UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Review of the Events Surrounding the January 6, 2021, Takeover of the U.S. Capitol

Flash Report: Counter-Surveillance and Threat Assessment

Investigative Number 2021-I-0003-C

April 2021

~~**Report Restriction Language**~~

~~**Distribution of this Document is Restricted**~~

~~This report may contain sensitive law enforcement information and/or is part of the deliberative process privilege. This is the property of the Office of Inspector General and is intended solely for the official use of the United States Capitol Police, the Capitol Police Board, or any agency or organization receiving the report directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the United States Capitol Police or the Capitol Police Board, by them or by other agencies or organizations, without prior authorization by the Inspector General or the Capitol Police Board.~~

UNITED STATES CAPITOL POLICE
WASHINGTON, DC 20003

INSPECTOR GENERAL

PREFACE

The Office of Inspector General (OIG) prepared this report pursuant to the Inspector General Act of 1978, as amended. It is one of a series of audits, reviews, and investigative and special reports OIG prepares periodically as part of its oversight responsibility with respect to the United States Capitol Police (USCP) to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the office or function under review. Our work was based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

We developed our recommendations based on the best knowledge available to OIG. Because this is a flash report, we did not discuss the draft findings with those responsible for implementation. It is my hope that the recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to those contributing to the preparation of this report.

Michael A. Bolton
Inspector General

TABLE OF CONTENTS

Abbreviations and Acronyms

[redacted]	[redacted]
Federal Bureau of Investigation	FBI
Full-Time Employee	FTE
Intelligence and Interagency Coordination Division	IICD
Intelligence Operations Section	IOS
Investigations Division	ID
Office of Inspector General	OIG
Protective Services Bureau	PSB
Standard Operating Procedure	SOP
Task Force Officer	TFO
Threat Assessment Section	TAS
United States Capitol Police	USCP or Department
United States Secret Service	USSS

EXECUTIVE SUMMARY

On January 6, 2021, a physical breach of U.S. Capitol Building security occurred during a Joint Session of Congress to certify the Electoral College vote. [redacted]

In accordance with our statutory authority Public Law (P.L.) 109-55, the USCP Office of Inspector General (OIG) began a review of the events surrounding the takeover of the U.S. Capitol on January 6, 2021. Our objectives for this review were to determine if the Department (1) established adequate measures for ensuring the safety and security of the Capitol Complex as well as Members of Congress, (2) established adequate internal controls and processes for ensuring compliance with Department policies, and (3) complied with applicable policies and procedures as well as applicable laws and regulations. The scope included controls, processes, and operations surrounding the security measures prior to the planned demonstrations and response during the takeover of the Capitol building.

Based on ongoing work, this flash report is designed to communicate any deficiencies with the Department's counter-surveillance and threat assessment operations. Deficiencies included (a) outdated or vague guidance, (b) failure to adequately report stop or contact activities, (c) lack of a dedicated counter-surveillance entity, (d) insufficient resources for supporting counter-surveillance operations, and (e) inadequate resources for supporting its Threat Assessment Section (TAS).

The Department did not have adequately detailed and up-to-date guidance in place for its counter-surveillance and threat assessment operations, which could have led to unclear guidance and accountability. Additionally, a lack of clear and detailed communication procedures could have increased inefficiencies with processes as well as led to critical counter-surveillance information not being appropriately communicated throughout the Department. Furthermore, the Department did not adequately document, collect, and analyze [redacted], which may have impeded its ability to identify trends or patterns that warranted further investigation or dissemination.

A stand-alone entity, with a defined mission dedicated to counter-surveillance activities in support of protecting the Congressional Community, would improve the Department's ability to identify and disrupt individuals or groups intent on engaging in illegal activity directed at the Congressional Community and its legislative process. The entity should be sufficiently staffed to accomplish its mission and have adequate resources, including dedicated analyst support and a central desk to exploit, investigate, disseminate, and triage information in real time.

