UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Evaluation of the
United States Capitol Police
Division of Intelligence and Information Analysis

Report Number OIG-2016-04

March 2016

[redacted]

[redacted]

OFFICE OF 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 is 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 in draft 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.

Fay F. Ropella

Fay F. Ropella
Inspector General

TABLE OF CONTENTS

Abbreviations and Acronyms

[redacted]	[redacted]
Division of Intelligence and Information Analysis	DIIA
Director of National Intelligence	DNI
[redacted]	[redacted]
For Official Use Only	FOUO
Fiscal Year	FY
Government Accountability Office	GAO
Intelligence Section-Investigations	IS-I
Law Enforcement Sensitive	LES
Memorandum of Understanding	MOU
[redacted]	[redacted]
[redacted]	[redacted]
Office of General Counsel	OGC
Office of Inspector General	OIG
Office of Policy and Management Systems	OPOL
Operational Security	OPSEC
Open Source Section	OSS
Protective Services Bureau	PSB
Sensitive Compartmented Information Facility	SCIF
Standard Operating Procedure	SOP
Special Security Officer	SSO
Security Services Bureau	SSB
Technical Countermeasures Division	TCD
Threat Assessment Section	TAS
United States Capitol Police	USCP or Department

EXECUTIVE SUMMARY

The United States Capitol Police (USCP or the Department) has established mechanisms—including an intelligence framework and analytic planning process for protecting Members of Congress, other statutory protectees, other U.S. Government officials, visiting foreign dignitaries, and property under the jurisdiction of the U.S. Congress—for providing threat warning information and analysis of intelligence on terrorist activities worldwide on a time-sensitive basis.

In accordance with the Office of Inspector General (OIG) annual plan and as part of our oversight responsibility of the Department, we evaluated the Division of Intelligence and Information Analysis (DIIA) within the Protective Services Bureau (PSB). DIIA has four sections: Analysis Section, Open Source Section (OSS), Special Security Section, and Liaison Section.

Our primary objectives were to determine if the Department (1) established adequate internal controls and processes for ensuring collection and dissemination of information that would enhance the ability of the Department to carry out its mandated mission, and (2) complied with applicable policies and procedures as well as applicable laws, regulations, and best practices. Our scope included internal controls, processes, and operations during fiscal years (FYs) 2014 and 2015.

DIIA did not establish adequate internal controls and processes for ensuring the integrity of its program. The division did not maintain written procedures for many of its processes. Although DIIA used mechanisms for producing threat assessments for [redacted], special events, and terrorism, the division did not document the procedures or processes. And although the Department had standard operating procedures (SOPs) for some controls, DIIA did not update many SOPs to reflect a change in its processes. Of the 15 SOPs OIG reviewed, DIIA had not updated 13 of the SOPs since 2006. As a result, DIIA did not accurately reflect its intelligence and information processes in its SOPs.

Because SOPs were outdated and the division did not always follow written procedures, DIIA could not provide supporting documentation that it complied with many of its SOPs. [redacted] DIIA also did not always comply with guidance related to several critical functions. Those functions included such things as [redacted]

[redacted] and on-call schedules. For example, in September 2015, DIIA issued an "Open Source" newsletter about an October 10, 2015, *Nation of Islam* rally commemorating the 20th Anniversary of the Million Man March. DIIA did not provide source attribution or obtain approval for newsletter content from senior officials. The newsletter contained language some viewed as inflammatory and resulted in the Chief of Police immediately retracting the newsletter, stating that it "does not reflect the viewpoint or values of the United States Capitol Police, nor was it intended to provide instruction or guidance to our employees." DIIA did not have an SOP concerning strategic goals for newsletters, which would in all likelihood have mitigated the risk of releasing inappropriate, misleading, or inflammatory information.

Although USCP established a framework for intelligence and information analysis, the Department did not integrate intelligence activities throughout USCP. DIIA is primarily responsible for intelligence and information analysis, yet similar activities took place throughout various bureaus, offices, and divisions not integrated or functioning as intended. For example, the Threat Assessment Section (TAS) and Intelligence Section-Investigations (IS-I) within the Investigation Division of PSB regularly interact with DIIA on intelligence-related matters. TAS investigates threats to Congress and IS-I is responsible for [redacted] and suspicious-activity investigations. The Technical Countermeasures Division (TCD) within the Security Services Bureau [redacted]

The framework did not establish strategic departmental intelligence priorities that can be used to help with annual planning decisions, such as which analytic activities should be pursued and level of investment. As a result, USCP did not have reasonable assurance that analytic activities for components and resource investments successfully supported departmental priorities.

