



UNITED STATES CAPITOL POLICE OFFICE OF INSPECTOR GENERAL

Assessment of the United States Capitol Police Threat Assessment Section

Investigative Number 2020-I-0006

September 2020

~~**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 and discussed 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.



A handwritten signature in black ink, which appears to read "M. A. Bolton", is positioned above the printed name.

Michael A. Bolton
Inspector General

TABLE OF CONTENTS

	<u>Page</u>
Abbreviations and Acronyms	ii
Executive Summary	1
Background	2
Objective, Scope, and Methodology	3
Results	4
Appendices	11
Appendix A – List of Recommendations	12
Appendix B – Department Comments	13

Abbreviations and Acronyms

Assistant United States Attorney	AUSA
Federal Bureau of Investigation	FBI
Federal Law Enforcement Training Center	FLETC
Government Accountability Office	GAO
Investigations Division	ID
National Capital Region	NCR
Office of Inspector General	OIG
Protective Intelligence & Assessment Division	PID
Protective Services Bureau	PSB
Standard Operating Procedure	SOP
Threat Assessment Section	TAS
Training Management System	TMS
United States Capitol Police	USCP or Department
United States Secret Service	USSS
	

EXECUTIVE SUMMARY

Section 1966, title 2, United States Code (2 U.S.C. 1966) authorizes the United States Capitol Police (USCP or Department) to investigate threats against Members of Congress, officers of Congress, and members of their families. According to PoliceNet,¹ the USCP Threat Assessment Section (TAS) is responsible for (1) identifying individuals who inappropriately communicate, contact, or threaten USCP protectees; (2) assessing those individuals for the potential level of danger; and (3) managing those individuals TAS has determined to be dangerous to USCP protectees.

In accordance with our annual plan, the Office of Inspector General (OIG) assessed TAS to determine if (1) the organizational structure and training for the Department's management of threats against protectees was the most efficient and effective and (2) the Department complied with applicable policies and procedures as well as applicable laws, regulations, and best practices. Our scope included the TAS organizational structure, training, processes, and operations during Fiscal Years 2019 and 2020.

Changes to the organizational structure would improve the efficiency and effectiveness of the Department's management of threats against protectees. The TAS staff members are based in the National Capital Region (NCR), but the majority of TAS cases were generated by incidents outside of the NCR. As a result, TAS must rely on assistance from Federal and local partner agencies to complete many of its cases. In response, the Department has been considering changing to a regional approach for threat management by creating and assigning TAS agents to Regional Field Offices. A regional approach for threat management would give TAS more control over its cases, allow opportunity for more thorough investigative work, and give TAS more opportunity to develop relationships with partner entities.

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 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 perform at other agencies. Allowing investigative analysts to assume some responsibilities from agents would help TAS maintain a manageable caseload for its staff.

TAS agents receive from both external and internal sources basic and advanced training related to criminal investigations and threat assessments. The training was not, however, always documented in the Department's official system of record as USCP Directive [REDACTED]

¹ PoliceNet is the Department's intranet.

[REDACTED], dated February 14, 2019, requires. Additionally, guidance specific to TAS was outdated and did not reflect changes with its processes over time.

The Department could have managed threats against protectees more efficiently and effectively with a regional approach to threat management and by using investigative analysts to augment TAS staffing. Additionally, the Department should ensure documentation of the training TAS staff members receive within its official system of record and implement updated guidance that effectively communicates TAS procedures. See Appendix A for a complete list of recommendations.

On September 1, 2020, we provided a draft report to the Department for comment and attached the response in its entirety in Appendix B.