The number of threat cases has significantly increased in the last 5 years. Although the Department has increased the number of Full-Time Employees (FTEs) within TAS, the section has experienced issues because of the increase of threats cases. Because its caseload continues to increase, TAS has been requiring more resources to keep pace with demand without sacrificing quality. [redacted]

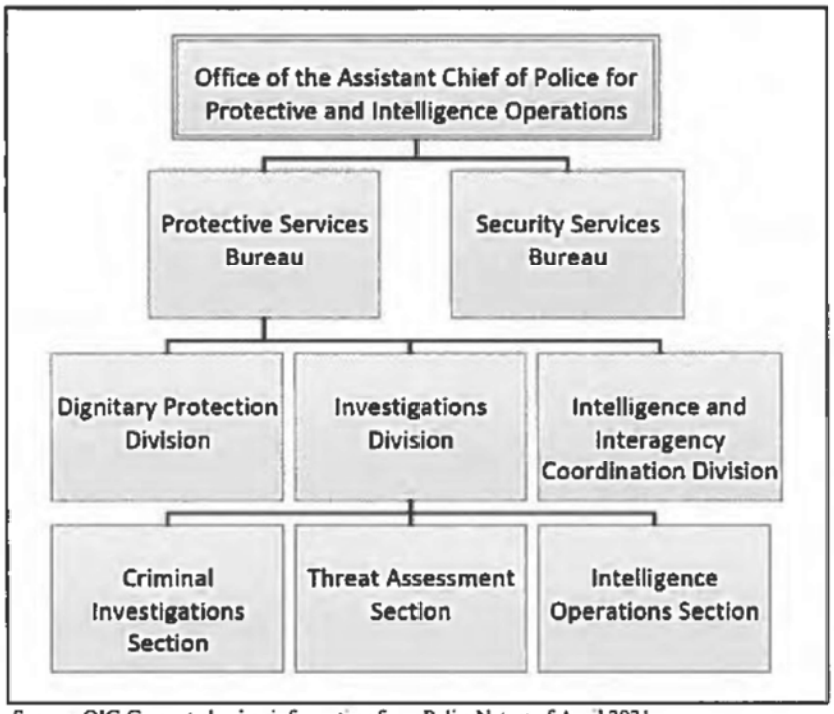
This is the third in a series of flash reports OIG will produce as part of the ongoing review of the events surrounding the takeover of the U.S. Capitol on January 6, 2021. Therefore, we may still perform additional, in-depth work related to these areas during our review. We anticipate that our next flash report will focus on the Department's Containment Emergency Response Team and First Responders Unit.

BACKGROUND

On January 6, 2021, a physical breach of U.S. Capitol security occurred during a Joint Session of Congress to certify the Electoral College vote. [redacted]

As shown in Exhibit 1, the Department's Protective Services Bureau (PSB) is one of two operational bureaus reporting to the Assistant Chief of Police for Protective and Intelligence Operations. PSB has a Dignitary Protection Division, Investigations Division (ID), and Intelligence and Interagency Coordination Division (IICD). ID has three sections: the Criminal Investigations Section, Intelligence Operations Section (IOS), and Threat Assessment Section (TAS).

Exhibit 1 – Chain of Command



Source: OIG Generated using information from PoliceNet as of April 2021.

IOS is primarily responsible for USCP counter-surveillance operations. PoliceNet states that IOS:

[redacted]

- Provides an investigative response to identified or reported suspicious activity to determine any nexus to terrorism or other criminal activity.
- Conducts protective intelligence operations to support Department operations related to Member Protection, Threat Assessment, and Intelligence Collection.
- Coordinates law enforcement operations with local, state and federal law enforcement agencies to support Congressional events and/or serve as a liaison for a wide spectrum of issues that impact USCP interests.

According to the IOS *Executive Summary* for January 6, 2021, IOS staffing had [redacted] Sergeants and [redacted] of which were detailed to [redacted] On January 6, 2021, IOS scheduled [redacted] Agents to deploy on or around the Capitol Grounds, as shown in Table 1.

Table 1 – January 6, 2021, IOS Scheduled Deployment

Shift	*Agents*
[redacted]	

Source: OIG Generated from IOS *Executive Summary* for January 6, 2021.

An ID official stated that Sergeants sometimes supplement counter surveillance teams to either complete or enhance a team as needed. IOS scheduled [redacted] Sergeants to be on or around the Capitol Grounds on January 6, 2021— [redacted] Our work revealed that [redacted] was in the field conducting counter-surveillance. According to an ID official, counter-surveillance teams generally consist of [redacted] agents who are [redacted] Our work revealed that on January 6, 2021, [redacted]

PoliceNet states that TAS is responsible for (1) identifying individuals who inappropriately communicate, contact, or threaten USCP protectees; (2) assessing those individuals for the level of potential danger; and (3) managing individuals TAS determines dangerous to USCP protectees. USCP and FBI each have authority to investigate threats against Members of Congress, officers of Congress, and members of their families. USCP receives its authority through section 1966, title 2, United States Code (2 U.S.C. 1966). The FBI receives its authority through 18 U.S.C. 351 as well as Department of Justice authorization to investigate threats against Federal officials pursuant to title 18 of the United States Code.

