Approved for Public Release (without appendices) by the Capitol Police Board on June 24th, 2024

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: Operational Planning and Intelligence

Investigative Number 2021-I-0003-A

February 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 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.

Michael A. Bolton
Inspector General

TABLE OF CONTENTS

Abbreviations and Acronyms

Civil Disturbance Unit	CDU
Command and Coordination Bureau	CCB
Containment and Emergency Response Team	CERT
[redacted]	
Government Accountability Office	GAO
Intelligence and Interagency Coordination Division	IICD
Intelligence Operations Section	IOS
Office of Inspector General	OIG
Operational Services Bureau	OSB
Protective Services Bureau	PSB
Special Operations Division	SOD
Standard Operating Procedure	SOP
Task Force Officer	TFO
Uniformed Services Bureau	USB
United States Capitol Police	USCP or Department

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. See Appendix A for the United States Capitol Police's (USCP or Department) official timeline of events leading up to and during the physical security breach.

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 this ongoing work, this flash report is designed to communicate any deficiencies with the Department's operational planning and intelligence for planned demonstrations on January 6, 2021. The deficiencies included the following (a) lack of a comprehensive operational plan or adequate guidance for operational planning, (b) failure to disseminate relevant information obtained from outside sources, (c) lack of consensus on the interpretation of threat analyses, (d) dissemination of conflicting intelligence, and (e) lack of security clearances.

In order to improve its operational planning capabilities, USCP should implement detailed guidance for operational planning. The guidance should include policies and procedures that designate the entity or entities responsible for overseeing the operational planning and execution process, require documentation of supervisory review and approval, and standardize planning document formats. Guidance should also require that individual units develop plans and coordinate those plans with other units for a comprehensive, Department-wide effort. Additionally, the guidance should communicate when specific operational planning documents are required. For, example the Department could use a multi-tiered system based on the anticipated size and scope of an event as criteria for determining the required level of operational planning documentation it needs to prepare.

Implementing formal guidance requiring that employees communicate any intelligence reports and concerns from external sources to appropriate commanders would improve USCP ability to effectively disseminate intelligence throughout the Department. Providing additional training to personnel on how to better understand intelligence assessments and an increased role for

Department entities that have intelligence analysis and dissemination responsibilities in operational planning would also improve USCP ability to achieve a consensus on threat analyses. Furthermore, the Department should require supervisory review and approval for intelligence products to ensure the products are supported by relevant intelligence information and are internally consistent. Lastly, receiving classified briefings on emerging threats and tactics would better prepare the Department's sworn and operational civilian employees to identify and counter threats and tactics in the field. See Appendix B for a complete list of recommendations.

This is the first in a series of flash reports OIG will produce as part of its 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 those areas during our review. We anticipate that our next flash report will focus on the Department's intelligence operations and Civil Disturbance 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. See Appendix A for the United States Capitol Police's (USCP or Department) official timeline of events leading up to and during the physical security breach.

The Department's Protective Services Bureau (PSB) and Security Services Bureau are the two operational bureaus that report to the Assistant Chief of Police for Protective and Intelligence Operations. According to PoliceNet,[1] PSB's mission is to "provide safety and security to the Capitol, Members of Congress, Officers of Congress, and their immediate family." PSB has a Dignitary Protection Division, Investigations Division, and Intelligence and Interagency Coordination Division (IICD).

The PSB Investigations Division has three sections: the Criminal Investigations Section, the Threat Assessment Section, and the Intelligence Operations Section (IOS).

PoliceNet states that IOS:

- Provides overt and covert patrol of the Congressional Community to identify and disrupt individuals or groups intent on engaging in illegal activity directed at the Congressional Community and its legislative process.
- 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.

[1] PoliceNet is the Department's intranet.

- 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.

PoliceNet states that IICD is responsible for:

- Coordinating with the intelligence and law enforcement community at the federal, state, local, and tribal levels to increase the collection and sharing of intelligence information.
- Maximizing the collection and analysis of all source information and intelligence.
- Identifying potential threats, from both domestic and foreign entities or groups, to the federal Legislative Branch, statutory protectees, Congressional facilities, Congressional employees, and the visiting public.
- Briefing and advising the USCP Executive Team, Executive Management Team, Senior Management Team, Capitol Police Board, and other members of the Department regarding emerging tactics and threats posed by various terrorist groups or individuals.
- Analyzing and disseminating products and reports on international and domestic events and incidents that are of interest to, or may impact, the U.S. Capitol, the Legislative process, and our statutory protectees.
- Serving as the principal point of contact within the Intelligence Community for all domestic and foreign intelligence (and threat-related matters) impacting the security of the U.S. Congress.
- Maintaining the USCP Intelligence Priority Framework, identifying gaps in information, and determining the most suitable entity or entities to collect the information.

