Methodology

---

planned for and coordinated their efforts with Secret Service personnel.<sup>5</sup> For instance, during our discussions with state and local law enforcement officials assigned to the rally, officials explained the process used by the Secret Service to designate post assignments. Officials also described the interaction and coordination the Secret Service advance team had with non-law enforcement personnel, such as site venue and Donald Trump campaign staff while site security options were being considered. We also discussed the process used by the Secret Service to equip and staff the security room. The information from these sources helped inform, and in some cases corroborate, our assessment.

Using the information gathered through the above noted sources, we compared actions taken to secure the July 13, 2024, rally against roles and responsibilities as defined in Secret Service policies leading up to the event. We further compared Secret Service policies, including policies updated after the rally, to our *Standards for Internal Control in the Federal Government* and *Leading Practices for Interagency Collaboration* to determine whether the Secret Service's previous and updated policies addressed selected leading practices for interagency collaboration.<sup>6</sup>

---

## Threats and Intelligence

To determine whether there were gaps and noncompliance in the Secret Service's process for sharing threat and intelligence information, we reviewed Secret Service policies for sharing such information. We also interviewed personnel from the Federal Bureau of Investigation (FBI) and Secret Service's Office of Strategic Intelligence and Information, and the Donald Trump Protective Division. In addition, we met with the lead advance agent, the site agent, and multiple state and local law enforcement partners assigned to the rally to determine the extent to which Secret Service personnel shared threat-related information with members of the advance team and other law enforcement partners leading up to the rally. To determine what information was shared, we

---

<sup>5</sup>We met with state and local law enforcement leadership at the July 13 rally in-person in Butler, Pennsylvania, including officials from Butler County, Butler Township, Butler Emergency Services Unit, and Pennsylvania State Police. We conducted a phone interview with a senior Beaver County official. We also contacted an official from Washington County; however, they declined to meet with us due to ongoing litigation.

<sup>6</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014). GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, [GAO-23-105520](#) (Washington, D.C.: May 24, 2023). Using the list of leading interagency collaboration practices found in [GAO-23-105520](#), we selected the practices most relevant and applicable to the actions and processes used by the Secret Service to prepare for the July 13, 2024, campaign rally.

**Appendix I: Objective, Scope, and  
Methodology**

---

reviewed email communications that corroborated phone calls between the Secret Service and Intelligence Community officials. We also met with the Secret Service and Intelligence Community officials that received classified threat information prior to the rally. This information helped inform our determination of how, and to what extent, threat information was shared. In addition, we reviewed open-source threat assessments, trip reports, and other site security documentation developed by the Secret Service and the Western Pennsylvania Fusion Center, as well as open-source posts of interest shared by the Western Pennsylvania Fusion Center and Butler Emergency Services. Further, we reviewed classified information provided by the Secret Service and the Intelligence Community. We reviewed these documents to determine what threat information, if any, informed the Secret Service's security planning for the rally.

---

**Resources and  
Technology**

To determine how the Secret Service makes resource decisions for protected events, and whether these decisions are risk-based, we reviewed Secret Service policies in place at the time of the July 13, 2024, rally and recently updated policies. To identify whether there were gaps and noncompliance in Secret Service's resource decision-making process, we reviewed Secret Service Office of Protective Operations (OPO) and division-level policies that documented this decision-making process. We reviewed these policies to determine whether the Secret Service requires personnel responsible for resource decision-making to use a risk-based approach when determining what assets to approve and provide for a protected event. We also reviewed the policies to understand what threat and risk information should be shared with resource decision-makers.

In addition, we met with officials from the OPO Office of Staffing and Logistics, also known as the War Room—an entity that includes senior officials within OPO and the Field Office that facilitates resource decision-making for protected events. We compared Secret Service resource decision-making policies to *DHS Risk Management Fundamentals* to determine the extent to which Secret Service's policies were consistent with DHS's policies for risk-based decision-making.<sup>7</sup> Additionally, we interviewed other senior OPO officials that can make unilateral resource

---

<sup>7</sup>Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, D.C.: Apr. 2011).

**Appendix I: Objective, Scope, and  
Methodology**

---

decisions to determine whether those officials consider identified risk when making resource decisions.

We further determined the extent to which Secret Service policies identified nontechnological and technological assets that are to be used during protected events by reviewing Secret Service policies for former Presidents, candidates, and nominees.<sup>8</sup> We compared assets identified in Secret Service policy that could be requested by the advance team for protected events to assets used. To determine what specialized technology the Secret Service used to maintain operational awareness and coordination during the rally, we reviewed documented requests and approvals for nontechnological and technological assets for the July 13 rally. We further used equipment usage reports maintained by the Secret Service to identify what assets were utilized during the rally. In addition, to corroborate information on what assets were requested, approved, and used for the rally, and whether technologies were used in accordance with Secret Service policy, we interviewed key Secret Service personnel from the Secret Service advance team, Donald Trump Protective Division, Technical Security Division, Operational Communications and Integration Division, Office of Training, OPO, and Office of Staffing and Logistics.

Further, to assess whether Secret Service technologies used during the rally were acquired in accordance with Secret Service policy and operated as intended, we reviewed applicable policies and requirements for operating technology such as radios, cell phones, and the cUAS used by the Secret Service during the rally.<sup>9</sup> We also reviewed updated policies developed by the Secret Service since the July 13 rally aimed at addressing policy gaps that contributed to security failures that day. Further, we met with Secret Service officials to discuss actions taken since the rally to address security shortfalls, including steps taken by the Secret Service to establish new Secret Service divisions and plans for acquiring and obtaining additional personnel, technology and equipment.

---

<sup>8</sup>For the purpose of this report, “nontechnological assets” refer to Secret Service personnel that either comprise the advance team or are deployed from a specialized Secret Service division to support protective operations for the advance. We refer to equipment as “technological assets.” NSSEs were excluded from the scope of our review and were therefore excluded from our assessment of assets that could be provided.

<sup>9</sup>Our review of cell phone and bandwidth assessment policies considered National Institute of Standards and Technology guidance. See, for example National Institute of Standards and Technology, *NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations* (Washington, D.C.: Dec. 10, 2020).

**Appendix I: Objective, Scope, and  
Methodology**

---

We conducted this performance audit from August 2024 to July 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: National Special Security Events and Special Event Assessment Rating Events

---

The Secret Service serves as the lead agency responsible for securing certain special events, as designated by the Secretary of Homeland Security, including National Special Security Events (NSSE).<sup>1</sup> Further, the Department of Homeland Security (DHS) and other federal agencies coordinate with state and local entities to determine security operations for Special Event Assessment Rating (SEAR) events.<sup>2</sup>

## **National Special Security Event (NSSE) Designation Factors**

According to Department of Homeland Security (DHS) policy, multiple factors are considered when recommending whether a NSSE designation is appropriate, including the

- anticipated attendance by U.S. officials and foreign dignitaries,
- size of the event, and
- significance of the event.

## **Special Event Assessment Rating (SEAR) Risk Score Factors**

A SEAR risk score is assigned for each event submission using an applied methodology that considers multiple factors, including the

- threat,
- vulnerability, and
- consequence.

Source: GAO analysis of DHS documentation. | GAO-25-108568SU

Generally, NSSEs are designated if they warrant the full protective, incident management, and counterterrorism capabilities of the federal government, given the potential for the event to be a target for foreign or domestic terrorists. The NSSE Working Group—which is co-chaired by the Secret Service, the Federal Bureau of Investigation (FBI), and Federal Emergency Management Agency—assists the Secretary of Homeland Security in the designation process. The Secretary may designate major federal government, or public events considered nationally significant as NSSEs. Examples of NSSEs include the Democratic and Republican National Conventions, the Presidential Inauguration, United Nations General Assembly, and the State of the Union address.<sup>3</sup>

A SEAR event is a special event that is typically preplanned by a state or local jurisdiction or a private entity but is not designated as an NSSE. State and local entities will typically submit their event for a SEAR rating to the Special Events Working Group, which comprises over 60 agencies including the FBI, DHS, and National Counterterrorism Center where they will assign a SEAR level for that event.<sup>4</sup> SEAR events are rated one through five. A Level 1 SEAR event is an event of national or international importance which requires extensive federal agency support, while a Level 5 SEAR event generally may only have state importance and receive local level support.<sup>5</sup> Examples of SEARs include the Super Bowl, the funeral of Supreme Court Justice Ruth Bader Ginsburg, and the National Cherry Blossom Festival.

---

<sup>1</sup>18 U.S.C. § 3056(e)(1).

<sup>2</sup>The rally held on July 13, 2024, in Butler, Pennsylvania was not considered a NSSE or a SEAR event.

<sup>3</sup>GAO, *Capital Attack: Special Event Designations Could Have Been Requested for January 6, 2021, but Not All DHS Guidance Is Clear*, [GAO-21-105255](#) (Washington, D.C.: Aug. 9, 2021).

<sup>4</sup>[GAO-21-105255](#).

<sup>5</sup>[GAO-21-105255](#).



# Appendix III: Recommendations Made to the Secret Service in 2024 and 2025 by Other Congressional Investigative Committees

In 2024, the Senate Committee on Homeland Security and Governmental Affairs, a Department of Homeland Security Independent Review Panel, and a House Task Force all issued reports that examined the Secret Service's planning and security failures leading up to and during the July 13, 2024, Trump rally. Each report provided key recommendations to help ensure the failures of the July 13 rally are not repeated in the future. Tables 3, 4, and 5 provide the recommendations included each report, respectively.