In a previous report, Investigative Number 2020-I-0006, *Assessment of the United States Capitol Police Threat Assessment Section,* dated September 2020, OIG found TAS caseloads steadily increased from the beginning of calendar year 2017 through the end of 2019. Department officials and TAS Agents stated that increased caseloads as well as staffing levels were some of the greatest challenges for TAS. TAS did not have Investigative Analysts, and TAS agents performed tasks, such as database checks, that Investigative Analysts performed at other agencies. OIG found allowing Investigative Analysts to assume some responsibilities from agents would help TAS maintain a manageable caseload for its staff.

OBJECTIVE, SCOPE, AND METHODOLOGY

In accordance with our statutory authority Public Law (P.L.) 109-55, the USCP Office of Inspector General (OIG) began a review of the events surrounding the takeover of the U.S. Capitol on January 6, 2021. Our objectives were to determine if the Department (1) established

adequate measures for ensuring the safety and security of the U.S. Capitol Complex as well as Members of Congress, (2) established adequate internal controls and processes for ensuring compliance with Department policies, and (3) complied with applicable policies and procedures as well as applicable laws and regulations. The scope of this review included controls, processes, and operations surrounding security measures prior to the planned demonstrations and response during the takeover of the U.S. Capitol. Based on this ongoing work, we produced this flash report to communicate deficiencies with the Department's operational planning and intelligence for planned demonstrations on January 6, 2021.

Our work included interviews with Department officials. We also reviewed documentation related to the Department's counter-surveillance and threat assessment operations on or around January 6, 2021. Additionally, we researched Department guidance related to counter-surveillance and threat assessments. To research best practices, OIG consulted with a former Deputy Assistant Director for Special Intelligence and Information for the U.S. Secret Service (USSS) and a former FBI Unit Chief. Furthermore, we reviewed Report Number 2020-I-0006 as well as correspondence between OIG and USCP related to closure of the recommendations in the report.

This flash report is based upon work conducted in Washington, D.C., from March through April 2021. We did not conduct an audit, the objective of which would be the expression of an opinion on Department programs. Accordingly, we did not express such an opinion. Had we performed additional procedures, other issues might have come to our attention that we would have reported. ~~This report is intended solely for the information and use of the Department, the Capitol Police Board, and the USCP Oversight Committees and should not be used by anyone other than the specified parties.~~

This is the third in a series of flash reports OIG will produce as part of our ongoing review of the events surrounding the takeover of the U.S. Capitol on January 6, 2021. Therefore, we may still perform additional, in-depth work related to these areas during our review. We anticipate that our next flash report will focus on the Department's Containment Emergency Response Team and First Responders Unit.

RESULTS

We produced this flash report to communicate deficiencies with the Department's counter-surveillance and threat assessment operations. Deficiencies included (a) outdated or vague guidance, (b) failure to adequately report stop or contact activities, (c) lack of a dedicated counter-surveillance entity, (d) insufficient resources for supporting counter-surveillance operations, and (e) inadequate resources for supporting TAS.

Policies and Procedures

Some policies and procedures related to TAS and IOS were outdated or vague. On January 6, 2021, sworn employees did not adequately report stop or contact activities using the [redacted] report as guidance requires.

Outdated Counter-Surveillance & Threats Policies and Procedures

USCP did not have up-to-date policies and procedures related to TAS and IOS. Specifically, the Department last updated the following Standard Operating Procedures (SOPs) in 2009 and 2010:

- SOP [redacted] dated March 31, 2009
- SOP [redacted] dated March 31, 2009
- SOP [redacted] dated July 7, 2009
- SOP [redacted] November 20, 2009
- SOP [redacted] dated July 7, 2009
- SOP [redacted], dated May 26, 2010

Many of the policies include outdated information. For example, many of the SOPs refer to the Intelligence Section – Investigative, which is now IOS. Additionally, [redacted] states that "ID Command will establish communication reporting requirements to include BlackBerry distribution lists." The Department has not used BlackBerry devices for several years.

Since January 6, 2021, USCP has updated or removed some other ID SOPs from PoliceNet; therefore, we will not make any recommendations related to those SOPs.