The Department's Command and Coordination Bureau (CCB), Uniformed Services Bureau (USB), and Operational Services Bureau (OSB) are the three operational bureaus reporting to the Assistant Chief of Police for Uniformed Operations. According to PoliceNet, CCB provides capabilities to acquire, coordinate, and execute mission critical objectives. CCB has a Command Division and Coordination Division.

According to PoliceNet, USB is divided into the Capitol Division, Senate Division, House Division, and Library Division. USB's responsibilities include providing police services and security for the Capitol Building and Grounds, Senate Office Buildings, House Office Buildings, and Library of Congress.

USCP PoliceNet states the mission of OSB is to "provide specialized and emergency response to support the Department's operational needs. This is accomplished in the form of specialized training, enforcement, coordination, planning, equipment, and response policy development." The divisions within OSB are the Hazardous Incident Response Division and the Special Operations Division (SOD).

SOD provides police services on the Capitol Grounds and other areas through motorized, bicycle, and foot patrols; canine operations; prisoner processing and transportation; drug and alcohol enforcement; crime scene search; and the Containment and Emergency Response Team (CERT). According to USCP [redacted] dated May 28, 2012, "the Department provides ready response for situations requiring special weapons and tactics by maintaining CERT."

The Department's Civil Disturbance Unit (CDU) is an *ad hoc* unit within SOD. According to draft [redacted] dated February 2, 2021, CDU's mission is to "ensure the legislative functions of Congress are not disrupted by civil unrest or protest activity, while respecting the Civil Rights of all citizens."

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 the 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 operational planning and intelligence for planned demonstrations on January 6, 2021. Additionally, we researched Department guidance related to operational planning and intelligence. To research best practices, OIG consulted with a former Deputy Assistant Director for Special Intelligence and Information for the U. S. Secret Service and reviewed guidance from the Government Accountability Office (GAO).

This flash report is based upon work OIG conducted in Washington, D.C., from January through February 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 first 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 intelligence operations and CDU.

RESULTS

We produced this flash report to communicate deficiencies with the Department's operational planning and intelligence ahead of the planned demonstrations on January 6, 2021. Deficiencies included the (a) lack of a comprehensive operational plan or adequate guidance for operational planning, (b) failure to disseminate relevant information obtained from outside sources, (c) lack of consensus on the interpretation of threat analyses, (d) dissemination of conflicting intelligence, and (e) lack of security clearances.

Operational Planning

USCP did not prepare a comprehensive, Department-wide operational plan for demonstrations planned for January 6, 2021, and lacked adequate guidance for operational planning.

Lack of a Comprehensive Operational Plan

USCP did not prepare a comprehensive, Department-wide operational plan for demonstrations planned for on January 6, 2021. OSB prepared a [redacted] for January 6, 2021 [redacted] dated January 5, 2021, the Hazardous Materials Response Team prepared a one-page [redacted] and USB prepared a one-and-one-half-page [redacted] with an outline of non-routine USB operations for the day but did not include detailed plans. We made multiple requests for documents and inquired with several Department officials about whether any other planning documents existed for January 6, 2021, but those inquiries did not reveal the existence of any additional planning documents.

The [redacted] focuses on CDU and contains abbreviated details on certain other units within the Department such as the Hazardous Incident Response Division, SOD patrols, Crime Scene Search, and CERT. The [redacted] however, lacks detailed operational plans for those units. Many other USCP entities planned non-routine operations for January 6, 2021, but the Department could not provide detailed operational planning documents for those entities. For example, the [redacted] lists several non-routine USB operations for that day but it does not include detailed operational planning documents for USB or any of its divisions. Additionally, the Department's timeline includes several non-routine Dignitary Protection Division operations for the week of January 3,

2021, and specifically January 6, 2021, but the Department could not provide detailed operational planning documents communicating such plans.