**Table 3: Recommendations Included in Senate Homeland Security and Governmental Affairs Report**

Recommendation	Description of recommendation	Due date
1. Planning and coordination	<p>Congress should require Secret Service to identify defined roles and responsibilities for Secret Service personnel responsible for advance planning of any protective event.</p> <ul style="list-style-type: none"> <li>For all protective events, the Secret Service should improve coordination and specify roles and responsibilities between and among federal, state, and local law enforcement partners.</li> <li>Secret Service policies and protocols should require advance planning leads to request and review state and local operational plans in advance of any protective event to ensure a shared understanding of security responsibilities and vulnerabilities as well as other critical planning and security components</li> </ul>	None
2. Responsibility	In advance of each protective event, Secret Service should designate a single individual responsible for approving all plans, including the responsibility for approving security perimeters.	None
3. Communications	<p>The Department of Homeland Security (DHS) and Secret Service should ensure communications plans between federal, state, and local law enforcement agencies and first responders are properly executed and should ensure records retention capabilities.</p> <ul style="list-style-type: none"> <li>Congress should require that Secret Service record its radio transmissions at all protective events.</li> <li>Congress should require DHS and Secret Service to evaluate the steps it needs to take to ensure communication plans with state and local partners are fully executed when conducting law enforcement and/or first response activities at a given location.</li> <li>Congress should require that DHS and Secret Service report to Congress any steps taken to remedy past failures to execute communications plans and to ensure compliance with those plans in the future.</li> </ul>	None
4. Intelligence	Secret Service should consider sending additional assets, including counter snipers, to all future outdoor protective events as it evaluates intelligence and threats against protectees. Secret Service should also ensure that the appropriate agents working protective events are informed of relevant intelligence and threats against protectees.	None
5. Resources	<p>Congress should evaluate Secret Service budget and resources. Security requirements should be determined depending on various threat levels, ranging from less severe threat environments to the highest level of security at National Special Security Events.</p> <ul style="list-style-type: none"> <li>Congress should require that Secret Service allocate assets and resources based on the threat level, not the position or title of the protectee.</li> </ul>	None

Source: U.S. Senate Committee on Homeland Security and Governmental Affairs. | GAO-25-108568SU

Note: information is from U.S. Senate, Committee on Homeland Security and Governmental Affairs, Examination of Secret Service Planning and Security Failures Related to July 13, 2024 Assassination Attempt (Washington, D.C.: Sept. 2024).

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

**Table 4: Recommendations Included in DHS Report of the Independent Review Panel**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
1. Physically integrated communications and incident tracking setup	For all large events, the Secret Service shall ensure that one or more representatives from the Secret Service, each state law enforcement agency operating at the event, and each local law enforcement agency operating at the event are physically collocated with one another in the space which is serving as the central communications hub for the event, for the purpose of facilitating centralized communications. Any exception to this policy shall require the approval of a Deputy Assistant Director or person of higher rank within the Office of Protective Operations or of the Director of the Secret Service. In addition, for all large events, the Secret Service shall ensure that the space that is serving as the central communications hub for the event is making use of a unified electronic incident command system (a real-time incident command management system) for the centralized reporting and tracking of events and issues that arise at the site.	None
2. Mandatory situation report at the time of the protectee's arrival	The Secret Service shall implement a required policy whereby, upon the protectee's arrival at a site, the lead site agent shall provide the head of the protectee's detail (or whichever other agent is serving in that role for purposes of the site visit and traveling with the protectee) with a concise, face-to-face, verbal situation report for the site, to include any outstanding suspicious persons issues and other relevant site security details. It is expected that, in anticipation of the protectee's arrival, to fulfill this policy, the lead site agent shall gather up-to-date site security situational information in coordination with the agent assigned to lead communications in the Security Room to ensure that the report provided is thorough, timely, and accurate.	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

Recommendation	Description of recommendation	Due date
3. Overhead surveillance for outdoor events	<p>For all outdoor events involving candidates, nominees, and former Presidents, the Secret Service shall operate some form of technology-based overhead surveillance, including but not limited to drone-based surveillance or overhead video-based surveillance, to provide the Secret Service with improved site overwatch. The technology-based overhead surveillance system shall be operated by Secret Service agents or other personnel who have received formal training in the operation of the system and have been assessed, and then periodically reassessed, for demonstrated competency in the maintenance and operation of the given system. The feed(s) from the technology-based overhead surveillance shall be directed into the space which is serving as the central communications hub for the event.</p> <p>Additional Commentary: This remediation begins with basic, general technologies to provide the Secret Service with flexibility in its implementation, including overhead drone surveillance (tethered or untethered) and overhead video surveillance. The Secret Service should assess and consider other, more sophisticated options as well, including implementations of those two basic technologies that integrate AI-assisted (including machine learning) threat detection. Which level of technology is deployed should ultimately be based on the perceived potential threat level at the site.</p> <p>The Panel has heard some personnel describe the historical perspective in the Secret Service that operating both unmanned aircraft systems (UAS) and counter UAS (cUAS) simultaneously is overly technologically challenging; therefore, the Secret Service favors cUAS. The Panel believes this is likely an outdated view—even currently, much less in the future, as these technologies evolve—and that it is technologically feasible to intermix both systems. However, in the event of an intransigent interoperability conflict between cUAS and UAS at a site, the Secret Service will have the option to rely on video-based overhead surveillance instead of UAS.</p> <p>Agents must receive sufficient cUAS / UAS training, and the requisite equipment needs to be tested regularly, including in the day(s) before an outdoor event. cUAS and UAS technology is important and helpful, and Secret Service agents can—and can fairly be expected to—become experts in its use. To the extent sufficient hardware is unavailable, this is a suitable budget priority, and the technology can be sourced from vetted American manufacturers. None of this needs to be invented anew by the Secret Service; rather, focused training and deployment will complete the reform.</p> <p>More generally, the Panel emphasizes the criticality of the Secret Service intelligently integrating available technologies, including off-the-shelf options, into its protective methodologies. The Panel believes strongly that the Secret Service must increase its efforts in this regard to achieve its protective objectives.</p>	None
4. Explicit description of line-of-sight risk mitigations	<p>The Secret Service shall require that all Secret Service site security plans include a specific description of the method(s) of mitigation for each location at the site within 1,000 yards of the intended primary position of the protectee presenting line of sight risk, regardless of whether the given risk is within a particular perimeter; the method(s) of mitigation shall be specified on a location-by-location basis within the site security plan.</p>	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
5. Training on threat identification, speak up, information transparency, communications, and ownership (Training I)	Training shall be provided to all agents across the Secret Service regarding risk-based threat identification and the criticality of "Speak Up," information transparency, and appropriate communications protocols, to be completed by end of year 2025. The training can be conducted through local field offices and detail locations as appropriate, and a train the trainer approach can be employed if desired, but the baseline materials and content of the course shall be standardized for all agents. Scenario-based training can be used. The training shall also be integrated into the Secret Service's standard training curriculum going forward. Reinforcement training on these same issues shall be provided to all agents across the Secret Service by end of year 2027. In addition, a separate submodule of the training shall be provided to all personnel at or above the General Schedule (GS)-13 pay scale, all Assistants to the Special Agent in Charge, all Assistant Special Agents in Charge, all Special Agents in Charge, and equivalent senior-level personnel, emphasizing the importance of ownership of site preparation and security responsibilities by such personnel. The training shall be completed by end of year 2025. The training shall also be integrated into the Secret Service's standard training curriculum going forward. And reinforcement training shall be provided to all applicable personnel across the Secret Service by end of year 2027.	December 31, 2025 December 31, 2027
6. Revisions to written policies concerning advance and site responsibility and training related thereto (Training II)	Applicable Secret Service written policies concerning (a) site advance planning, and (b) site security on the day-of events shall be revised to further stress overall responsibility for site advance planning and site security consistent with an Incident Command System / Unified Command approach, including in more complex scenarios such as those involving detail agents (not from the presidential protection division) interacting with agents from a local field office. Regarding site advance planning, the revised policy should clearly identify the single individual with overall command authority for the site advance planning, identify individuals with subsidiary command authority regarding specific components of site advance planning as appropriate, and include a detailed chain of command and process for interactions between field office, detail, and other Secret Service personnel concerning site advance planning. The revisions shall also describe how this chain of command should interact with other federal, state, and local elements on the day of the event. Regarding site security on the day-of events, the revised policies should identify the single individual with overall command authority for an event, identify individuals with subsidiary command authority regarding specific components of site security as appropriate, and include a detailed chain of command and processes for interactions between field office, detail, and other Secret Service personnel present at the event. The revisions shall also describe how this chain of command should interact with other federal, state, and local elements on the day of the event. Upon completion of the policy revisions, a formal communication shall be broadcast to all Secret Service personnel highlighting the revisions. Finally, by June 30, 2025, all Secret Service personnel shall receive training regarding the revised policies.	June 30, 2025