The Department did not have adequate, updated SOPs in place for TAS and IOS. The lack of up-to-date policies and procedures for TAS and IOS could have not only created ambiguity and lack of accountability and coordination for Department personnel but also impeded the effectiveness of the units.

Vague Threats and Counter-Surveillance Policies

USCP policies and procedures related to TAS and IOS are vague. For example, SOP [redacted], dated July 7, 2009, fails to provide sufficient details for completing and monitoring daily reports. For example, the SOP states that the "Section Command will maintain situational awareness on known events that may have a

criminal impact associated with such events. This is to be accomplished by monitoring daily reports completed by the Office of Intelligence Analysis." However, the SOP does not detail what information or what type of events are to be identified in these daily reports.

In addition, SOP [redacted] dated July 7, 2009, requires that supervisors review and forward monthly reports from detailed agents. However, that policy merely states that the agents must maintain routine contact with their supervisor and does not specify monthly reporting. We selected 6 months from Fiscal Year 2018 through March 31, 2021, and requested the monthly reports for the [redacted] task forces with detailed USCP Agents, for a total of [redacted] reports. The Department could not provide reports for one of those months, and could only provide [redacted] reports. Of the [redacted] reports the Department provided, [redacted] included an email evidencing the agent detailee sent the report to the supervisor. The Department could not provide any evidence that a supervisor reviewed or forwarded any of the reports.

Furthermore, the Department did not have an SOP adequately detailing the procedure for Counter-Surveillance agents to communicate information through the chain of command. According to one department official, [redacted] While it is standard practice for Counter-Surveillance Agents in the field to communicate [redacted] no formal SOP exists that communicates such a procedure and the details required to be communicated. Furthermore, USCP lacks a policy outlining how information received from counter-surveillance teams should be elevated and communicated throughout the Department.

Finally, although it has informal standards for TAS and IOS training, the Department did not document those standards in formal policies. For example, officers complete Federal Law Enforcement Training Center and USCP basic and advanced courses. The Department does not however, have a written SOP or Directive requiring completion of those courses.

The Department did not have adequately detailed SOPs in place for TAS and IOS. Lack of detailed policies and procedures for TAS and IOS could have created ambiguity that may have affected accountability. In addition, lack of clear and detailed communication procedures could have increased inefficiencies and may have led to critical counter-surveillance information not having been communicated throughout the Department.

Inadequate [redacted] Stop or Contact Reporting and Collection

Sworn employees in the Department did not adequately report "stop or contact" activities using the [redacted] on January 6, 2021, as Directive [redacted], [redacted] dated May 28, 2012, and SOP [redacted] dated November 20, 2009, require.

The Department provided a total of four [redacted] reports for January 6, 2021. [redacted] In the days leading up to January 6, the Department had six [redacted]—two for January 4 and four for January 5. We reviewed radio communications for the morning of January 6 and noted a number of instances in which officers stopped or contacted individuals. The Department did not, however, document those occurrences on a [redacted]

The Department did not adequately document, collect, and analyze [redacted] reports. Such reports are important and when sworn officers do not sufficiently record that type of information, it impedes the ability of analysts to identify trends or patterns, and supervisors to disseminate potentially crucial information to other bureaus. This may impede the Department's ability to identify a trend or pattern that warrants further investigation or dissemination.

Conclusions

The Department did not have adequately detailed and updated SOPs in place for TAS and IOS, which could have created ambiguity and a lack of accountability. Additionally, a lack of clear and detailed communication procedures could have increased process inefficiencies and led to critical counter-surveillance information not being communicated throughout the Department. Furthermore, the Department did not adequately document, collect, and analyze [redacted] reports, which may have impeded its ability to identify important trends or patterns that warranted further investigation or dissemination. Therefore, OIG makes the following recommendations.

Recommendation 1: We recommend that the United States Capitol Police update the following standard operating procedures to reflect current practices: (a) Standard Operating Procedure [redacted] dated March 31, 2009; (b) Standard Operating Procedure [redacted] dated March 31, 2009; (c) Standard Operating Procedure [redacted] dated July 7, 2009; (d) Standard Operating Procedure [redacted] 2009; (e) Standard Operating Procedure [redacted] dated July 7, 2009; and (f) Standard Operating Procedure [redacted] dated May 26, 2010.

Recommendation 2: We recommend that the United States Capitol Police establish a formal policy detailing communication procedures for Counter-Surveillance Agents including how and what detailed information is communicated through the chain of command and throughout the Department.

