Open-Source Threats to U.S. Secret Service Protectees Leading up to January 6, 2021

November 18, 2022

Fiscal Year 2022 Report to Congress

Homeland Security

United States Secret Service

Message from the Director

November 18, 2022

I am pleased to present the following report, "Open-Source Threats to U.S. Secret Service Protectees Leading up to January 6, 2021," which was prepared by the U.S. Secret Service (Secret Service).

The report was compiled pursuant to direction in the Joint Explanatory Statement accompanying the Fiscal Year (FY) 2022 Department of Homeland Security Appropriations Act (P.L. 117-103). As directed, this document examines the efforts to identify open-source threats against any protectees in the lead-up to the events of January 6, 2021.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable Lucille Roybal-Allard
Chairwoman, House Appropriations Subcommittee on Homeland Security

The Honorable Chuck Fleischmann
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Chris Murphy
Chair, Senate Appropriations Subcommittee on Homeland Security

The Honorable Shelley Moore Capito
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If you have any questions, please do not hesitate to contact me at (202) 406-5700 or Deputy Director Faron Paramore at (202) 406-5705.

Sincerely,

Kimberly Cheatle
Director
U.S. Secret Service

Executive Summary

The Secret Service's 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 (PID), which houses the Secret Service Open Source Intelligence Branch (OSB). OSB 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.

The web-based behaviors of interest indexed by PID in late December 2020, and in early January 2021, toward the President, Vice President, President-elect, and Vice President-elect were commensurate with weekly trends in the preceding weeks and were commensurate with similar post-election/pre-inauguration periods of prior administrations. Some web-based behaviors were discovered by OSB, while others were reported to PID by concerned citizens, local law enforcement, or other federal agencies. Only two web-based behaviors of interest during this period directly referenced the January 6, 2021, "March for Trump" event or the certification of election results at the U.S. Capitol. In the week preceding January 6, 2021, OSB focused its searches of publicly available information on the "March for Trump" event and prepared a product to provide situational awareness for Secret Service protective operations. OSB identified groups organizing, participating, and potentially counterprotesting the "March for Trump" event. OSB did not discover any actionable information indicating planned civil disobedience or violence while conducting these searches.

The Secret Service recognizes the legislative language from Congress requiring the inclusion of detailed recommendations for any resource needs identified for OSB along with a detailed justification for such request. The Secret Service will continue to review OSB resource needs as it works through future budget requests.

Open-Source Threats to U.S. Secret Service Protectees Leading up to January 6, 2021

Table of Contents

I. Legislative Language

This report was compiled pursuant to direction set forth in the Joint Explanatory Statement accompanying the Fiscal Year (FY) 2022 Department of Homeland Security (DHS) Appropriations Act (P.L. 117-103), which states:

> *Report on Open Source Threats to USSS Protectees Prior to January 6th.*— Within 90 days of the date of enactment of this Act, USSS shall submit a report to the Committees that examines the efforts to identify open source threats against any protectees in the lead up to the events of January 6, 2021. The report shall include an evaluation of the lessons learned in light of the attack on the U.S. Capitol, summarize all open source and classified Intelligence Community sourced threats towards any protectee, include specific details identifying when USSS discovered such open-source threats against any protectee, and provide USSS response to such threats, including whether the protectee, or any other member of the Executive Branch, was made aware of such threats prior to January 6, 2021. The report shall clearly delineate the timeline for each item above. The report shall also provide detailed recommendations for any resource needs identified for the Open Source Branch and provide a detailed justification for such requests.

II. Background

The U.S. Secret Service's (Secret Service) Office of Strategic Intelligence and Information plans, directs, and coordinates all 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 (PID), which houses the Secret Service Open Source Intelligence Branch (OSB). OSB 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.

OSB staff proactively reviews publicly available information daily on many major social media platforms to provide situational awareness that may affect protective operations. OSB works to identify behaviors of interest toward Secret Service protectees and to share within the Secret Service information that may assist in mitigating the risk of unwanted outcomes toward protected entities. OSB research focuses on identifying and locating unknown individuals and on analyzing the publicly available content on the individuals' social media accounts to aid protective intelligence investigative efforts. OSB also identifies groups that have demonstrated the potential for engaging in activities that may affect protective operations adversely. In FYs 2020 and 2021 combined, OSB staff identified more than 3,000 pieces of protective intelligence information.