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
7. Changes to better integrate state and local elements	<p>The following remediations are directed toward better integrating state and local elements in the development and execution of site security plans and toward achieving a more systematic approach for Secret Service/State-Local interactions at the field office level.</p> <p>(a) The advance planning process shall be revised so that the lead site agent must receive an operational plan or plans from involved state and local enforcement agencies setting out the roles and posts for all state and local law enforcement elements involved in the event, regardless of their location within or outside the event inner perimeter. The lead site agent also must hold a coordination meeting encompassing representatives from all state and local assets intended to be present at the event to address any questions and resolve any open issues. Finally, the lead site agent must integrate the state and local operational plans into the final site security plan, which shall then be reviewed and approved consistent with Service procedure.</p> <p>Additional Commentary: It is not enough that state and local entities generally participate in the advance planning work in the run-up to an event. Rather, the Secret Service must specifically understand each entity's operational plan in light of the Secret Service's own plan so that a cohesive security vision is achieved and then vetted and approved. This is critically important given the vital role that state and local assets play in maintaining the integrity of event sites, particularly for large events like Butler.</p> <p>(b) The field offices shall achieve a working understanding of the resources and capabilities of the state and local enforcement agencies they may rely on to support protective missions. This understanding should not be developed just in the days prior to a protective event but rather should be a point of continuous knowledge within the field office, periodically refreshed, to facilitate better planning. To achieve this end, it is appropriate to employ a checklist, survey, or similar, standardized method of information gathering, with information to be provided by state and local partners and then periodically refreshed.</p> <p>(c) The Secret Service shall develop a State and Local Field Handbook, to be distributed by the field offices to all state and local partners, which provides information regarding protective operations and sets out Secret Service expectations in terms of capabilities of state and local partners. This Field Handbook shall be periodically refreshed.</p>	None
8. Implementation of experience-based policies for the selection of site and advance agents within details and field offices	<p>The Secret Service shall require all agents assigned to former, candidate, and nominee details, along with all field offices, to adopt a policy requiring the use of experience-based selection methods for the selection of site and advance agents. The policy shall also require the agent(s) selected for any given event to be approved by the Special Agent in Charge of the detail or field office or their functional equivalent.</p>	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
9. Extraction retraining (Training III)	<p>The Secret Service shall provide scenario-based extraction retraining to all protective operations personnel by end of year 2025, emphasizing the necessity of appropriate urgency in extractions and the criticality of ensuring that the protectee is not exposed during the extraction, consistent with long-standing protective principles. The Secret Service shall also ensure that all protectees receive extraction and related protection training, to be conducted by their detail, and that this training is periodically refreshed for protectees.</p> <p>Additional Commentary: The detail agents who responded to former President Trump within seconds of shots being fired to form the “body bunker” performed bravely and, regarding that initial response, in a manner consistent with Secret Service training and policy. However, during the extraction of former President Trump from the stage to his armored vehicle, upper portions of the former President’s body were visibly exposed for critical seconds during a time when no one knew definitively whether there were additional shooters in his vicinity.</p>	December 31, 2025

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

Recommendation	Description of recommendation	Due date
10. Refocus on the Secret Service's protective mission	<p>The Secret Service must be the world's leading governmental protective organization. The events at Butler on July 13 demonstrate that, currently, it is not. To achieve this mission, the Secret Service must ensure that its operations, training, budgeting, personnel, and all other critical organizational inputs are hyper focused on its protective mission, and the Secret Service shall conduct a comprehensive assessment to identify any factors that currently detract from that focus. As part of this assessment, the Secret Service shall specifically consider what current responsibilities the Secret Service needs to shed or discharge so that it can provide its protective mission with all resources required to fulfill that responsibility. To the extent that any investigative priorities remain within the Secret Service's portfolio of responsibilities, they must be directly supportive of and subordinate to the overriding protective mission.</p> <p>The Panel notes that the Secret Service has a budget of \$3.1 billion and approximately 3,200 special agents. Whatever else the Secret Service may do, its core, essential, and unique mission is to protect its protectees, including the President, Vice President, and nominees for President in an election. No other federal law enforcement agency can discharge this duty. And the duty is a zero-failure mission. All assets should be allocated to that mission before any other tasks—including law enforcement responsibility for financial frauds, for example, or perhaps law enforcement duties entirely—are undertaken. There is simply no excuse to need to “do more with less” concerning protection of national leaders; unless and until those responsibilities are fulfilled, no resources (funds or time) should be allocated to other missions that are not centrally related to the protective function.</p> <p>As an additional means to increase the Secret Service's prioritization of its protective mission above all else, the Secret Service shall implement a reorganization so that certain of its Offices shall report directly to the Office of Protective Operations, which shall be elevated above them in the Secret Service's organizational structure. In particular, the Panel recommends that the Office of Investigations, the Office of Strategic Intelligence and Information, the Office of Technical Development and Mission Support, and the Office of Training all report into the Office of Protective Operations, along with any additional major operational support units in the Secret Service's organizational structure, with appropriate sub-level restructuring as needed to facilitate this reorganization.</p> <p>The Panel does not make these recommendations or related observations lightly, but rather offers them in view of the crucial nature of the Secret Service's protective mission for the ongoing continuity of American government and democratic functioning and the extent to which the events of July 13 at Butler have revealed critical deficits in the Secret Service's ability to operate that mission. In that context, in the Panel's opinion, it is simply unacceptable for the Secret Service to have anything less than a paramount focus on its protective mission, particularly while that protective mission function is presently suboptimal.</p> <p>In addition to ensuring focus on the protective mission, the Panel believes this refocus will assist the Secret Service in concentrating resources to further support protective operations and, in the longer term, will beneficially drive cultural change to emphasize the cardinal role of protective operations and better empower agents to conduct their “no fail” mission.</p>	None