Recommendation 3: **We recommend that the United States Capitol Police establish a formal policy detailing basic and advanced training requirements for the Threat Assessment Section and Intelligence Operations Section.**

Recommendation 4: **We recommend that the United States Capitol Police enforce its policies regarding completion of form [redacted] for stops or contacts officers initiate.**

Counter-Surveillance

USCP did not have a stand-alone entity dedicated to counter-surveillance or adequate resources dedicated to supporting the analysis and communication of counter-surveillance information.

Lack of a Dedicated Counter-Surveillance Entity

USCP did not have a stand-alone entity dedicated to counter-surveillance [redacted] However, IOS is also responsible for providing an investigative response for suspicious activities, conducting protective intelligence operations to support Member Protection, and coordinating law enforcement operations with local, state and Federal law enforcement agencies supporting Congressional events and/or travel.

An official in ID stated that the various assignments for IOS make it tough for it to have a focused mission and suggested that the Department should have a stand-alone entity similar to that of USSS dedicated to counter-surveillance. According to that official, the rotation of IOS agents between counter-surveillance and collateral assignments does not allow for any consistency and makes it difficult for agents to get a baseline for counter-surveillance observations. [redacted]

On January 6, 2021, IOS collateral duties impacted counter-surveillance coverage. An official in ID stated that IOS plans "got blown to shreds" after the discovery of the hazardous devices and that the discovery distracted IOS. Our work revealed that after the discovery of the hazardous devices, IOS resources and commanders were mainly focused on the response and investigation of those scenes and that [redacted] appeared to be still providing coverage to the Capitol Grounds. A stand-alone entity with a defined mission dedicated to counter-surveillance activities in support of protecting the Congressional Community adequately

staffed to accomplish its mission would improve the Department's ability to identify and disrupt individuals or groups intent on engaging in illegal activity directed at the Congressional Community and its legislative process.

Lack of Resources to Support Counter-Surveillance Operations

ID officials stated that increasing workloads and staffing levels are some of the greatest challenges for IOS. One official stated that in general IOS does not have enough agents to cover all its assignments correctly and assigning analysts to IOS as support staff would reduce workload for the agents. The same official also stated that although IOS maintains a log of observations in the Department's case management system it does not have any analysts available to interpret the data. Our work revealed that on January 6, 2021, counter-surveillance agents had other agents and an IICD official responding to requests for criminal history and social media checks, which are tasks that could have been completed by dedicated counter-surveillance analysts.

In Report Number 2020-I-0006, OIG reported that allowing Investigative Analysts to assume certain responsibilities from agents, similar to agencies such as FBI and USSS, would assist the Department in maintaining a manageable caseload for its staff and allow agents to focus more on other investigative responsibilities. Our research into best practices revealed that the USSS Protective Intelligence & Assessment Division had an analyst-to-agent ratio of around [redacted] for its threat management resources and had a "Suspicious Activity Reports Desk" that supported the USSS Counter-Surveillance Division.

On January 6, 2021, a lack of supporting resources affected the ability of IOS to effectively communicate information. Our work revealed that IOS agents emailed information to individuals, distribution lists, and certain leaders without the opportunity to unify and synthesize the information. That left IOS agents questioning if information had been received and/or triaged. Counter-surveillance activities should have a central desk for exploiting, investigating, disseminating, and triaging information in real time. The central desk should be staffed with analysts, agents, and officers from the Department and should have a dedicated commander whose focus is on that process and providing guidance and direction to agents in the field.

Conclusions

A stand-alone entity, with a defined mission dedicated to counter-surveillance activities in support of protecting the Congressional Community adequately staffed to accomplish its mission and with adequate supporting resources would improve the Department's ability to identify and disrupt individuals or groups intent on engaging in illegal activity directed at the Congressional Community and its legislative process. Thus, OIG makes the following recommendations.

Recommendation 5: We recommend the United States Capitol Police establish a stand-alone entity with a defined mission dedicated to counter-surveillance activities in support of protecting the Congressional Community and that is adequately staffed to accomplish its mission.

Recommendation 6: We recommend the United States Capitol Police use Investigative Analysts to augment its counter-surveillance resources.

Recommendation 7: We recommend the United States Capitol Police establish a central desk staffed with analysts, agents, and officers that can exploit, investigate, disseminate and triage information for counter-surveillance activities in real time. The desk should have a dedicated commander whose focus is on that process and providing guidance and direction to agents in the field.