The integration of intelligence mechanisms should provide insight into the work of each component throughout the Department and help the Department avoid any unnecessary overlap and redundant functions. [redacted] Although OIG agrees with the Department's proposal to separate DIIA from PSB, we also believe the Department should include as elements in its proposed intelligence bureau TCD as well as TAS and IS-I. Reorganization and consolidation of all of the intelligence elements within the Department should increase the efficiency and effectiveness of intelligence resources as well as better support departmental priorities.

We surveyed officials from the Investigations Division and TCD, who believe DIIA information has been useful. However, officials of [redacted] In the February 26,

2016 response to the draft report, the Department stated it will seek legal advice regarding [redacted]

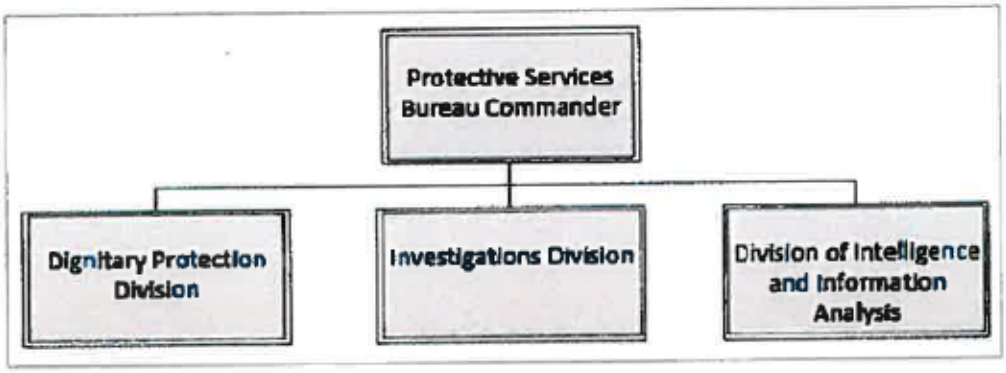
USCP partners with external intelligence and law enforcement agencies and provides liaisons at each agency. Those agencies are [redacted] DIIA is the USCP point of contact within the Intelligence Community (agencies and liaisons). However, the Department did not maintain Memorandums of Understanding (MOU) with each agency with assigned USCP liaisons. After a considerable amount of time, the Office of General Counsel and the Office of Human Resources were able to provide a MOU for [redacted] liaison positions [redacted]. Lack of an appropriate MOU could have put the Department in a vulnerable position without reasonable assurance that component analytic activities were producing products or resource investments aligned, which supported departmental priorities. OIG recommends that USCP establish (1) controls and strategic intelligence priorities and use them to inform analytic activities and (2) mechanisms for evaluating workforce initiatives and use results to determine any needed changes. See Appendix A for a complete list of recommendations.

On February 10, 2016, OIG conducted an exit conference with Department officials and provided a draft report for comment. Considering the February 26, 2016, Department response to the OIG draft report, we revised Recommendation 6 and attached the Department's response in its entirety in Appendix B.

BACKGROUND

As of February 2016, the United States Capitol Police (USCP or the Department) Protective Services Bureau (PSB) is one of the five operational bureaus reporting to the Chief of Operations. USCP PoliceNet states the mission of PSB is "to provide safety and security to the Capitol, Members of Congress, Officers of Congress, and their immediate family." The divisions within PSB are the Dignitary Protection Division, Investigations Division, and the Division of Intelligence and Information Analysis (DIIA) as shown in Exhibit 1.

Exhibit 1 – Organization Chart of the Protective Services Bureau

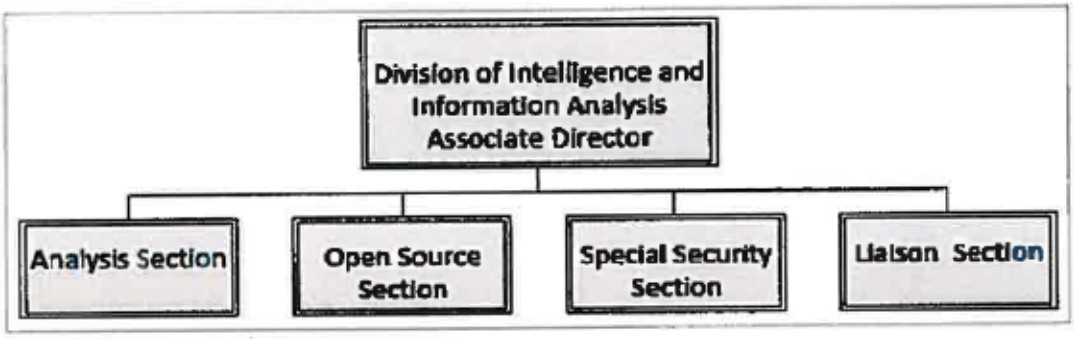


Source: OIG generated using information provided by Department officials and PoliceNet as of February 2016.