OSB staff also prepares various finished open-source intelligence products to inform protective operations and executive leadership. Such products include:

- Open-source trip reports in advance of presidential travel outside the National Capital Region;
- Open-source protectee reports summarizing the protectee's publicly available open-source footprint and social media sentiment toward the protectee for a specific, prior point in time;
- Open-source event reports summarizing public awareness, publicly available demonstration activity, and social media sentiment for significant events with a large protective posture; and
- Open-source protective intelligence briefs covering a range of open-source-related topics of interest to protective operations.

OSB staff rely on publicly available, as well as, procured tools to perform their open-source searches.

Operations are conducted to support the protective mission while respecting First Amendment protected activities. OSB adheres to DHS Directive 110-01, "Privacy Policy for Operational Use of Social Media." OSB staff members are required to complete a 3-month, in-house training program, in which they learn the best ways to utilize the procured tools and how to fine-tune their open-source skills. OSB staff members subsequently are required to complete a minimum of 32 hours of open-source training annually to maintain and enhance their skill sets.

III. Analysis

OSB analyzes publicly available open-source social media information for Secret Service protected persons, sites, and events. When analyzing social media, OSB staff conducts broad searches using protectee names, combined with threatening or inappropriate terms to narrow the focus on content of a protective intelligence concern.

Following the large, post-election public gatherings in November and December 2020 in Washington, D.C., OSB analyzed publicly available social media information and produced a protective intelligence brief the week prior to the January 6, 2021, "March for Trump" event. This briefing document provided situational awareness for protective operations, identifying the groups that claimed responsibility for organizing the event and providing publicly available background information on each group. OSB's protective intelligence brief also identified hashtags that were used to organize the event and the caravans traveling across the country to join the event. For situational awareness and to inform protective operations, the brief included a summary detailing the number of anticipated participants and any indicators of planned civil disobedience that were publicly available. At the time that the protective intelligence brief was prepared, 2 of the 47 publicly available pro-Trump organized events had privacy restriction settings on their social media chat that prevented OSB from being able to view the content. OSB did not find any indications of planned civil disobedience in the available content related to pro-Trump events.

To provide situational awareness for protective operations, OSB also completed social media analysis on potential counterdemonstrations to the "March for Trump" event. OSB conducted research in the week prior to this event and observed less social media activity among the potential counterprotestors leading up to this event when compared to the November and December 2020 events. OSB also provided publicly available background information on potential counterprotest groups. OSB reviews of publicly available information related to counterprotest groups did not reveal any planned civil disobedience. Because of the anticipated participation of many of the same pro-Trump and counterprotest groups in January 2021, as in November and December 2020, PID assessed clashes were likely to occur between opposing demonstration groups.

Between December 30, 2020, and January 5, 2021, PID identified 80 web-based behaviors of interest directed toward President Donald Trump, Vice President Michael Pence, President-elect Joseph Biden, or Vice President-elect Kamala Harris, with some individuals expressing a behavior of interest in more than one Secret Service protectee. The behaviors of interest either were discovered by OSB analysts directly or were reported by concerned citizens or other government agencies. These web-based behaviors of interest were assessed as routine protective intelligence incidents, and all known threats toward Secret Service protectees were investigated in accordance with agency policies and procedures. The volume of protective intelligence directions of interest for each protectee was commensurate with normal weekly trends in the preceding weeks and was commensurate with similar post-election/pre-inauguration periods of prior administrations. Of these 80 web-based behaviors of interest:

- Two specifically referenced the "March for Trump" event or the certification of election results taking place at the U.S. Capitol on January 6, 2021; and
- One individual was arrested for violation of 18 U.S. Code (U.S.C.) 871 (Threats against the President) and 18 U.S.C. 875 (Interstate Communications), while another individual subsequently was held for mental health treatment by local law enforcement. Neither individual referred specifically to the "March for Trump" event in the web-based behaviors of interest that were identified.

PID did not receive from the Intelligence Community any unclassified or classified information regarding threats directed toward any Secret Service protectees leading up to January 6, 2021.

PID does not discuss threats or behaviors of interest with Secret Service protectees, but rather provides that information to protective detail special agents to assist their protective operations. When PID provides protective details with information on specific threats or behaviors of interest, agency protocol is for protective detail supervisors to brief senior staff members of the protectee; however, there may be instances that merit the detail supervisor's direct discussion with a protectee. PID has shared and continues to share relevant information with partner agencies and receives information from partner agencies that may affect agency operations.