**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
11. Fresh leadership perspectives	<p>The first steps of leadership change at the Secret Service have already begun with the former Director having stepped down in July 2024 and the Service currently being led by an acting rather than permanent Director. The Panel agrees that a failure of the magnitude that occurred at Butler on July 13 necessitates such change at the Secret Service as soon as practicable, including at the top of the Service and various areas throughout. Many of the issues that the Panel has identified throughout this report, particularly regarding the Panel's "deeper concerns," are ultimately attributable, directly or indirectly, to the Secret Service's culture. A refreshment of leadership, with new perspectives, will contribute to the Secret Service's resolution of those issues.</p> <p>Moreover, the Panel strongly believes it is important that: (a) the new leadership of the Secret Service come from outside the Secret Service rather than internal promotion, and (b) the newly selected Director be allowed to bring in the leadership team he or she thinks most fit. Of course, that leadership must have relevant prior experience regarding protection and security. But, although experience within the Secret Service is laudable and important, and some members of a future leadership team will likely be Secret Service veterans, the events of Butler suggest that there is an urgent need for fresh thinking informed by external experience and perspective; the new, external leadership will still undoubtedly draw on subordinates with deep experience within the Secret Service to aid them in their acclimation, but ultimately, the non-Secret Service perspective will benefit the protective mission during this critical juncture.</p> <p>The Panel reiterates its belief that a leadership change will assist the Secret Service in addressing many of the issues identified in this Report, including the present sense of complacency within the Secret Service—observed by this Panel and others—as well as the need for Secret Service leaders to exhibit extreme ownership to ensure success in carrying out their "no fail" mission.</p>	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
12. Leadership training, training with state and local partners, and prioritization of training for the success of the protective mission (Training IV)	<p>The training recommendations in the prior section respond to certain of the specific failures and breakdowns at Butler, but the Panel also perceives the opportunity for training to address certain of the deeper issues it has identified.</p> <ul style="list-style-type: none"> <li>a) The Secret Service shall institute a Leadership Training Institute, modeled after other senior government level leadership training programs, to better develop the necessary leadership skills in its senior personnel corps, including senior leaders of field offices and details. Leadership training shall be available to—and in appropriate instances, required of— personnel from an early-stage of their career where it can make the most impact in terms of fostering leadership skills, rather than delaying such training until personnel are already in positions of leadership, at which point the personnel will be deprived of the full benefit of such training (though ongoing leadership training for senior-level personnel is also important and should be implemented). The Panel believes this will be an important step in rectifying the observed lack of ownership by senior level personnel regarding Butler.</li> <li>b) The Secret Service shall institute a nationwide program pairing Secret Service field office personnel with their state and local law enforcement partners in a manner designed to provide training to state and local partners on principles in protective operations as well as how state and local assets will interoperate with the Secret Service for protective events. This training should include a component of practiced interoperation between Secret Service and state and local personnel, and the training should reoccur at least every 2 years with advanced course options also available for state and local participants who have already completed the foundational course. This effort admittedly will take time, which, again, may require shedding certain peripheral responsibilities like financial fraud and counterfeiting investigations, and perhaps all criminal investigative work that is not directly tethered to the protective mission.</li> <li>c) The Secret Service must realign its expenditure of time, resources, and responsibilities so that training on the core protective mission is a top-tier priority. The Secret Service shall ensure that all agents receive regular, required training throughout their careers. Scheduling must account for this training commitment so that agents are not routinely taken out of scheduled training to, for example, staff trips or events. If the objection to such a realignment is that “there isn’t enough time for training on the protective mission,” then the responsibilities and activities that prevent such training—including law enforcement efforts on matters such as financial fraud or counterfeiting—should be reallocated to other federal law enforcement agencies.</li> </ul> <p>Additional Commentary: Training is certainly one area where additional resources are needed. As described above, the Panel received briefings reflecting that Secret Service agents spend a modest, or perhaps even minimal, amount of time training, particularly during election years, but also more generally. The Panel also understands that only approximately 2 percent of the Secret Service’s current non-pay budget is allocated to training, which is woefully inadequate. Finally, the Panel understands that the Secret Service’s training facilities are generally in need of significant physical upgrades. The essential point is that it is unfair—to protectees, the Secret Service itself, and to the American public—for the Secret Service to have inadequate time or focus to train to elite levels on all aspects of the core protective mission.</p>	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
13. Longer-term communications solutions	<p>The communications remediations in the prior subsection address the most immediate, direct communications issues which affected personnel at Butler on July 13. But the Secret Service must also evaluate longer term, more sweeping remediations to communications interoperability, including using revised communications technologies to facilitate interoperability with the Secret Service's state and local partners in complex protection settings.</p> <p>Additional Commentary: The topic of communications interoperability has been a subject of discussion within the law enforcement community for decades, and its criticality has been repeatedly highlighted for many years, including within the Department of Homeland Security. This should not be an impossible task—law enforcement has been discussing these issues for decades, and similar coordination is required at professional and collegiate sports events, the Olympics, and so forth. Highly reputable and vetted American companies have already developed this sort of technology; this reform should not require inventing new paradigms or equipment that do not presently exist. Again, failure on this front is not an option.</p> <p>While not a formal recommendation of the Panel, the Secret Service may be benefited by the formation of a working group to fill in the technical particulars of this longer-term approach to interoperability. If this is pursued, the working group should be composed of personnel from both within the Secret Service and outside it, with expertise in communications technology, protective operations, law enforcement, and related regulatory and policy matters. The first step of any such group would be to draw on the large body of existing work and analysis that has been generated on this topic, including by the Department of Homeland Security. The availability of this pre-existing body of work suggests that an appropriate timeline for the group to deliver a report and recommendations to the Secret Service and/or Secretary is within 3–6 months of its formation.</p>	None
14. Development of a continuous improvement and auditing center	<p>The Secret Service shall develop, fund, and staff a continuous improvement and auditing center, designed to both engage in continuous improvement and auditing activities directed toward the field offices and details and assist the field offices and details in developing their own slates of continuous improvement and auditing activities, including through written policy requiring the implementation of such activities. Examples of the types of conduct to be considered include</p> <ul style="list-style-type: none"> <li>a) formalized after-action assessments following planned events;</li> <li>b) randomized periodic auditing of historical site security plans for retroactive assessment and development of lessons learned, or equivalent tabletop or full-scale exercises;</li> <li>c) regularized day-of event auditing by dedicated personnel solely tasked with ensuring that standards and specifications are being met;</li> <li>d) periodic “red teaming” exercises by external personnel;</li> <li>e) quality assurance processes to confirm integration and retention of lessons learned over time; and</li> <li>f) external benchmarking or pacing against organizations and institutions with demonstrated capability for protective excellence.</li> </ul>	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
15. Evaluation of methodology for protectee resourcing	<p>The Secret Service shall evaluate its methodology for protectee resourcing, including regarding detail staffing and allocation of protective resources to details and for protectee events, with a focus on assessing whether the current method of protectee resourcing is overly formulaic (for example, placing undue weight on whether a protectee is a “former” versus “candidate” versus “nominee”) as compared with a more flexible method which places greater emphasis on the threat environment facing the protectee over the protectee’s title.</p> <p>Additional Commentary: Certain individuals attract more attention and emotion—from the public, from the media, on social media and the internet, and so forth. Allocation of resources must be risk-based, with dynamic assessments, in practice. There are, to be sure, certain responsibilities attendant to the President (for example, Commander-in-Chief duties) and Vice President that are unique. However, the threat to a presidential candidate, and the attendant loss of public confidence in the federal government if something preventable happened to a candidate, are profound. There were various enhanced measures put in place to protect former President Trump and others in the wake of the Butler shooting, but those measures fairly should have been expected and deployed before the tragic events that occurred there.</p> <p>To reiterate, the Panel appreciates that determining the appropriate level of protectee resourcing involves a complicated balancing act and must necessarily include considerations of the role of the protectee—a sitting President, who is responsible, for example for carrying the nation’s nuclear codes, is different from a candidate or a former office holder. Nonetheless, the Panel’s perception is that the Secret Service’s resourcing model may have struggled with the unique, hybrid nature of former President Trump as both a former President but also, from almost immediately upon his exit from office, a prospective candidate for the presidency—a situation not encountered in the country since at least 1940 with Herbert Hoover, who was not even a nominee that election.</p> <p>This struggle appears to have affected, for example, the resourcing and staffing of the former President’s detail, with back-and-forth between the detail and Secret Service headquarters regarding appropriate personnel levels and whether former President Trump’s status as a “former” in the Secret Service’s resourcing model adequately captured the unique security threats he might engender as not just a former president but a former President with significant and unique associated risk who also appeared to be conducting himself in the manner of a prospective candidate. The Panel also again emphasizes that achieving the proper level of resourcing for formers, candidates, and nominees is a vital component of the Secret Service’s protective mission, as the loss of a protectee would have profound ramifications on the democratic process.</p>	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
16. Budget and personnel considerations	<p>The Panel reiterates and emphasizes its view that, while additional resources to the Secret Service would be helpful, if the remediation and reform dialogue around the failures of July 13 devolves into a discussion about how much additional money the Secret Service should receive, critical lessons from July 13 will have been lost. The failures of July 13, as embodied in the specific breakdowns and deeper concerns canvassed above, are not primarily tied to budgetary deficiencies at the Secret Service. Put otherwise, even an unlimited budget would not, by itself, remediate many of the failures of July 13. This is not to suggest that additional budgetary funding could not be beneficial to the Secret Service—it could, particularly if it is targeted to address the deficiencies identified in this Panel’s report and is used judiciously and thoughtfully.</p> <p>Additional funds would also mitigate a “do more with less” mentality and the attendant effects it can have on agents (including burnout). Secret Service agents work incredibly hard and, during election years in particular, are sent across the nation and abroad on a moment’s notice to protect the country’s former, current, and potential future leaders and their families. Additional agent resources, coupled with a paramount focus on the protective mission, will advance the critically important goal of ensuring that all agents are continually trained and retrained and that they will be appropriately rested and ready when called upon to perform their protective mission. That said, an influx of funds, without more, will not address the problems July 13 revealed.</p> <p>The Panel also recommends that any effort to increase protective personnel staffing levels within the Secret Service be accompanied by two initiatives: (a) an evaluation of the allocation of existing protective personnel to ensure that staffing is being rationally allocated—for example, are there opportunities to re-allocate 1811s to task types for which they are specifically needed and off-task types that can be conducted by non-1811s, and (b) an assessment to identify potential opportunities to increase the use of Department of Homeland Security resources specifically for protective operations, including but not limited to Homeland Security Investigations and Transportation Security Administration agents, in ways that would increase the Secret Service’s protective capacity without compromising the quality of those protective operations.</p>	None
17. Recommendation status update	As a final recommendation, the Panel requests that an evaluation of the status of its recommendations be commenced by an independent party or parties engaged by the Department of Homeland Security by or before October 1, 2025, with a fulsome report to the Panel by or before December 31, 2025 and then subsequent reporting to the Department of Homeland Security.	<p>October 1, 2025</p> <p>December 31, 2025</p>

Source: Department of Homeland Security (DHS). | GAO-25-108568SU

Note: information is from Department of Homeland Security, Report of the Independent Review Panel of the July 13, 2024, Assassination Attempt in Butler, Pennsylvania (Washington, D.C.: Oct. 15, 2024).

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

**Table 5: Recommendations Included in Final House Task Force Report**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
1. Consolidate all operations plans	The Secret Service has the ultimate responsibility for securing the site for every protectee visit. The advance agents should therefore be aware of where every partner agency is posting personnel. Moving forward, the Secret Service should request copies of the operations plans of all law enforcement entities working the event and consolidate the assigned posts for each of the participating entities. For the July 13 event in Butler, the Secret Service advance agents did not have copies of all participating entities' operations plans, nor did they have copies of the locations of each officer providing security.	None
2. Consider coverage inside and outside secured perimeter	The Secret Service must maintain vigilance over state and local counterparts in ensuring the security of its protectees. As part of its zero-fail mission, the Secret Service should assess and address all security concerns both inside and outside of any event perimeter. While the Secret Service should consider support from local partners and their ability to secure areas surrounding an event, Secret Service must fully understand and verify the local assets available. Regardless of a location within or outside of any particular perimeter, the Secret Service must own responsibility for the security of the site, filling any gaps with its own personnel in the event that local counterparts are unable to provide adequate security or to the extent heightened security concerns demand Secret Service presence.	None
3. Document all line-of-sight vulnerabilities	Secret Service site agents must identify all potential lines of sight to the protectee that a trained sniper could reasonably be expected to utilize, state how such lines of sight will be mitigated, and ensure that a supervisor has approved the mitigation strategy for each. The Secret Service Counter Sniper team lead must be given the opportunity to review the mitigation plan if counter-snipers are utilized for an event, and the mitigation plan should be shared with state and local law enforcement no later than the final meeting prior to the arrival of the protectee.	None
4. Implement written policy that clearly articulates a threat-based methodology for asset and resource approval	The nature of the campaign event in Butler, Pennsylvania on July 13, 2024—outdoors, in front of a large crowd, with an active [LES] from a [LES], among other risk characteristics—should have necessitated a specific protocol of mitigation assets. Instead, the Secret Service made ad hoc determinations as to the assets and manpower that were available to the planning team.	None
5. Utilize Secret Service counter-surveillance assets for all large outdoor events	The written policy should require counter-surveillance assets for all large outdoor events. Planners should not have to request those assets from Secret Service leadership and should not be empowered to waive or decline to incorporate those assets into the operations plan for any large outdoor event.	None
6. Implement a policy on sharing relevant intelligence for an advance trip among the Protective Intelligence and Assessment Division, the detail, and the relevant field office	The list of individuals read into the threat intelligence should include working supervisors such as the field office Special Agent In Charge, the protective intelligence agent, the lead advance agent, and the site agent to ensure proper assets are requested and vulnerabilities are mitigated.	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
7. Improve counter unmanned aircraft surveillance (cUAS) mitigation strategies for when cUAS or other drone systems fail	Secret Service should put in place policies and procedures for cUAS asset failure contingencies, to include certain requirements such as (1) required testing of assets the day prior to an event, (2) the possession of backup materials—cUAS operators should be required to carry as well as bring certain additional back up materials and parts to events, (3) creation of redundancies in the event of cUAS asset failure, and (4) implementing standardized troubleshooting procedures.	None
8. Implement and increase formalized training, certification, and cross-functional platform training for drone and cUAS operator	The Technical Security Division should implement a comprehensive, Secret Service-wide formal training and certification process for all drone and cUAS technologies, including a standardized “cUAS advance checklist.” Additionally, cross-functional training should be established to enable any agent to assume a collateral duty as a drone or cUAS operator if necessary. This training should also include a contingencies portion, which not only includes a section on troubleshooting cUAS assets, but also backup materials and items the cUAS agent should keep on hand in the event of an emergency. As part of the training program for cUAS, operators should be required to participate in a program where they shadow another cUAS agent from the beginning of the advance process through the event to ascertain on-the-job experience and to obtain first-hand knowledge of what the cUAS process entails in a real-life scenario.	None
9. Ensure that drone and cUAS operators assigned to events have passed and maintained required training and certification as well as any necessary updates	Special agents must be familiar with the equipment they employ and be prepared to address last minute or technical issues.	None
10. The DHS and Secret Service should consider utilizing Department of Defense drone operators to supplement Secret Service efforts at protectee events under the Presidential Protection Assistance Act	Deploying Department of Defense drone operators would free up other special agents for protectee duties, alleviate manpower strain, and enhance the effectiveness of surveillance operations.	None
11. Congress should consider whether current legal authorities to mitigate credible threats posed by unmanned aircraft systems (UAS) should be expanded	The rapid expansion of the commercial UAS market has increased the threat of drone incursions at protectee events. Congress should consider legislative proposals that would responsibly extend and justifiably expand legal authorities to respond to credible threats all the while balanced by appropriate safeguards to protect Americans’ privacy, ensure aviation security, and allow for authorized commercial activity. For instance, Congress should consider authorizing DHS to establish a cUAS mitigation pilot program under which selected state and covered local law enforcement agencies may operate approved cUAS mitigation systems and mitigate unauthorized UAS operations on behalf of covered entities within their jurisdictions.	None
12. The Secret Service needs to make every effort to ensure representatives from all state and local law enforcement agencies assisting with security for a protectee event are in a unified security room	While the Office of Protective Operations (OPO)-08 policy update is a step in the right direction, a unified security room helps ensure real-time information sharing among all security partners.	None