As stated, the [redacted] brief details on CERT but does not include detailed, operational plans for the unit. Our review of the plan and interviews with Department officials revealed inconsistencies about how the Department planned to use CERT on January 6, 2021. The [redacted] states CERT would deploy [redacted] to monitor events. Both Acting Chief of Police Yogananda Pittman and Assistant Chief of Police for Uniformed Operations Chad Thomas stated in interviews that the Department planned to use CERT to extract non-compliant violators and disarm protesters if necessary. Acting Chief Pittman also stated, however, that all of CERT ([redacted]) was present and available for duty on January 6, 2021. The [redacted] does not provide how CERT would disarm or extract protesters nor does it account for all of CERT being present for duty that day. Additionally, OSB officials stated in interviews that they were not familiar with any plans to have CERT arrest or disarm protesters.

USCP officials stated that the Department has made changes to its operational planning process since January 6, 2021. OIG obtained and reviewed several plans the Department prepared for events taking place after January 6, 2021. The plans are more comprehensive and provide a higher level of detail than planning documents before January 6, 2021. A Department official described the plans as a "drastically different format" from past planning documents. According to the official, the intent of the changes are:

- To increase compatibility with the Department of Homeland Security Incident Command System that a majority of agencies across the country utilize.
- To increase the assigned Incident Commander's ability to dictate planning goals.
- To increase the Department's capability to plan to a greater level of detail by specifying the required planning entities.
- To increase flexibility to have operational planning positively impact operational implementation.

The official stated the plans are the first implementations of this format and that the Coordination Division in CCB continues to accept feedback from entities to refine the product.

Lack of Guidance for Operational Planning

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.

The Department lacked adequate guidance for operational planning. USCP did not have policies and procedures in place that communicated which personnel were responsible for operational planning, what type of operational planning documents its personnel should prepare, or when its personnel should prepare operational planning documents. Additionally, USCP lacked guidance requiring that its various entities coordinate their planning efforts into a comprehensive plan.

Interviews with Department officials revealed inconsistencies in the types of planning documents USCP should have prepared for January 6, 2021. Former Chief of Police Steven Sund stated the Department used documents commonly referred to as a "Plan of Action" for large events and that such a Plan of Action signed by Assistant Chief Thomas should have existed for the events of January 6, 2021. Former Chief Sund also stated that the Commander of the USB Capitol Division should have completed an "Incident Action Plan" for the Joint Session of Congress. Former Chief Sund stated that he believed there were Department policies addressing those planning documents. However, we could not find any policies that clearly addressed creation of those specific planning documents.

According to the OSB official responsible for preparing [redacted], prior to the summer of 2020 there were no formal planning documents for CDU events. After protest activity during the summer of 2020, OSB began utilizing a planning document from the International Association of Chiefs of Police as a guide for creating such a plan. The official stated that OSB forwards a [redacted] by email to Assistant Chief Thomas for approval and OSB receives a confirmation with no correspondence log or other documented approval. Certain CDU commanders provide input [redacted] but OSB does not distribute the plan to any other Department commanders. Several Department officials stated that they were not familiar with [redacted] for January 6, 2021.

Conclusions

USCP should have implemented detailed operational planning guidance. The guidance should have included policies and procedures for designating an entity responsible for overseeing the operational planning and execution process, requiring documentation of supervisory review and approval, and standardizing planning document formats. Guidance should also have required that individual units develop plans and coordinate those plans with other units into a

comprehensive, Department-wide effort. Additionally, the guidance should have communicated when certain operational planning documents are required. For example, the Department could use a multi-tiered system based on the anticipated size and scope of an event as criteria for determining the level of operational planning documentation it should prepare. Therefore, OIG makes the following recommendations.

Recommendation 1: We recommend the United States Capitol Police establish policies and procedures requiring documentation for supervisory review and approval, standardized planning document formats, and communication to personnel of criteria for determining the level of operational planning documentation necessary for each anticipated event.

Recommendation 2: We recommend the United States Capitol Police establish policies and procedures designating the specific entity or entities responsible for overseeing the operational planning and execution process for each anticipated event.

Recommendation 3: We recommend the United States Capitol Police establish policies and procedures requiring that individual units develop operational plans and coordinate those plans with other units for a comprehensive, Department-wide effort.

Intelligence

USCP failed to disseminate relevant information obtained from outside sources, lacked consensus on the interpretation of threat analyses, and disseminated conflicting intelligence information regarding planned events for January 6, 2021. Additionally, the Department did not require that all of its sworn and operational civilian employees obtain security clearances.