According to USCP PoliceNet, the role of DIIA is to "protect Members of Congress, other statutory protectees, other U.S. Government officials, visiting foreign dignitaries, and property under the jurisdiction of the U.S. Congress by providing threat warning information and analysis of current intelligence on terrorist activities worldwide on a time sensitive basis." Other DIIA responsibilities include serving as the Department's point of contact within the Intelligence Community and providing briefings, reports, and assessments to the Department as well as Capitol Police Board on any potential threats to Congress and the Capitol Complex.

As of December 2015, DIIA had 13 employees—11 civilian employees and 2 sworn employees who were detailed from the PSB Investigations Division. An Associate Director, who reports to the PSB Commander, commands DIIA. DIIA has four sections: Analysis Section, Open Source Section (OSS), Special Security Section and Liaison Section as shown in Exhibit 2.

Exhibit 2 – Organization Chart of the Division of Intelligence and Information Analysis



Source: OIG generated using information provided by Department officials and PoliceNet as of February 2016.

The Analysis Section is responsible for (1) analyzing and disseminating classified intelligence information related to Congress and the Capitol Complex; (2) producing threat assessments for [redacted], special events and potential terrorism including emerging techniques, tactics and procedures that terrorists could use; and (3) conducting briefings on threats related to Congress and the Capitol Complex.

OSS is responsible for (1) collecting information concerning Congress and the Capitol Complex [redacted] (2) fulfilling requests for information from other sections within the Department; (3) completing assessments for special event permit applications; and (4) conducting briefings on possible threats related to Congress and the Capitol Complex. OSS refers any threats or items of interest discovered to the USCP Investigations Division.

The Special Security Section (1) manages and addresses security clearance matters within USCP; and (2) maintains the Department's security clearance process, including handling secured clearance visitation requests, investigating security clearance violations, and conducting security briefings to clearance applicants as well as terminated personnel.

The Liaison Section is responsible for representing the Department and providing an avenue for information sharing with external partner intelligence and law enforcement agencies. DIIA has a liaison at the [redacted].

Other elements within the Department engaging in intelligence-related activities include the Threat Assessment Section (TAS) and Intelligence Section-Investigations (IS-I) within PSB's Investigation Division and the Technical Countermeasures Division (TCD) within the Security Services Bureau (SSB). TAS is responsible for identifying, assessing, and managing individuals who inappropriately communicate, contact, or threaten U.S. Capitol Police protectees. IS-I is responsible for [redacted] investigating suspicious activity for any nexus to terrorism and conducting protective intelligence operations. TCD is responsible for the [redacted] as well as providing Congress with a secure environment to discuss classified information.

The Office of Policy and Management Systems (OPOL) is responsible for the Department's Written Directive System, which includes policies and standard operating procedures (SOPs).

OBJECTIVE, SCOPE, AND METHODOLOGY

In accordance with the Office of Inspector General (OIG) annual plan and as part of our oversight responsibility for the Department, we conducted an independent evaluation of DIIA. Our primary objectives were to determine if the Department (1) established adequate internal controls and processes for ensuring collection and dissemination of information that would enhance the ability of the Department to carry out its mandated mission, and (2) complied with applicable policies and procedures as well as applicable laws, regulations, and best practices. Our scope included internal controls, processes, and operations during Fiscal Years (FYs) 2014 and 2015.

To accomplish our objectives, we interviewed relevant Department officials to gain an understanding of the following areas:

- DIIA processes as well as related policies and procedures
- The organizational and functional structure of DIIA
- Issues related to DIIA and/or ways in which the Department could improve its collection, analysis, and dissemination of intelligence information

We reviewed available SOPs and directives related to DIIA, including those in draft. We also reviewed staffing and organizational information related to DIIA. Of the [redacted] Memorandums of Understanding (MOUs) with external partner intelligence and law enforcement agencies, we

reviewed only [redacted] which the Department was able to provide. Additionally, we reviewed guidance from the Government Accountability Office (GAO).