**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
13. The Secret Service should ensure that all state and local law enforcement partners have a communications plan in place for protectee events, and a Secret Service special agent should be designated to collect and review those plans	This will help ensure communications between command post personnel and every law enforcement entity at the event.	None
14. Secret Service should ensure that its personnel and its state and local partners all establish a hierarchy for method of communication and each entity alert its law enforcement officers when switching to a different medium	Generally, radios and government-issued devices should be used, with personal devices as a last resort. Also, it is helpful for state and local law enforcement radios to have interoperability to be able to listen to other channels.	None
15. To assist with any potential reviews and investigations, Secret Service should record all Secret Service radio communications	Secret Service should record its radio communications and preserve any written communications while prohibiting the use of encrypted messages apps (e.g., Signal) that do not preserve data. Given how video footage helps with providing clarity to the public, Secret Service should make it a best practice for post-standers to use body-worn-cameras during events.	None
16. Secret Service should assess already-available technology and examine ways to utilize it to improve their operations	N/A	None
17. Prioritize periodic training on protective operations in order to ensure that agents stay current on their training, even during busy times	Many agents testified that when operational tempo is high, training often becomes a casualty.	None
18. Provide more defined training curriculum and set specific requirements and time frames for regular training	Many agents testified that they do not have set ongoing training standards.	None
19. Work with DHS Homeland Security and Investigations (HSI) to ensure that HSI agents that participate in Secret Service-led protective operations receive training that is appropriate to the tasks that they are asked to support	N/A	None
20. Confirm key points of contact	Early in the planning process, the Secret Service advance team needs to confirm the primary representative for each state and local law enforcement agency and which agencies will be working jointly and independently drafting operations plans.	None
21. Provide a unified briefing on the day of the event	The Secret Service needs to provide a unified briefing either the day of a protectee visit or the day before, which includes at least one representative from all state and local law enforcement agencies assisting with an event. Doing so will help eliminate gaps in situational awareness and ensure critical information is shared more broadly.	None
22. Conduct mandatory pre-event meetings for key stakeholders on a daily basis	Secret Service should also consider mandating daily "check-in" meetings in the days immediately before an event for all relevant state and local counterparts involved in event security.	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
23. Secret Service must affirmatively state which Secret Service office or protective detail is the lead for an event	This designation should be based on the event location, available resources, protectee threat assessment, and overall risk profile of an event. The protective detail and local field office should undoubtedly work together to complement each other's strengths—the local field office may be better acquainted with a site and have relationships with local law enforcement while a detail has insight into the protectee's expectations—but the Secret Service must designate and document the single lead entity and reporting lines for an event.	None
24. Record all radio transmissions and evaluate communications retention policies	Secret Service should record its radio transmissions for all protective events and should consider its overall approach to records retention, including maintaining SMS and email communications. On July 13, the Secret Service did not record its radio communications. The absence of radio logs or recordings significantly limits the ability to reconstruct events for either investigative or evaluative purposes. Acting Director Rowe testified to directing the Secret Service to record radio transmissions for such events going forward, but the agency's updated policies still condition radio recording for Presidential nominee and certain other protectee events on staffing and equipment availability. To the extent that there are any technological limitations that prevent radio recordings or logs for all protective events, the Secret Service must prioritize addressing those challenges to enable this capability.	None
25. Consider staffing redundancies for high pressure moments	The Secret Service may consider additional staffing or flex posts to increase adaptability to evolving situations, but at the core of this recommendation is the suggestion to develop its contingency planning, particularly in chaotic and emergency situations, to ensure that personnel are available to respond to all communications and actions. The Task Force identified multiple instances in which Secret Service personnel reported they could not perform one function while attending to another urgent need. The agency should reassess its staffing of critical posts such as the command post or security room agent and counter-sniper teams, which may be more likely to have competing demands during critical response periods. Further, the number of roving posts such as counter surveillance response, site protective intelligence, and relief agents should match the demands of an event site. The demands of an event situated on a 100-acre property with an anticipated 15,000 attendees well exceeded the capacity of only three agents, each with unique roles that state and local counterparts could augment but not replace.	None
26. Develop and formalize process for escalating conflicts with protectee staff	The Secret Service should implement a formal process by which personnel may raise concerns in their planning with protectee staff. Over the course of our investigation, several members of the Secret Service expressed frustrations in negotiating with staff, regardless of political party or protectee. Ultimately the Secret Service is responsible for protectee security, but the agency may find itself working with staff who assert competing interests such as scheduling and optics. A formal process by which personnel may raise concerns in their dealings with protectee staff will empower agents to raise those issues to supervisors and leave Secret Service with a record of the dispute to evaluate should further issues arise. Any such documentation should be considered confidential and should be exempt from any public disclosure requests.	None

**Appendix III: Recommendations Made to the  
Secret Service in 2024 and 2025 by Other  
Congressional Investigative Committees**

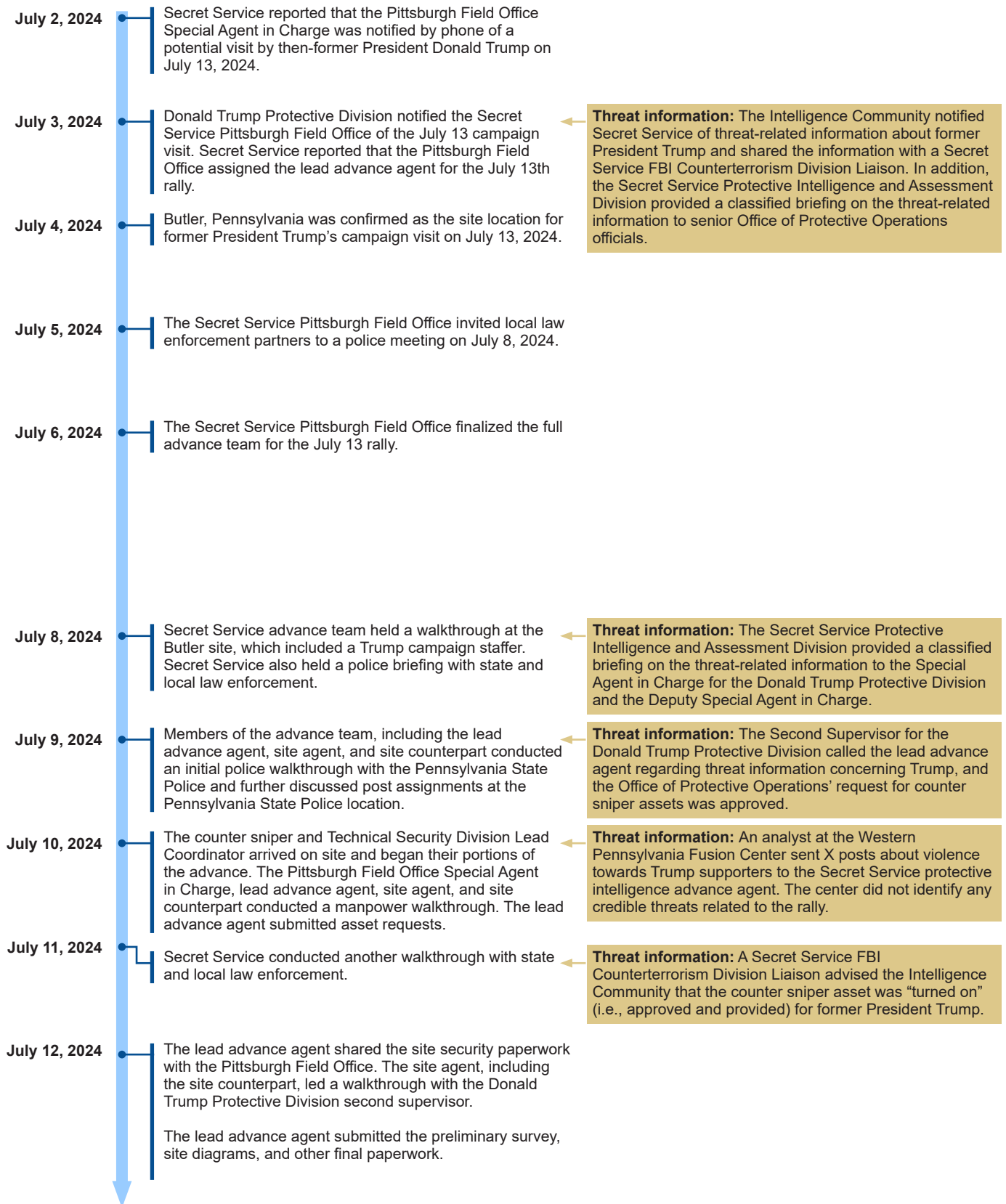
<b>Recommendation</b>	<b>Description of recommendation</b>	<b>Due date</b>
27. Provide more robust training for non-Secret Service federal personnel on-site	When assigned to Secret Service protective missions, non-Secret Service federal personnel have the same zero-fail mission as Secret Service personnel—to protect the protectee. DHS supported former President Trump’s July 13 event by providing HSI agents, but Secret Service personnel testified to the Task Force that these agents—and HSI agents generally—can be challenging to manage because “you’re having to explain the posts a lot more and you don’t know whether they even have worked with us before.” The Task Force obtained testimony that for July 13, HSI agents allegedly received “a 1-hour PowerPoint or something like that,” and that the Secret Service would otherwise only provide the morning briefing and the relevant paperwork on the day of an event. While the Task Force did not observe critical HSI agent failures on July 13 during the course of its investigation, the Secret Service failures that day demonstrate that trainings and preparations for non-Secret Service federal personnel must be strengthened and more robust for protective missions.	None
28. Prioritize experience in assignment process	Secret Service personnel must have an avenue to gain experience in protection details and in particular to be able to fulfill their responsibilities in advanced planning assignments. To develop that expertise, Secret Service should allow less-experienced personnel to participate in advance planning. However, high-risk protection events are not an appropriate setting for less experienced agents to gain on-the-job training in leadership roles. For high-risk events, such as the July 13 campaign event in Butler—an event that was outdoors, drew a large crowd, and featured one of the most prominent protectees—only agents with experience in advance planning should be assigned leading roles.	None
29. In-person advance activities must include all relevant subject matter experts	The Secret Service cites the strain on headcount and the heightened pace of the campaign season for not having all advance agents on the ground for the entire advance, with one aspect of work—the counter assault team (CAT) advance—being performed over the phone. While the Task Force did not identify failures of the CAT advance team for this particular event, Secret Service should—and indeed already has—addressed the unnecessary risk of tactical advance agents not being on the ground to scope sites. All substantive advance decisions that require viewing the site should be made by somebody who has assessed the location in person.	None