The posture, capabilities, and functionality of OSB have not changed markedly since the events that transpired on January 6, 2021, at the U.S. Capitol. The sheer volume of publicly available content presents challenges for protective intelligence personnel. As this volume continues to increase, with some platforms having advanced search capabilities that narrow the results to relevant data and others requiring manual review, the demands on OSB staffing will continue to increase. Utilizing open-source tools that aggregate publicly available content from major social media platforms also requires staff to analyze context further in a way that only the human mind can understand. An independent social media analytical company reports that there are 4.62 billion active social media users globally.[1] Further, open-source research on the most popular social media sites revealed that 6,000 tweets per second are posted to Twitter[2]; 1 billion stories are posted daily on Facebook[3]; and more than 1 billion videos are watched on TikTok[4] per day.[5] As of August 1, 2022, OSB is staffed with 26 personnel, including supervisors. With the support of Congress, OSB was provided with 26 additional positions in FY 2022 (for a total of 52 personnel).

Additionally, protective intelligence information available via public sources is researched further to aid the subsequent protective intelligence investigation. Unexpected, exigent situations lead to increased demands and stressors for operational entities just meeting their

[1] Kemp, Simon. "Digital 2022: The Rise of Connected Tech Continues." *Hootsuite*, www.hootsuite.com/resources/digital-trends. Accessed 8 January 2022.

[2] Beveridge, Claire. "33 Twitter Stats That Matter to Marketers in 2022." *Hootsuite*, 16 March 2022, https://blog.hootsuite.com/twitter-statistics/.

[3] Martin, Michelle. "39 Facebook Stats That Matter to Marketers in 2022." *Hootsuite*, 2 March 2022, https://blog.hootsuite.com/facebook-statistics/.

[4] Ruby, Daniel. "TikTok User Statistics (2022): How Many TikTok Users Are There." *DemandSage*, 12 July 2022, www.demandsage.com/tiktok-user-statistics.

[5] Kemp, Simon. "Digital 2022: The Rise of Connected Tech Continues." *Hootsuite*, www.hootsuite.com/resources/digital-trends. Accessed 8 January 2022.

scheduled needs. OSB staff currently use tools and keyword searches to narrow the amount of social media data relevant to Secret Service protectees and equities, the content still needs to be analyzed manually to take into account the context or intent of the original post prior to pursuing protective intelligence investigations. A full manual review and analysis also are necessary to discover posts of protective intelligence concern that are posted utilizing GIFs, pictures, or videos, which cannot be captured by commercial tools or advanced searches, along with posts on certain platforms that lack advanced search capabilities.

The Secret Service recognizes the legislative language from Congress requiring the inclusion of detailed recommendations for any resource needs identified for OSB along with a detailed justification for such request. The Secret Service continuously reviews OSB's technologies and tradecrafts as social media platforms continue to evolve and grow. As additional resource needs are identified, the Secret Service will work with Congress to address those needs.

IV. Conclusion

OSB consistently works to review and analyze publicly available information to identify behaviors of interest and actionable information that require further investigation. This also is true for the days preceding January 6, 2021. Discovered information properly and expeditiously was disseminated internally and externally with appropriate law enforcement partners.

OSB will continue to support the Secret Service protective posture by providing actionable information consistent with applicable law and policy. Daily, OSB staff also will continue to review publicly available information on many major social media platforms proactively to provide situational awareness that may affect protective operations. OSB staff will identify behaviors of interest toward Secret Service protectees to assist in mitigating the risk of unwanted outcomes toward protected entities. Further, OSB will continue to identify groups that have demonstrated the potential for engaging in activities that may affect protective operations negatively.

Although the posture, capabilities, and functionality of OSB have not changed markedly in the last year, the Secret Service understands that the volume of information available will continue to rise and that urgent, unexpected, and time-sensitive circumstances will continue to increase investigative workloads that tax operational personnel. Therefore, the Secret Service will continue to address staffing needs and resources for OSB.

V. List of Abbreviations

Abbreviation	Definition
DHS	Department of Homeland Security
FY	Fiscal Year
OSB	Open Source Intelligence Branch
PID	Protective Intelligence and Assessment Division
Secret Service	U.S. Secret Service
U.S.C.	U.S. Code
USSS	U.S. Secret Service