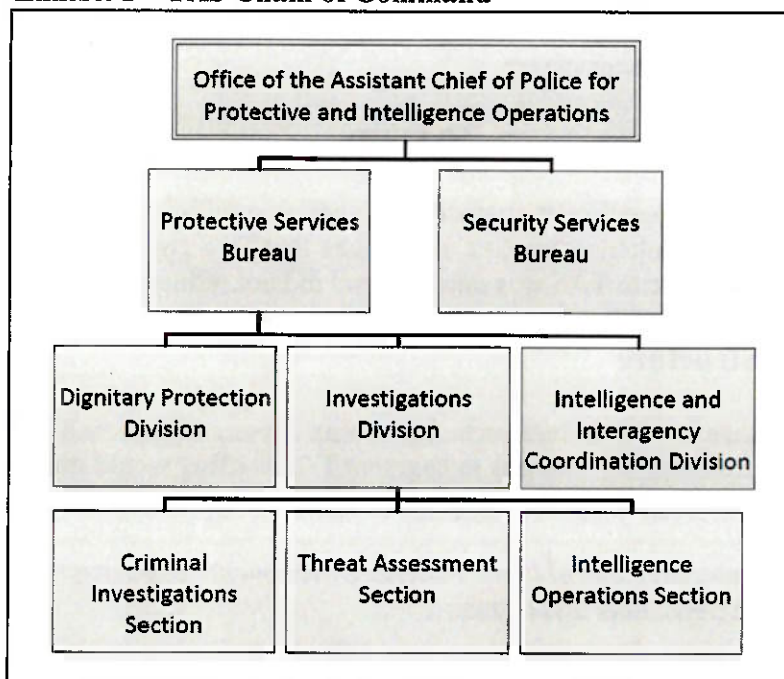
BACKGROUND

The United States Capitol Police (USCP or Department) and Federal Bureau of Investigation (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.

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. According to PoliceNet,² PSB's mission is "provide safety and security to the Capitol, Members of Congress, Officers of Congress, and their immediate family." PSB has a Dignitary Protection Division, Intelligence and Interagency Coordination Division, and Investigations Division (ID). ID has three sections: the Criminal Investigations Section, the Intelligence Operations Section, and the Threat Assessment Section (TAS). 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.

² PoliceNet is the Department's intranet.

Exhibit 1 – TAS Chain of Command



Source: OIG Generated using information from PoliceNet as of April 2020.

OBJECTIVE, SCOPE, AND METHODOLOGY

In accordance with our annual plan, the Office of Inspector General (OIG) assessed TAS to determine if (1) the organizational structure and training for the Department's management of threats against protectees was the most efficient and effective and (2) the Department complied with applicable policies and procedures as well as applicable laws, regulations and best practices. Our scope included the TAS organizational structure, training, processes, and operations throughout Fiscal Years 2019 and 2020.

To accomplish our objectives, we interviewed Department officials and TAS agents. We also reviewed documentation related to TAS training and operations as well as policies and procedures related to TAS including those in draft form. Additionally, we reviewed a sample of TAS case files to gain an understanding of procedures. To research best practices, OIG interviewed a representative from the United States Secret Service (USSS) regarding the organization of its threat management resources, reviewed FBI threat case summaries, and reviewed guidance from the Government Accountability Office (GAO).

OIG conducted this assessment in Washington, D.C., from March through August 2020. 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 (Board), and the USCP Oversight Committees and should not be used by anyone other than the specified parties.~~

RESULTS

The Department could manage threats against protectees more efficiently and effectively if it made changes to its organizational structure and require that TAS consistently comply with guidance. Guidance specific to TAS was outdated and did not reflect changes with its processes.

Organizational Structure

Changes to the organizational structure such as pursuing a regional approach to the management of threats and using investigative analysts to augment TAS staffing would improve the efficiency and effectiveness of the Department's management of threats against protectees.

GAO Standards for Internal Control in the Federal Government; Organizational Structure, GAO-14-704G, dated September 2014, state:

Management develops an organizational structure with an understanding of the overall responsibilities, and assigns these responsibilities to discrete units to enable the organization to operate in an efficient and effective manner, comply with applicable laws and regulations, and reliably report quality information. Based on the nature of the assigned responsibility, management chooses the type and number of discrete units, such as divisions, offices, and related subunits.