Dissemination of Information from Outside Sources

USCP failed to disseminate relevant information obtained from outside sources regarding planned events for January 6, 2021. According [redacted] on January 5, 2021, at approximately 7 p.m. to 8 p.m., a USCP task force agent [redacted] emailed [redacted] details regarding the January 6, 2021, event. OIG obtained a copy of the memorandum [redacted]

Acting Assistant Chief of Police for Protective and Intelligence Operations Sean Gallagher stated that the memorandum was a [redacted] which he viewed differently than an Intelligence Assessment because [redacted] are not necessarily authenticated or followed-up, [redacted] produces them to communicate something its agents saw or learned. Acting Assistant Chief Gallagher acknowledged it was hard to view it that way after January 6, 2021. Acting Assistant Chief Gallagher also stated that to his knowledge [redacted]

never formally sent [redacted] to USCP. The [redacted] produced the document, and it was then placed on an [redacted] intranet or other internal system. Late in the evening on January 5, 2021, a USCP task force officer (TFO) assigned to the [redacted] pulled [redacted] from [redacted] and emailed it to a USCP IOS email distribution list.

According to Acting Assistant Chief Gallagher, [redacted] did not surface again until it was attached to an information package sent out late on January 6, 2021, after the security breach occurred. In the days following January 6, 2021, [redacted] began to surface in the media and Members of Congress began to ask USCP if it had received it. The Department was originally under the impression that it had not received the document until a Department official inquired with USCP's TFOs about it. Acting Assistant Chief Gallagher stated that to his knowledge, prior to the events of January 6, 2021, [redacted] did not make it out of the IOS email distribution list to IICD or other Department commanders.

[redacted]

Lack of Consensus Regarding the Threat Analysis

[redacted] dated January 3, 2021, was IICD's final special event assessment for planned events on January 6, 2021. In this final assessment, IICD's overall analysis states:

[redacted]

[redacted]

Interviews with USCP officials revealed a lack of consensus about whether intelligence information regarding planned events on January 6, 2021, actually indicated specific known threats to the Joint Session of Congress. Certain officials believed USCP intelligence products indicated there may be threats but did not identify anything specific, while other officials believed it would be inaccurate to state that there were no known specific threats to the Joint Session based on those same USCP intelligence products.

The threat analysis in the [redacted] for January 6, 2021, dated January 5, 2021, states, "At this time there are no specific known threats related to the Joint Session of Congress – Electoral College Vote Certification." While a prior version of [redacted] contains the exact same statement and updated versions of the assessment published later that month contain similar language, the final version dated January 3, 2021, does not contain that statement. The IICD Director stated that IICD periodically revised the assessment as it received more information, and IICD updated the final version based on concerns communicated by the Department's law enforcement partners. An OSB official responsible for preparing the [redacted] dated January 5, 2021, admitted it was most likely an error on their part that the threat analysis [redacted] was not updated. However, multiple Department officials with intelligence dissemination responsibilities stated they had never even seen the threat analysis included in [redacted] dated January 5, 2021.

Providing additional training to personnel on how to better understand and interpret intelligence assessments and requiring that any threat analyses included in operational planning are coordinated with Department entities with intelligence analysis and dissemination responsibilities would improve USCP ability to achieve a consensus on its threat analyses.

Daily Intelligence Report

The Department disseminated conflicting intelligence information regarding planned events on January 6, 2021. IICD publishes a [redacted] which the Department uploads to PoliceNet. The report includes details of any upcoming demonstrations, activity, and issues for the U.S. Capitol as well as the District of Columbia. The [redacted] includes a level of assessed probability of acts of civil disobedience/arrests occurring based on current intelligence information and includes the following terms to describe those levels:

- Remote- [redacted]
- Highly Improbable- [redacted]
- Improbable- [redacted]
- Roughly Even Odds- [redacted]
- Probable- [redacted]

- Highly Probable-[redacted]
- Nearly Certain-[redacted]

The report does not, however, communicate any criteria that IICD uses to determine the level of probability. As shown in Figure 1, the [redacted] for January 6, 2021, lists an upcoming event as "Million MAGA March/US Capitol (Possibly)" and reports the level of probability of acts of civil disobedience/arrests occurring based on current intelligence information as "Improbable."

[redacted]

[redacted]

We inquired with the IICD Director about the criteria IICD uses for determining the probability levels published in its [redacted] and how it corresponded to its January 3, 2021, [redacted]. According to the IICD Director, [redacted] are two separate documents that serve different purposes. A [redacted] has been responsible for compiling the [redacted] for a number of years, and it has been published without supervisory review. [redacted]. The IICD Director was not aware of what criteria the analyst used to determine the probability level for acts of civil disobedience/arrests.