N/A: not applicable

Source: House Task Force. | GAO-25-108568SU

Note: This information is from House Task Force, Attempted Assassination of Donald Trump (Washington, D.C.: Dec. 5, 2024). We use [LES] to redact information Secret Service determined to be law enforcement sensitive.

# TIMELINE OF KEY EVENTS RELATED TO THE JULY 13, 2024 RALLY



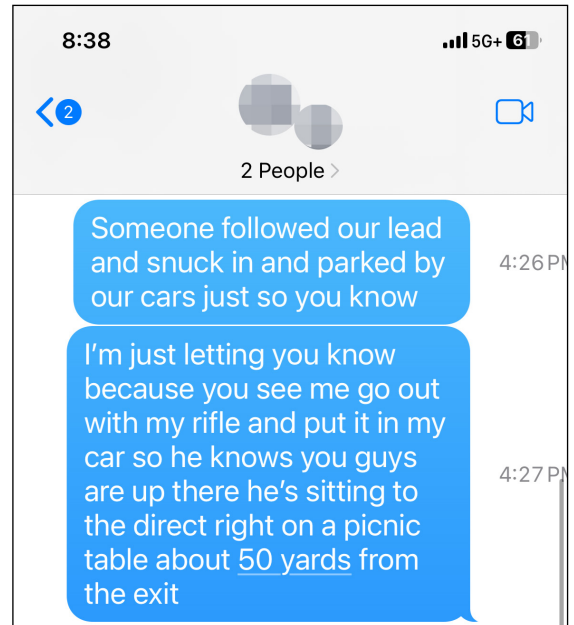
Appendix IV: Timeline of Key Events Related to the July 13, 2024 Rally

July 13, 2024

Trump campaign rally on July 13, 2024:

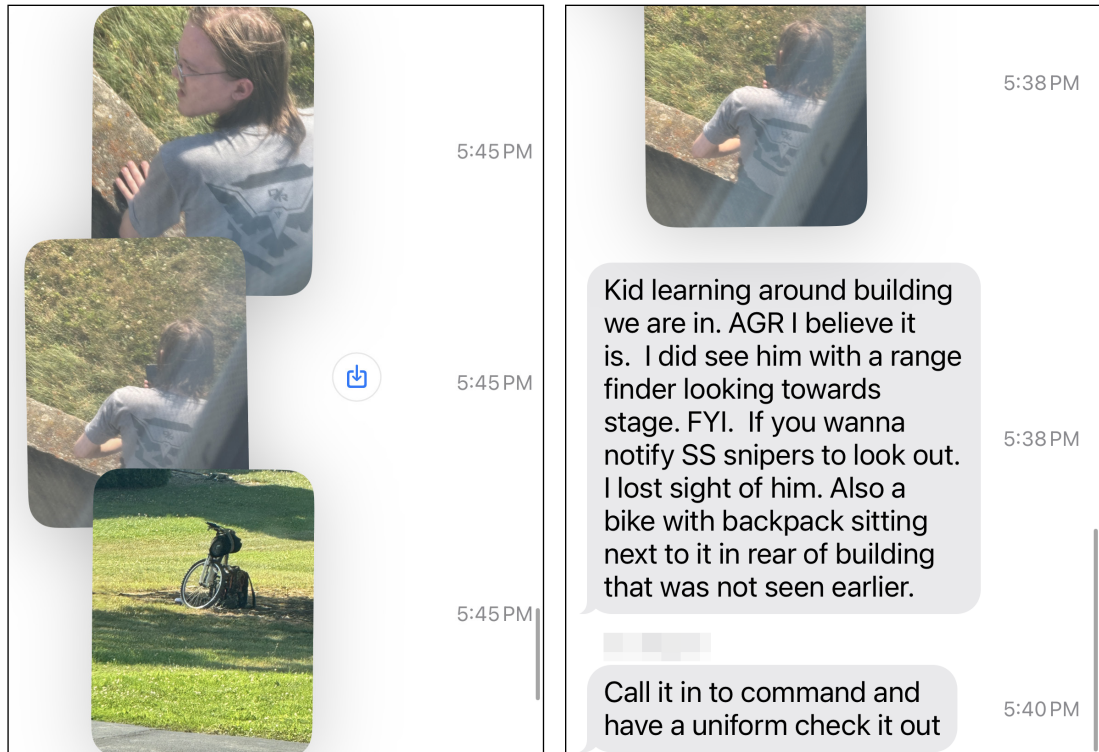
- **9:15 am:** Butler Emergency Services Unit briefed local law enforcement.
- **10:00 am:** Secret Service site agent briefed Homeland Security Investigations agents.
- **11:00 am:** Donald Trump Protective Division Counter Unmanned Aircraft Systems (cUAS) began to test the cUAS equipment.
- **11:21 am:** Butler Emergency Management Services shared a social media post about threats to Donald Trump with the protective intelligence advance agent, who then shared it with members of the advance team.
- **11:30 am:** The cUAS advance agent for the Donald Trump Protective Division determined the cUAS equipment was inoperable and began to troubleshoot.
- **3:51 pm:** According to the FBI, the gunman, Thomas Matthew Crooks, flew his drone for approximately 11 minutes in the vicinity of the site.
- **4:26 pm:** Beaver County snipers note that they observed an individual sitting on a picnic table, who parked in a restricted area and observed Beaver County snipers move into the AGR International, Inc. (AGR) building.
- **4:29 pm:** The cUAS equipment became operational.
- **5:14 pm:** Beaver County snipers located inside the AGR building notice Crooks sitting on a small concrete wall.
- **5:38 pm:** Beaver County snipers located inside the AGR building observed Crooks with a range finder and were asked to call it in to the command post.

**Figure 6: Text Message from Beaver County Sniper Group Chat on July 13th, 2024**



Source: Beaver Counter Police Department. | GAO-25-108568SU

**Figure 7: Text Messages From Beaver County Sniper Group Chat on July 13th, 2024**



Source: Beaver Counter Police Department. | GAO-25-108568SU

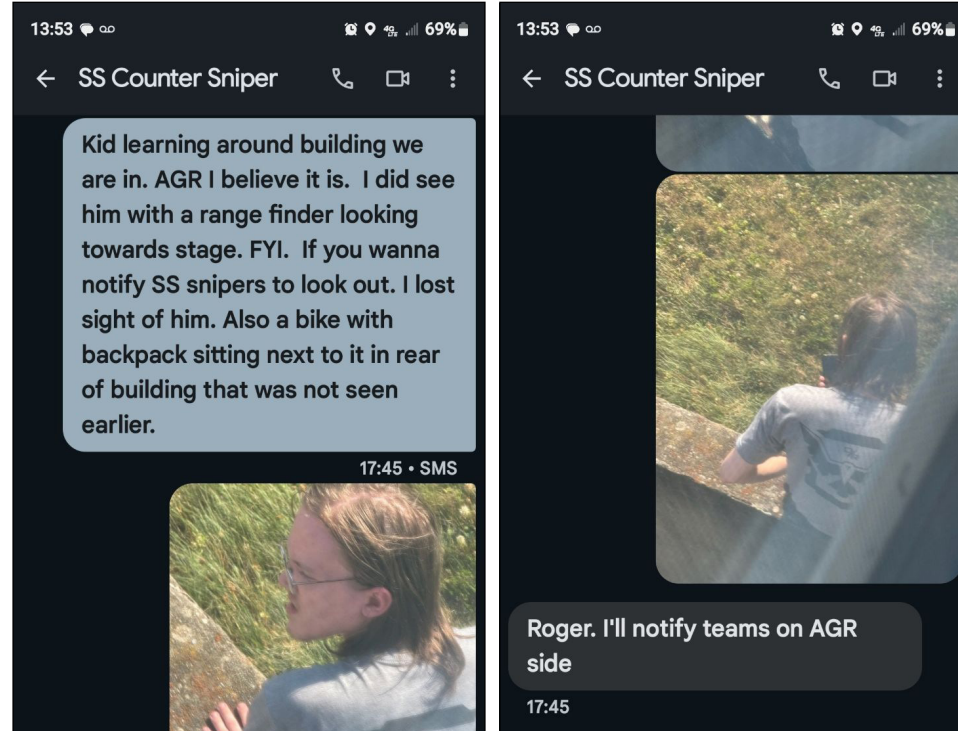


Appendix IV: Timeline of Key Events Related to the July 13, 2024 Rally

July 13, 2024  
(continued)

- **5:45 pm:** Butler County officers radioed to be on the lookout for a young white male with blond hair and a backpack near the AGR building. Beaver County snipers and Butler Emergency Services Unit personnel sent photos of Crooks to the local mobile command post and to Secret Service counter snipers.