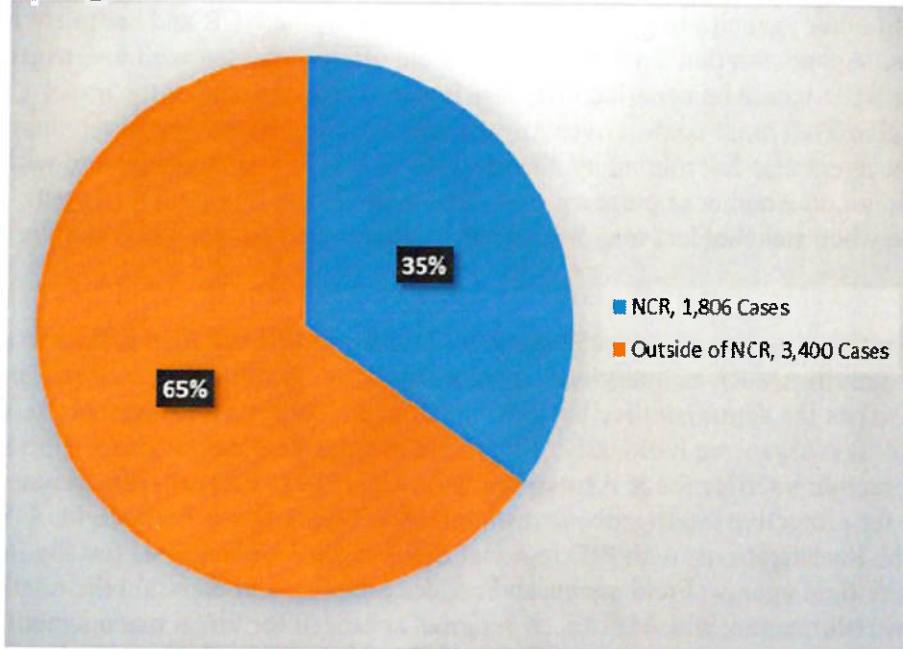
As part of establishing an organizational structure, management considers how units interact in order to fulfill their overall responsibilities. Management establishes reporting lines within an organizational structure so that units can communicate the quality information necessary for each unit to fulfill its overall responsibilities. Reporting lines are defined at all levels of the organization and provide methods of communication that can flow down, across, up, and around the structure. Management also considers the entity's overall responsibilities to external stakeholders and establishes reporting lines that allow the entity to both communicate and receive information from external stakeholders.

Management periodically evaluates the organizational structure so that it meets the entity's objectives and has adapted to any new objectives for the entity, such as a new law or regulation.

As of March 31, 2020, TAS had [REDACTED] Supervisory Special Agents, [REDACTED] Special Agents [REDACTED] the FBI

[REDACTED]

**Exhibit 2 – TAS Cases Generated During Calendar Year 2018
by Region**



Source: OIG Generated from data provided by a Department official.

In response, the Department is considering changing to a regional approach for threat management and district event protection by creating and assigning TAS agents to Regional Field Offices that would each have an area of responsibility. According to a draft USCP information paper titled [REDACTED]

[REDACTED], approximately 1,587 TAS cases involved subject interviews in calendar year 2019. The paper states that outside agencies assisting TAS conducted a majority of the interviews. The paper also states that

typically Federal and local police do not receive training in threat management and mainly focus on whether the subjects are an imminent threat to themselves or others. In addition, the paper states that more in-depth interviews would increase the Department's effectiveness in developing an accurate threat picture and risk assessment for a protectee.

Department officials and TAS agents stated that establishing field offices would benefit USCP by helping TAS build relationships with partner entities throughout the country, including Assistant U.S. Attorneys (AUSAs). OIG heard from agents that TAS must rely more and more on the FBI and other agencies to accomplish tasks outside of the NCR and complete its investigations. Agents felt that TAS establishing field offices to assist with investigations outside of the NCR would be beneficial because it would reduce some of the travel TAS agents must do and give TAS more control over its own investigations by having to rely less on other agencies. One agent also felt that many AUSAs look at USCP as an outsider and will defer to the FBI's opinion on whether to pursue a case. The agent stated this sometimes puts TAS in a difficult place when stakeholders may want them to continue to pursue a case but the FBI does not.

Our research into best practices revealed that both USSS and FBI use field offices to assist with investigative activities, such as interviews, outside the NCR. Additionally, our research revealed that USSS also has the administrative support functions for its threat management resources, such as duty desks, organized regionally. The threat management resources for USSS reside within its Protective Intelligence & Assessment Division (PID). PID provides guidance and coordination for protective intelligence investigations to USSS agents in the field. USSS Field Offices run the investigations, with PID regional desks (agents and analyst) serving in a support function for the field agents. Field agents and offices establish and maintain the relationships with local law enforcement and AUSAs. A regional approach for threat management would give TAS more control over its cases, allow opportunity for more thorough investigative work, and provide TAS with additional opportunities to develop relationships with partner entities.