OIG reviewed guidance related to IICD intelligence products. Our review revealed that Standard Operating Procedure (SOP) [redacted], dated February 1, 2018, states that for expressions of likelihood or probability, an analytic product must use one of the terms listed previously, ranging from remote to nearly certain. SOP [redacted] also states,

> All analytic judgments should be effectively supported by relevant intelligence information and coherent reasoning. Language and syntax should convey meaning unambiguously. Products should be internally consistent and acknowledge significant supporting and contrary information affecting judgments.

SOP [redacted] requires that the IICD Associate Director conduct periodic reviews and evaluations of IICD analytic intelligence products, but it does not require supervisory review of all IICD analytic intelligence products. The Department should revise IICD guidance to require supervisory review and approval for all intelligence products to ensure its products are supported by relevant intelligence information and internally consistent.

Security Clearances

Media reports revealed that some USCP officers believed the Department failed to provide them with adequate intelligence leading up to the events that occurred on January 6, 2021. In a previous report, Investigative Number 2018-I-0008, *Follow-up Analysis of the United States Capitol Police Intelligence Analysis Division*,[2] dated March 2019, OIG found the Department did not require that all of its sworn and operational civilian employees obtain security clearances. As a result, IICD can only disseminate information to many of the Department's sworn and operational civilian employees at a law enforcement sensitive level. According to a then-IICD official, communication of intelligence within the Department would improve if all of its sworn

[2] The Intelligence Analysis Division was a past name for IICD.

and operational employees had clearances because that would allow IICD to provide classified briefings to those employees. OIG recommended that USCP consider requiring all new sworn recruits and operational civilian employees obtain a security clearance. Because it would be a change to conditions of employment and USCP may not be able to require its current employees to obtain a security clearance, OIG recommended that the Department consider providing current employees the opportunity to obtain one.

In a May 2, 2019, response to the recommendation, USCP indicated that it agreed with the recommendation, but that it would not be pursing security clearances for all employees at that time. The response also indicated USCP would engage counsel and PSB in the future to develop protocols for establishing a Secret-level clearance program.

Interviews we conducted as part of our ongoing review revealed that while the IICD Director believed the lack of security clearances did not pose a concern because much of the information IICD disseminates is not classified and derived from open sources, several other Department officials stated that they believe it did indeed affect USCP ability to disseminate intelligence throughout the Department. Our research into best practices revealed that the U.S. Secret Service requires all of its employees to obtain a Top Secret clearance. Receiving classified briefings on emerging threats and tactics would better prepare the Department's sworn and operational civilian employees to identify and counter threats and tactics in the field. In order to disseminate the maximum amount of real-time, up-to-date intelligence to its personnel, the Department should require its sworn and operational civilian employees to obtain a Top Secret clearance and require its administrative civilian employees to obtain at minimum a Secret clearance.

Conclusions

Implementing formal guidance requiring that employees communicate any intelligence reports and concerns from external sources to appropriate commanders would improve USCP ability to effectively disseminate intelligence throughout the Department. Additionally, providing additional training to USCP personnel on how to better understand intelligence assessments and an increased role for Department entities that have intelligence analysis and dissemination responsibilities in operational planning would improve USCP ability to achieve a consensus on its threat analyses. Furthermore, the Department should require supervisory review and approval for intelligence products to ensure those products are supported by relevant intelligence information and internally consistent. Lastly, receiving classified briefings on emerging threats and tactics would better prepare the Department's sworn and operational civilian employees to identify and counter threats and tactics in the field. Therefore, OIG makes the following recommendations.

Recommendation 4: We recommend the United States Capitol Police implement formal guidance requiring that employees communicate any intelligence reports and concerns from external sources to appropriate commanders.

Recommendation 5: We recommend the United States Capitol Police implement detailed policies and procedures requiring any threat analysis included in operational planning is coordinated with Department entities having intelligence analysis and dissemination responsibilities.

Recommendation 6: We recommend the United States Capitol Police provide training to its personnel on how better to understand and interpret intelligence assessments.

Recommendation 7: We recommend the United States Capitol Police revise Standard Operating Procedure [redacted], dated February 1, 2018, to require supervisory review and approval for intelligence products to ensure its products are supported by relevant intelligence information and internally consistent.

Recommendation 8: We recommend the United States Capitol Police require its sworn and operational civilian employees to obtain a Top Secret clearance and require that administrative civilian employees obtain a minimum of a Secret clearance.

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