**Figure 8: Text Messages Between Butler Emergency Services Unit Sniper and Secret Service Counter Sniper Regarding an Individual Near the AGR Building on July 13, 2024**



Source: Butler Emergency Services Unit. | GAO-25-108568SU

- **5:49 pm:** Butler County officers identified that the individual had a range finder and attempted to text pictures of the gunman, but experienced cell phone connectivity issues. As a result, they sent photos via email.
- **5:56 pm:** Local law enforcement observed Crooks with a backpack.
- **6:00 pm:** Local law enforcement observed Crooks entering an alcove between the AGR buildings.
- **6:08 pm:** Crooks was observed on the roof of the AGR building.

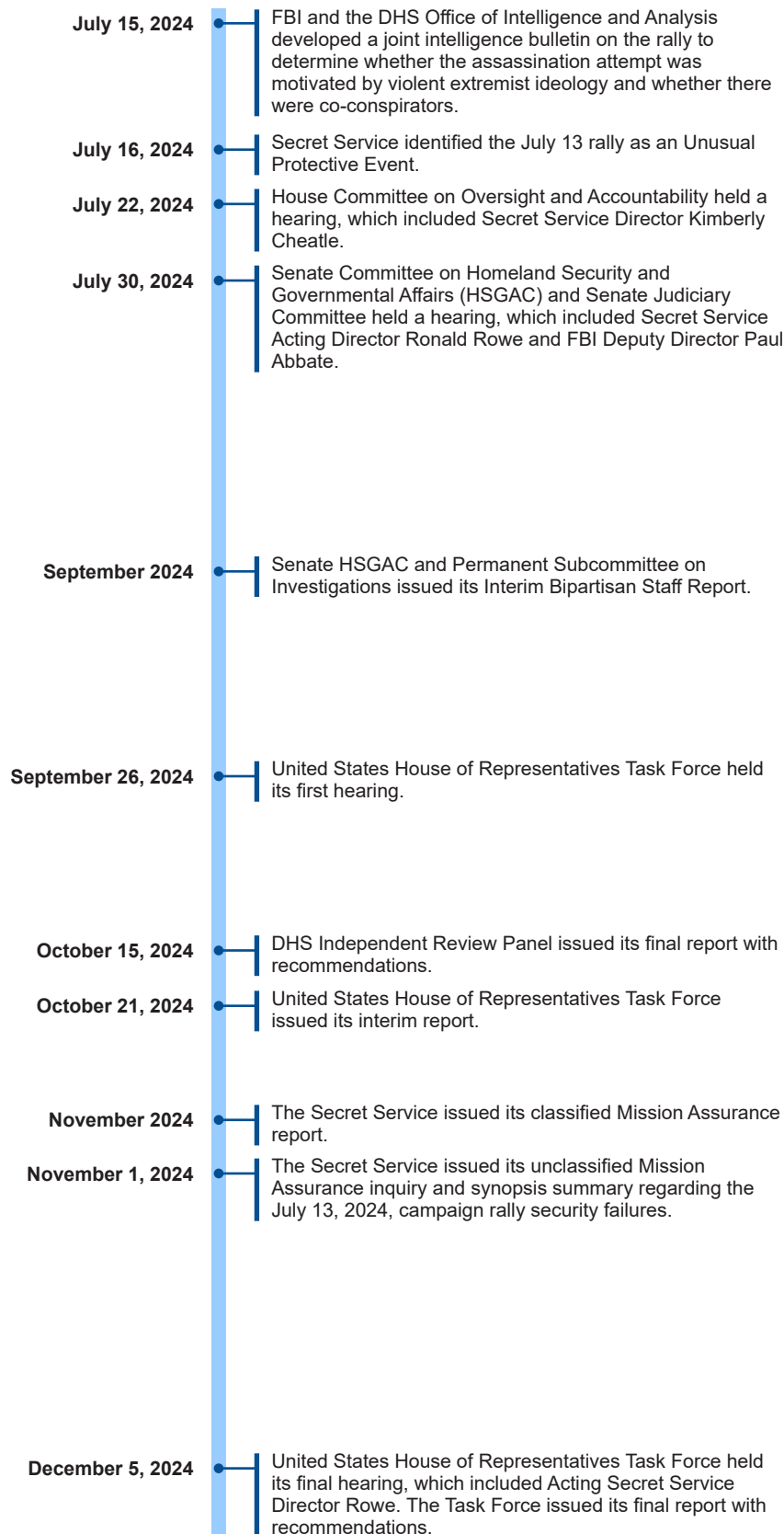
**Figure 9: Pennsylvania State Police Dash Cam Image of State Trooper Identifying an Individual on the roof of the AGR Building on July 13th, 2024**



Source: Pennsylvania State Police. | GAO-25-108568SU

- **6:11 pm:** Local law enforcement observed Crooks with a long gun, and Crooks fired shots.

Appendix IV: Timeline of Key Events Related to the July 13, 2024 Rally



Source: GAO analysis of U.S. Secret Service, Intelligence Community, Pennsylvania State Police, and local law enforcement information, which includes emails, texts, radio logs, and video footage. | GAO-25-108568SU



# Appendix V: Comments from the Department of Homeland Security

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



**Homeland  
Security**

BY ELECTRONIC SUBMISSION

July 9, 2025

Triana D. McNeil  
Director, Homeland Security and Justice  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548-0001

Re: Management Response to GAO-25-108568SU, "SECRET SERVICE: Gaps in Policy and Threat Information Sharing Hindered Efforts to Secure 2024 Trump Campaign Rally"

Dear Ms. McNeil:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the U.S. Government Accountability Office's (hereafter referred to as "the auditors") work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note the auditor's recognition of the importance of the U.S. Secret Service's "Zero-Fail" mission to protect the President and Vice President of the United States, as well as provide lifetime physical protection for former Presidents. DHS remains committed to strengthening processes and policy for sharing threat and risk information to ensure Secret Service agents and partners, as appropriate, have information needed to fulfil its mission to provide effective protection.

The draft report contained 8 recommendations, with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for the auditor's consideration, as appropriate.

**Appendix V: Comments from the Department  
of Homeland Security**

---

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.

Sincerely,

**JEFFREY M.  
BOBICH**

Digitally signed by  
JEFFREY M BOBICH  
Date: 2025.07.09  
16:01:40 -04'00'

**JEFFREY M. BOBICH**  
Senior Official Performing the Duties  
of the Chief Financial Officer

Enclosure

**Appendix V: Comments from the Department  
of Homeland Security**

**Enclosure: Management Response to Recommendations  
Contained in GAO-25-108568SU**

GAO recommended that the Director of the Secret Service:

**Recommendation 1:** Develop a resource (e.g., a checklist or other readily available quick guide or tool) that provides agents, by role, with readily available information needed to have a clear understanding of the tasks they need to complete to properly secure a protected event.

**Response:** Concur. The Secret Service Office of Protective Operations, will conduct a review to determine the appropriate resource, such as but not limited to a checklist, quick guide, or similar tool, to provide agents with readily available information needed to have a clear understanding of the tasks they must complete to secure a protected event. Once complete, the Secret Service will promulgate this resource, as appropriate, to agents and partners.

It is important that readers of this report are aware that the Secret Service maintains policy established prior to July 13, 2024, that addresses the intent of this recommendation, including OPO-04, "Protective Advance Guidelines," (dated June 20, 2024) and OPO-06, "Site Security," (dated May 10, 2022) by providing guidance on securing protected events. Further, as noted by the auditors, the Secret Service Office of Protective Operations updated and issued additional policies since July 13, 2024, including OPO-03(01), "Protective Advance Overview," and OPO-03(02), "Advance Team Components," (both dated April 10, 2025). These updated policies address shortfalls and policy gaps pertaining to the roles and responsibilities of personnel securing a protected event.

These administrative guidelines are in addition to the comprehensive training provided to special agent trainees as part of the approximately 23-week-long Special Agent Training Class at the James J. Rowley Training Center. As part of their training, special agent trainees are required to take and pass the General Protection course of study, which includes practical simulated-training and protective advance exercises. In the General Protection course of study, special agent trainees are provided a booklet, "The Seven Phases of Site Advance Development," which describes the steps for properly securing a site. This and other information, including a guide for lead advance agents, "Helpful Hints for Lead Advances" and other resources, are also readily available to Secret Service personnel on the James J. Rowley Training Center Secret Service intranet site.

As part of efforts to develop a tool to provide agents with readily available information needed to have a clear understanding of the tasks they must complete to secure a protected event, the Secret Service will consider how best to make this tool readily

3

Appendix V: Comments from the Department  
of Homeland Security

available from issued equipment (e.g. smart phone or computer). Estimated Completion Date: October 31, 2025.

**Recommendation 2:** Make changes to Secret Service policies to (1) proactively share threat information internally, and (2) establish methods for sharing potential trends and tactics adversaries may use against a protectee with those responsible for designing site security.