Threat Assessment Section

As part of our on-going work, OIG conducted a follow-up analysis of the Department's implementation of recommendations contained in Report Number 2020-I-0006 to confirm the Department took the corrective actions in implementing the recommendations. Based on our follow-up, a condition identified in the previous report reemerged. Because TAS's caseload has been steadily increasing, more resources are needed to keep up with the demand without sacrificing quality.

Status of Previous Recommendations

In Report Number 2020-I-0006, OIG found that TAS caseloads steadily increased from the beginning of calendar year 2017 through the end of 2019. Department officials and TAS Agents stated that the increasing caseload as well as staffing levels were some of the greatest challenges for TAS. TAS did not have Investigative Analysts and TAS Agents performed tasks such as database checks—tasks that Investigative Analysts perform at other agencies. OIG found allowing Investigative Analysts to assume some responsibilities from agents would help TAS maintain a manageable caseload for its staff.

As part of our on-going work, OIG conducted a follow-up analysis of the Department's implementation of recommendations contained in Report Number 2020-I-0006 to confirm the Department took the corrective actions in implementing the recommendations. Based on our follow-up, a condition identified in the previous report reemerged. Because of the growing number of TAS cases, a Department official stated more Investigative Analysts are needed to augment the staff. See the prior recommendations along with their status below:

Previous Recommendation 1: We recommend the United States Capitol Police continue to consider and pursue a regional approach for managing threats against protectees.

According to Department responses to recommendations in Report Number 2020-I-0006, the Department moved forward with that concept and received approval from the Capitol Police Board for its request for enhancements for protective intelligence services outside the National Capital Region.

Department officials stated they were in the selection phase to staff agents at two Fusion Centers—one located in San Francisco, California and one in Tampa Bay, Florida.

Previous Recommendation 2: We recommend the United States Capitol Police consider using Investigative Analysts to augment its threat management resources.

According to Department responses to recommendations in Report Number 2020-I-0006, the Department had a vacancy posted for an additional Intelligence Research Specialist that would enhance its ability to assist with intelligence analysis and investigative analysis that is afforded to TAS.

The Department did not, however, have an adequate number of Investigative Analysts to assume certain responsibilities from TAS Agents. Additional analysts could have assisted TAS in managing an ever-increasing caseload for its staff. OIG confirmed with a Department official within TAS that [redacted] hired and staffed within the section. Although [redacted] is currently used by the section, threat-related cases are continuing to increase. The official stated that TAS is still experiencing issues associated with human capital resources as cases increase. See new recommendation.

Previous Recommendation 3: We recommend the United States Capitol Police ensure documentation in the official system of record all training staff members of the Threat Assessment Section staff receive.

According to Department responses to recommendations in Report Number 2020-I-0006, on October 1, 2020, the Department implemented its official training of record management tool, APEX. The responses state that the internal and external training TAS investigators receive is now tracked and logged in APEX.

OIG confirmed with a Department official within TAS that its official training of record management tool is APEX. Additionally, the Department provided two transcripts demonstrating that training was uploaded and logged.

<u>Previous Recommendation 4:</u> We recommend the United States Capitol Police implement updated policies and procedures for its Threat Assessment Section that effectively communicate current Threat Assessment Section investigative procedures.

According to Department responses to recommendations in Report Number 2020-I-0006, PSB completed its review of the policies for TAS and all policies were published and implemented.

OIG obtained and reviewed the following SOPs: [redacted] dated December 17, 2020; [redacted] dated March 12, 2021; [redacted] dated December 17, 2020; [redacted] dated January 28, 2021; and [redacted] dated March 12, 2021. The Department completed its review of policies for TAS that effectively communicate current TAS Investigative Procedures.

Lack of Resources to Support the Threats Assessment Section

As of March 31, 2021, TAS was staffed with [redacted] Special Agents and [redacted] A Department official stated that the Department increased Full-Time Employees (FTEs) for TAS, but the section needed more personnel to properly address the growing number of cases. As previously provided, Department officials and TAS Agents stated that increasing caseloads and staffing levels have been some of the greatest challenges for TAS. According to statistics one Department official provided, Threat[1] and Direction of Interest[2] cases have risen since 2017, as shown in Table 2.

[1] SOP [redacted] December 17, 2020, defines a threat as "a communication or action showing clear or implied intent to inflict physical, psychological, or other harm."