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, Threat⁶ and Direction of Interest⁷ cases have risen in each of the last 3 calendar years, as shown in Table 1.

⁶ Draft Standard Operating Procedure [REDACTED], undated, defines a threat as "a communication or action showing clear or implied intent to inflict physical, psychological, or other harm."

⁷ Draft Standard Operating Procedure [REDACTED], undated, 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 1 – TAS Statistics Calendar Years 2017-2019

Category	Calendar Year		
	2017	2018	2019
Threat Cases	171	312	383
Direction of Interest Cases	3,768	4,894	6,572
Threat Cases Closed by Arrest	29	33	51

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 was [REDACTED]. TAS could, however, require up to [REDACTED] to conduct a more thorough investigation, with corroborative interviews and an adequate threat assessment. Assuming a constant level of [REDACTED] fully trained TAS agents, not assigned to task forces, throughout 2019, would result in a caseload of approximately [REDACTED] cases per agent during that year specifically.

One Department official stated that assigning investigative analysts to TAS would help address caseload and staffing challenges. That same official stated that although agencies such as USSS and FBI use analysts to perform a lot of initial case research such as database checks, TAS has its own agents performing those duties. The official stated that PSB has intelligence analysts in its Intelligence and Interagency Coordination Division but did not have any investigative analysts within ID. Our research into best practices revealed that USSS had an analyst-to-agent ratio of around [REDACTED] for its 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.

Conclusions

The Department could manage threats against protectees more efficiently and effectively with a regional approach to threat management. That change in organizational structure could reduce the Department's dependency on outside agencies in conducting critical aspects of its investigations. The priorities of the outside agencies may not align with the protective priorities of the Department and its stakeholders. Additionally, allowing investigative analysts to assume certain responsibilities from TAS agents would assist TAS in maintaining a manageable caseload for its staff. Thus, OIG makes the following recommendations.

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

Recommendation 2: We recommend the United States Capitol Police consider using investigative analysts to augment its threat management resources.

Training

TAS agents receive basic and advanced training related to criminal investigations and threat assessments from both external and internal sources. Upon assignment to TAS, agents complete the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC) and the USCP Basic Investigator Training Program. Following successful completion of the Basic Investigator Training Program, TAS assigns agents a Field Training Agent/Mentor for a minimum of 5 weeks. TAS assigns the Field Training Agent/Mentor a *New Agent Field Training Guide* for each agent they train. The *New Agent Field Training Guide* is a mandatory checklist of skills and tasks of which each new agent must demonstrate proficiency to complete basic training. The 5-week program consists of 3 weeks in the agent's assigned ID section followed by 1-week familiarity in the other two ID sections. A Department official stated that although initial completion of the training guide is a 5-week program, case assignments, travel, or a new agent's level of understanding might extend the length of the program.

Upon completion of basic training, TAS agents receive advanced training while assigned to TAS. The advanced training includes the USCP Experienced Investigator Training Program/Advanced Threat Assessment Refresher and a FLETC course entitled *Advanced Interviewing for Law Enforcement Investigators*. TAS also sends its agents to conferences and seminars provided by organizations such as the Association of Threat Assessment Professionals and the Intel and Law Enforcement Training Seminar. A Department official stated that TAS generally sends two agents at a time to each conference or seminar on a rotating basis. According to that same Department official, the conferences and seminars provide TAS agents with updates on emerging trends and issues related to threat assessments.

USCP Directive [REDACTED], dated February 14, 2019, states that the Training Management System (TMS) is a "computerized database for documenting and scheduling in-service training. The TMS is the official system of record for all courses of instruction offered, sponsored, or contracted by the USCP."⁸ The directive further states that all training is documented in TMS and that USCP organizational elements update training they conduct or contract for themselves into TMS. A Department official stated that not all training TAS agents received was documented in TMS. Failure to document training in TMS could cause inconsistencies and/or inaccuracies in USCP employee training records.