**Response:** Concur. The Secret Service Office of Strategic Intelligence and Information, as a matter of procedure already proactively shares threat information internally, and employs methods for sharing potential trends and tactics adversaries may use against a protectee with those responsible for designing site security. Specifically, the Office of Strategic Intelligence and Information initiated a comprehensive policy review to ensure guidance is updated as appropriate to reflect new procedures to document threat reporting notifications. Once this guidance is updated, the Secret Service will distribute this guidance to agents and partners as appropriate. However, it must also be noted that—while the Office of Strategic Intelligence and Information shares information to the greatest extent possible, the Secret Service is limited in its ability to broadly distribute classified information by classification controls and other constraints by the U.S. Intelligence Community. Estimated Completion Date: August 29, 2025.

**Recommendation 3:** Develop a process to ensure actionable threat information is shared with individuals developing the site security plan, including Secret Service stakeholders and law enforcement partners.

**Response:** Concur. The Secret Service Office of Strategic Intelligence and Information, as a matter of procedure, already uses a process to ensure actionable threat information is shared with individuals developing site security plans for a protected event, including stakeholders and law enforcement partners. However, while the Office of Strategic Intelligence and Information shares information to the greatest extent possible, the Secret Service is limited in its ability to broadly distribute classified information by classification controls and other constraints by the U.S. Intelligence Community. Nevertheless, a comprehensive policy review is underway to ensure guidance is updated to ensure actionable threat information is shared with individuals developing site security plans for a protected event, as appropriate, and is nearing completion. Once complete, the Secret Service will distribute this guidance to agents and partners as appropriate.

Further, it is important that readers of this report are aware that—to date—the Secret Service also already evaluated and modified threat and intelligence sharing policies and procedures as follows in response to inquiries and recommendations from the U.S. House of Representatives and United States Senate since the July 13, 2024 rally:

**Appendix V: Comments from the Department  
of Homeland Security**

- The Office of Protective Operations initiated revisions to the Protective Operations Manual which will clarify that the protective intelligence agent assigned to an advance is responsible for gathering, evaluating, and appropriately disseminating all relevant intelligence information related to the visit of a protectee. Once complete, these revisions will require that for all protective visits, the lead advance agent will work with the protective intelligence agent (if assigned) from the Secret Service Protective Intelligence and Assessment Division, and all advance team members to ensure that all agents assigned to the visit are informed of relevant intelligence and threats against the visit and protectee(s).
- From November-December 2024, the Office of Protective Operations and the Office of Strategic Intelligence and Information have made personnel and policy revisions to numerous documents<sup>1</sup> to address threat and intelligence sharing. Currently, the Secret Service advance team receives updates from the intelligence advance agent throughout the advance process. The intelligence advance agent is in regular communication with the Protective Intelligence and Assessment Division and the Protective Intelligence Operations Center, and collaborates with the state and/or local police counterpart that are assigned to the event to obtain information in a timely manner which is then passed to the detail advance team.

Estimated Completion Date: August 29, 2025.

**Recommendation 4:** Develop a list of assets that may be requested to secure protectees, along with circumstances under which they are likely to be provided, and ensure the list is readily available to Secret Service personnel responsible for securing protected events.

**Response:** Concur. The Secret Service Office of Protective Operations will develop a list of assets that may be requested to secure protectees, as well as guidance on the circumstances under which these assets are likely to be provided. Once this list is complete, the Secret Service will promulgate this list to ensure it is readily available to personnel responsible for securing protected events.

While a list of all available protective assets currently does not exist in a consolidated format, it is important that readers understand that Secret Service policy in OPO-03, "Protective Advance - Overview," which was established prior to July 13, 2024, listed available assets for protective operations and, in some cases, indicated when they were likely to be provided. On April 10, 2025, Secret Service made significant updates to that policy, resulting in OPO-03(02), "Advance Team Components," to provide greater clarity

<sup>1</sup> Counter Surveillance Division – Directives 01 through 05, which are the Strategic Intelligence and Information Divisions' manuals regarding counter surveillance planning, directing, and executing tactical surveillance detection operations, staffing, training, and administrative procedures. Also updated were the Protective Intelligence and Assessment Division advance manuals, which describe the Division's policies and procedures for conducting protective intelligence investigations and advances.

**Appendix V: Comments from the Department  
of Homeland Security**

to those assets. The Secret Service also made policy revisions to OPO-24, “Protective Operations Staffing and Logistics,” in November 2024, to address the intent of this recommendation.

In addition, it is important that readers understand that a Secret Service advance team coordinates to plan and secure a protective event and is comprised of personnel from multiple divisions within the Secret Service. The Secret Service relies on the intentional make-up of the advance team to identify vulnerabilities, assess known threats, and mitigate risk. These advance team members are subject matter experts and possess current knowledge of available Secret Service resources at their disposal to secure a protective site. Much of this knowledge is gained through training received at the James J. Rowley Training Center, where special agent trainees are required to take and pass the General Protection course of study.

In the General Protection course, special agent trainees are informed of all available protective assets. Trainees are evaluated on their understanding of this knowledge through a written test, and engage in a series of practical training exercises that simulate the various conditions where principles of protection learned in the classroom are applied in realistic scenarios. During these practical exercises, experienced instructors closely observe special agent trainees and provide guidance and feedback to ensure trainees understand how to apply principles of protection effectively and according to policy. Successful completion of practical protection training exercises is required to graduate from the Special Agent Training Class.

Ultimately, protective assets are finite resources; the development of an available resource list does not mean that all resources on this list will be provided for every protectee or protective event. Each protective event is unique, and as such, the extent of staffing and resources dedicated to an event will vary. When assessing staffing and resource needs for protective events, the Secret Service balances efficiencies with effectiveness, working to ensure that all requisite personnel and resources are dedicated accordingly. Decisions made to achieve this balance are frequently rooted in experience derived from previous protective events and are always made to ensure the success of its protective mission. Estimated Completion Date: October 31, 2025.

**Recommendation 5:** Develop and implement a process that manages risks by consistently sharing known risk information when making resource allocation decisions for a protected event.

**Response:** Concur. The Secret Service Office of Protective Operations will develop and implement a process that manages risks by consistently sharing known risk information when making resource allocation decisions for a protected event. Once this process is developed, the Secret Service will promulgate implementation and guidance, as appropriate, to personnel responsible for security protected events, including agents and

6



**Appendix V: Comments from the Department  
of Homeland Security**

partners. ECD: June 30, 2026.

**Recommendation 6:** Document, in policy, initial and periodic refresher training requirements for authorized Secret Service cUAS [Counter Unmanned Aerial Systems] operators.

**Response:** Concur. The Secret Service Office of Technical Development and Applied Research, Aviation and Airspace Security Division, Counter Unmanned Aerial Systems Branch will conduct a review to determine how best to document in policy the existing initial and periodic refresher training requirements for authorized Secret Service Counter Unmanned Aerial Systems operators. Once policies and associated guidance are updated, as appropriate, the Secret Service will promulgate this guidance to agents and partners.

Previously, the Aviation and Airspace Security Division developed a Counter Unmanned Aerial Systems basic operator training program that was rolled out in late calendar year 2024. Currently, over 90 agents and officers, including Federal Air Marshals who augment Secret Service operations, graduated from this training program. In June 2025, the Aviation and Airspace Security Division also began surveying former Presidents' details, inventorying equipment and providing Counter Unmanned Aerial Systems training. The Aviation and Airspace Security Division is currently working with the Office of Protective Operations on formalizing required training for former Presidents' details. Estimated Completion Date: June 30, 2026.

**Recommendation 7:** Document, in policy, requirements for the new Aviation and Air Security Division, including outlining the oversight and internal control mechanisms it will employ to ensure that [Counter Unmanned Aerial Systems] use and training policies are adhered to.

**Response:** Concur. The Secret Service Office of Technical Development and Applied Research, Aviation and Airspace Security Division, Counter Unmanned Aerial Systems Branch will conduct a review to determine how best to document in policy requirements for the Aviation and Air Security Division, to include guidance on the oversight and internal control mechanisms that will be employed to ensure that Counter Unmanned Aerial Systems personnel are in compliance with use and training policies. The Aviation and Airspace Security Division is already developing new policies and updating existing policies, and is coordinating the policy drafting and review process with the DHS Counter Unmanned Aerial Systems Program Management Office. Once policies and associated guidance are created or updated, as appropriate, the Secret Service will promulgate this guidance to agents and partners. Estimated Completion Date: June 30, 2026.

**Recommendation 8:** Develop a policy as soon as possible, but before 2026, to require Secret Service personnel to conduct a capability assessment to identify potential audio

7



**Appendix V: Comments from the Department  
of Homeland Security**

---

and data communication challenges along with mitigation measures prior to a large or complex protectee event.

**Response:** Concur. The Secret Service Office of Technical Development and Applied Research, Operational Communications and Integration Division, and Office of Operations will conduct a review to determine how best to establish a requirement that Secret Service personnel conduct a capability assessment to identify potential audio and data communication challenges, as well as mitigation measures prior to a large or complex protectee event. Once this review is complete, Secret Service will take action to develop a policy, or other guidance as appropriate. Estimated Completion Date: December 31, 2025.

# Appendix VI: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Triana McNeil, [mcneilt@gao.gov](mailto:mcneilt@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, Joseph P. Cruz (Assistant Director), Khaki LaRiviere Bryant, Lauri Barnes, Willie Commons III, and Michele Fejfar made key contributions to this report.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).  
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).  
Visit GAO on the web at <https://www.gao.gov>.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

---

## Media Relations

Sarah Kaczmarek, Managing Director, [Media@gao.gov](mailto:Media@gao.gov)

---

## Congressional Relations

A. Nicole Clowers, Managing Director, [CongRel@gao.gov](mailto:CongRel@gao.gov)

---

## General Inquiries

<https://www.gao.gov/about/contact-us>

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**



Please Print on Recycled Paper.