[2] SOP [redacted] December 17, 2020, defines a Direction of Interest as "information received by the USCP from any source where a subject expresses an unusual interest in any person or property under USCP jurisdiction. A direction of interest can also be information received by USCP that could be considered a threat; however, it is not directed against any person or property under the jurisdiction of the USCP (for example, information regarding the Secretary of State, the President, the Vice President, etc.)."

Table 2 – TAS Statistics Calendar Years 2017 through March 31, 2021

Category	Calendar Year				
	2017	2018	2019	2020	2021* (As of March 31, 2021)
Threat Cases	171	312	383	585	213
Direction of Interest Cases	3,768	4,894	6,572	8,778	3,021
Threat Cases Closed by Arrest	29	33	51	57	23

Source: OIG Generated from data provided by PSB

According to a Department official, the average time for investigating a low-level Direction of Interest case that includes database checks and case entry varies depending on the personnel but averages between [redacted] TAS requires more time to conduct a more thorough investigation, with corroborative interviews and an adequate threat assessment. The Department official stated that as of March 31, 2021, each TAS agent averages approximately 500 cases per year, but that the caseload for each agent should be closer to 100 cases for each Agent to complete a thorough and comprehensive threat investigation. The official also voiced concerns involving the quality of investigations because of the extensive increase of cases that additional TAS Agents and Investigative Analysts would be able to help mitigate. With [redacted] TAS has limited resources for its agents. Research into best practices revealed that USSS had an analyst-to-agent ratio of around [redacted] for threat management resources. Allowing Investigative Analysts to assume certain responsibilities from TAS Agents would assist TAS in maintaining a manageable caseload for its staff and allow its agents to focus more on other investigative responsibilities, such as conducting interviews.

As of March 31, 2021, there were [redacted] TAS Agents classified as Task Force Officers (TFOs). Of those agents, [redacted] one is [redacted] TFOs assigned to those task forces offer the Department additional resources from their respective partnering agency.

[redacted]

The Department's TFO participates full time in the [redacted] which includes many other Federal and state law enforcement agencies. [redacted] The [redacted] consults on cases; they do not prosecute them.

The [redacted] profilers on the task force receive extensive training. [redacted] The USCP TAS representative on the [redacted] has successfully completed both phases of the training and is a certified profiler.

[redacted] profiles the highest priority cases referred to it by the various law enforcement agencies. [redacted] Although it has provided support in the past, the [redacted] Unit Chief stated that the Department does not provide a lot of subjects to [redacted] for profiling. [redacted] The Unit Chief is aware of USCP's enormous volume of cases and advised that as of March 31, 2021, [redacted] could have the capacity to increase its level of support to USCP, if requested.

The USCP TAS representative on the [redacted] stated that the profiles [redacted] provides offer great investigative insights into the threat cases. [redacted] Because [redacted] is a force multiplier and does not cost the Department additional resources to present it more threat cases, we recommend the USCP consider increasing the number of cases it sends [redacted] to help TAS obtain better investigative insights on the highest priority cases contained within its large case load.

Conclusions

During the review, a condition identified in a previous report—the need for Investigative Analysts to augment TAS staff—reemerged. The number of threat cases has significantly increased in the last 5 years. Although the Department has increased the number of FTEs within TAS, the section continues to experience issues because of the immense increase of threats cases. Because the TAS caseload is increasing, more resources are needed to keep up with the demand without sacrificing quality. Therefore, OIG makes the following recommendations.

Recommendation 8: We recommend the United States Capitol Police increase the number of Threat Assessment Agents as the caseload increase.

Recommendation 9: **We recommend the United States Capitol Police use Investigative Analysts to augment its Threat Assessment Section at an analyst-to-agent ratio comparable to its partnering agencies.**

Recommendation 10: **We recommend the United States Capitol Police consider providing more of their highest priority threat cases to the [redacted] for in-depth analysis of their priority subjects.**

CONTACTING THE OFFICE OF INSPECTOR GENERAL

Success of the OIG mission to prevent fraud, waste, abuse, or mismanagement depends on the cooperation of employees and the public. There are several ways to report questionable activity.

Call us at 202-593-3868 or toll-free at 866-906-2446. A confidential or anonymous message can be left 24 hours a day/7 days a week.