⁸ From the Desk of the Chief [REDACTED], dated August 12, 2020, announced the launch of APEX, "a new, fully-integrated talent management system that automates, modernizes, and streamlines our human capital processes and operations." The announcement states "APEX Learning will launch on October 1, 2020. APEX Learning replaces the existing Training Management System (TMS), and it brings comprehensive training, scheduling, reporting, and tracking into one modern, state-of-the-art platform."

Conclusions

Although TAS agents received basic and advanced training related to criminal investigations and threat assessments from both external and internal sources, the training was not always documented in the Department's official system of record. Thus, OIG makes the following recommendation.

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.

Policies and Procedures

GAO Standards for Internal Control in the Federal Government; Documentation of the Internal Control System state:

Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.

Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

Of the seven Standard Operating Procedures (SOPs) specific to TAS listed on PoliceNet, TAS had not updated five SOPs since 2006, one SOP since 2009, and one other SOP since 2011:

- SOP [REDACTED], dated June 15, 2006
- SOP [REDACTED], dated July 7, 2009
- SOP [REDACTED], dated January 24, 2011
- SOP [REDACTED], dated June 15, 2006
- SOP [REDACTED], dated May 31, 2006
- SOP [REDACTED], dated May 31, 2006

- SOP [REDACTED], dated May 31, 2006

As a result, many of the SOPs the Department had in place for TAS did not accurately reflect the changes in its processes over time. For example, SOPs [REDACTED], and [REDACTED] do not list all of the personal and criminal history checks TAS completes for the subjects of its investigations. In addition, SOPs [REDACTED], [REDACTED], [REDACTED] and [REDACTED] still contain documentation requirements related to a case management system that TAS no longer uses.

During our assessment, TAS was reviewing and updating its SOPs. We reviewed the draft copies of updated SOPs. We also selected a random sample of 10 TAS threat cases and 10 TAS Direction of Interest cases closed during Fiscal Years 2019 and 2020 to review. Because TAS SOPs were outdated and updated SOPs still in draft form, we did not review the sampled cases for compliance with guidance and instead reviewed them to gain a better understanding of current TAS procedures. Our review revealed that once implemented the draft SOPs would more effectively communicate the investigative procedures TAS uses.

Conclusions

The SOPs the Department had in place for TAS were outdated and did not accurately reflect the changes in its processes over time. Once implemented, the updated draft SOPs for TAS will more effectively communicate the investigative procedures TAS uses. Thus, OIG makes the following recommendation.

Recommendation 4: 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.

APPENDICES

Listing of Recommendations

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

Recommendation 2: We recommend the United States Capitol Police consider using investigative analysts to augment its threat management resources.

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.

Recommendation 4: 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.

DEPARTMENT COMMENTS



UNITED STATES CAPITOL POLICE

119 D STREET, NE
WASHINGTON, DC 20510-7213
PHONE: 202-224-1677

September 15, 2020

COP 200335

MEMORANDUM

TO: Michael A. Bolton
Inspector General

FROM: Steven A. Sund
Chief of Police

SUBJECT: Response to Office of Inspector General draft report *Assessment of the United States Capitol Police Threat Assessment Section* (Investigative No. 2020-I-0006)

The purpose of this memorandum is to provide the United States Capitol Police response to the recommendations contained within the Office of Inspector General's (OIG) draft report *Assessment of the United States Capitol Police Threat Assessment Section* (Investigative No. 2020-I-0006).

The Department generally agrees with all of the recommendations and appreciates the opportunity to work with the OIG to further improve upon the policies and procedures in place for our Threat Assessment Section. The Department will assign Action Plans to appropriate personnel regarding each recommendation in effect in order to achieve long term resolution of these matters.

Thank you for the opportunity to respond to the OIG's draft report. Your continued support of the women and men of the United States Capitol Police is appreciated.

Very respectfully,

A handwritten signature in black ink, appearing to read "SASund".

Steven A. Sund
Chief of Police

cc: Assistant Chief Chad B. Thomas, Uniformed Operations
Assistant Chief Yogananda D. Pittman, Protective and Intelligence Operations
Richard L. Braddock, Chief Administrative Officer
[REDACTED] USCP Audit Liaison

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.