Toll-Free
1-866-906-2446

Write us – we are located at:
United States Capitol Police
Attn: Office of Inspector General, Investigations
119 D Street, NE
Washington, DC 20510

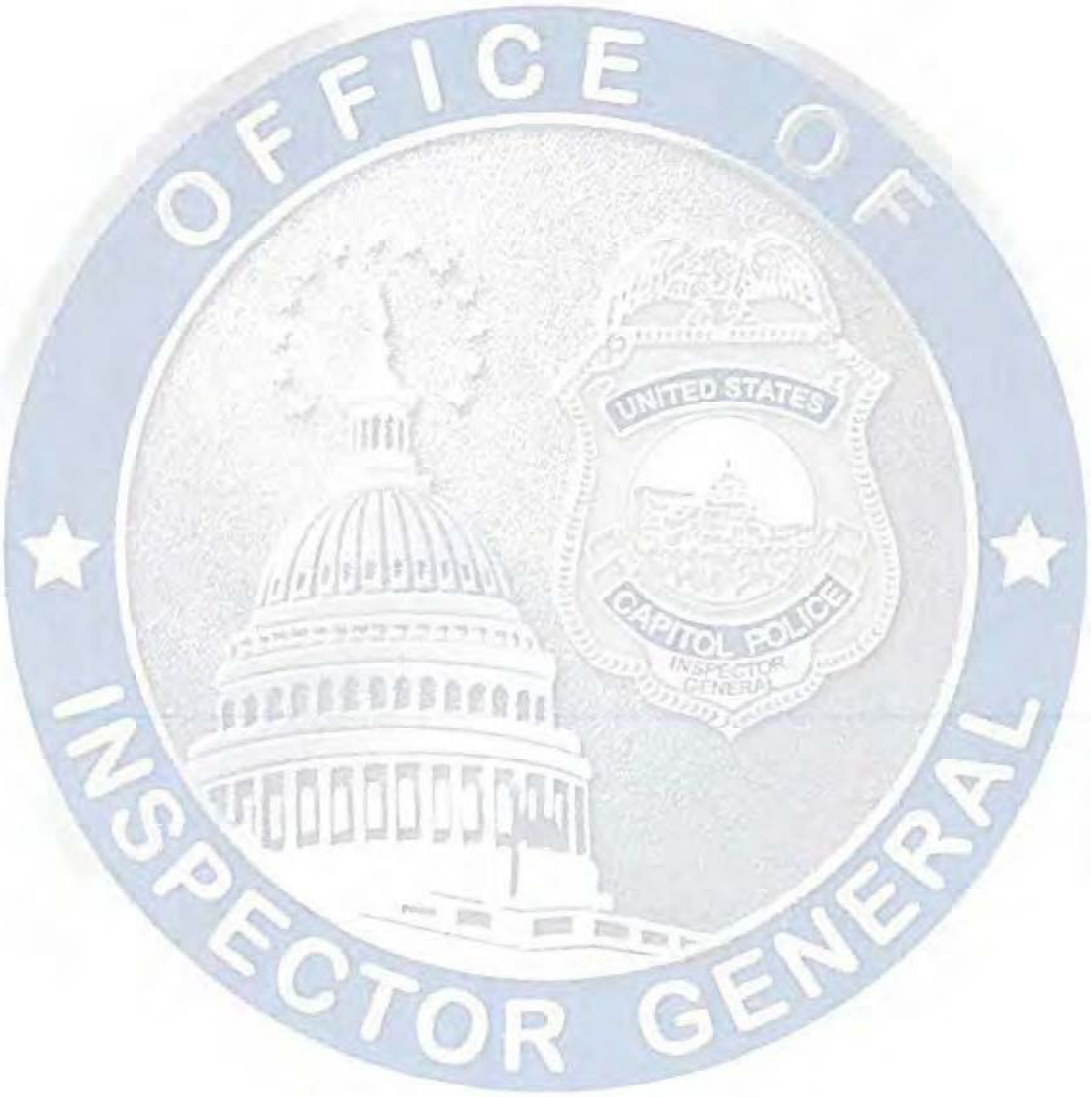
Or visit us – we are located at:
499 South Capitol Street, SW, Suite 345
Washington, DC 20003

You can also contact us by email at: OIG@USCP.GOV

When making a report, convey as much information as possible such as:
Who? What? Where? When? Why? Complaints may be made anonymously or you may request confidentiality.

Additional Information and Copies:

To obtain additional copies of this report, call OIG at 202-593-4201.


OFFICE OF
INSPECTOR GENERAL
UNITED STATES
CAPITOL POLICE
INSPECTOR GENERAL