To determine compliance, we reviewed the following guidance:

- SOP [redacted] May 31, 2006
- SOP [redacted], May 31, 2006
- SOP [redacted], May 31, 2006
- SOP [redacted] May 31, 2006
- SOP [redacted], May 31, 2006
- SOP [redacted] May 31, 2006
- SOP [redacted], May 31, 2006
- SOP [redacted], May 17, 2006
- SOP [redacted], June 15, 2006
- SOP [redacted], May 31, 2006
- SOP [redacted], May 31, 2006
- SOP [redacted], May 31, 2006
- SOP [redacted], May 31, 2006
- SOP [redacted], August 4, 2011
- SOP [redacted], August 4, 2011

We conducted fieldwork in Washington, D.C., from November 2015 through February 2016. We conducted our evaluation in accordance with the *Council of the Inspectors General on Integrity and Efficiency, Quality Standards for Inspection and Evaluation*. We did not conduct an audit,

the objective of which would be the expression of an opinion on DIIA programs. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that we would have reported. [redacted]

RESULTS

Overall, DIIA did not establish adequate internal controls and processes that would ensure the integrity of its program. DIIA also did not always comply with or have documentation supporting compliance with guidance. During this time of budget constraints, the Department should consider using its intelligence resources more efficiently and effectively.

Lack of Adequate Internal Controls

DIIA did not have adequate internal controls. Specifically, DIIA did not maintain up-to-date internal controls or procedures for many of its processes. GAO *Standards for Internal Control in the Federal Government; Documentation of the Internal Control System*, GAO-14-704G, September 2014, 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.

Inadequate Documentation of Policies and Procedures

As of January 2016, DIIA did not have adequate documentation of its policies and procedures. Specifically, DIIA did not maintain written internal control procedures for many of its processes. While it used practices to produce threat assessments for [redacted], special events, and terrorism, DIIA did not document the practices. As a result, its practices were not readily available for review and DIIA did not document repeatable business processes. Without official and written guidance, practices may lead to misinterpretation or noncompliance. For example, in September 2015, DIIA published a newsletter about an October 10, 2015, *Nation of Islam* rally to commemorate the 20th Anniversary of the Million Man March. DIIA distributed the newsletter by email to Department employees without including the sources for the newsletter, therefore giving the appearance that USCP was the source.

The newsletter contained language some viewed as inflammatory, and the Chief of Police immediately retracted the newsletter, offering that it "does not reflect the viewpoint or values of

the United States Capitol Police, nor was it intended to provide instruction or guidance to our employees." According to DIIA officials, sources of information are sometimes included, but not always. Most importantly, Department officials stated the newsletter did not receive approval from the Chief of Police, Assistant Chief of Police, or Bureau Commander before distribution. DIIA did not have an SOP addressing strategic goals or the approval process for newsletters. An SOP would have provided DIIA with uniform procedures it could reference to ensure it included sources with its newsletters on a consistent basis and submitted them to Department officials for approval.

DIIA had a draft SOP outlining the responsibilities of OSS, but the SOP did not address specific processes. According to a DIIA official, the division sent a draft SOP to OPOL in 2013, which the Department had not finalized as of January 2016. A DIIA official stated that the Department had not made a decision about procedures for processing USCP personnel for security clearances. On May 4, 2015, DIIA forwarded the decision paper to management. However, as of January 2016, the Department had not documented the procedures in any official SOP or directive.

Of the 15 SOPs listed on PoliceNet, DIIA did not update 13 SOPs since 2006 and 2 other SOPs since 2011. As a result, many of the SOPs the Department had in place for DIIA did not accurately reflect the changes in its processes.

Conclusions

DIIA did not have written internal control procedures for many of its processes, and most of the SOPs were outdated. Therefore, OIG makes the following recommendation.

> **Recommendation 1: We recommend that the United States Capitol Police update and formalize standard operating procedures for the Division of Intelligence and Information Analysis addressing all of its Sections including threat assessments, the "Open Source Newsletter," and security clearances.**

Non-compliance with Standard Operating Procedures

DIIA did not always comply with or have the required supporting documentation that it complied with guidance related to its SOPs. For example, DIIA did not comply with guidance in its SOPs related to the following areas: [redacted] and on-call schedules. [redacted]

Dissemination of Information Warning

SOP [redacted], May 31, 2006, states:

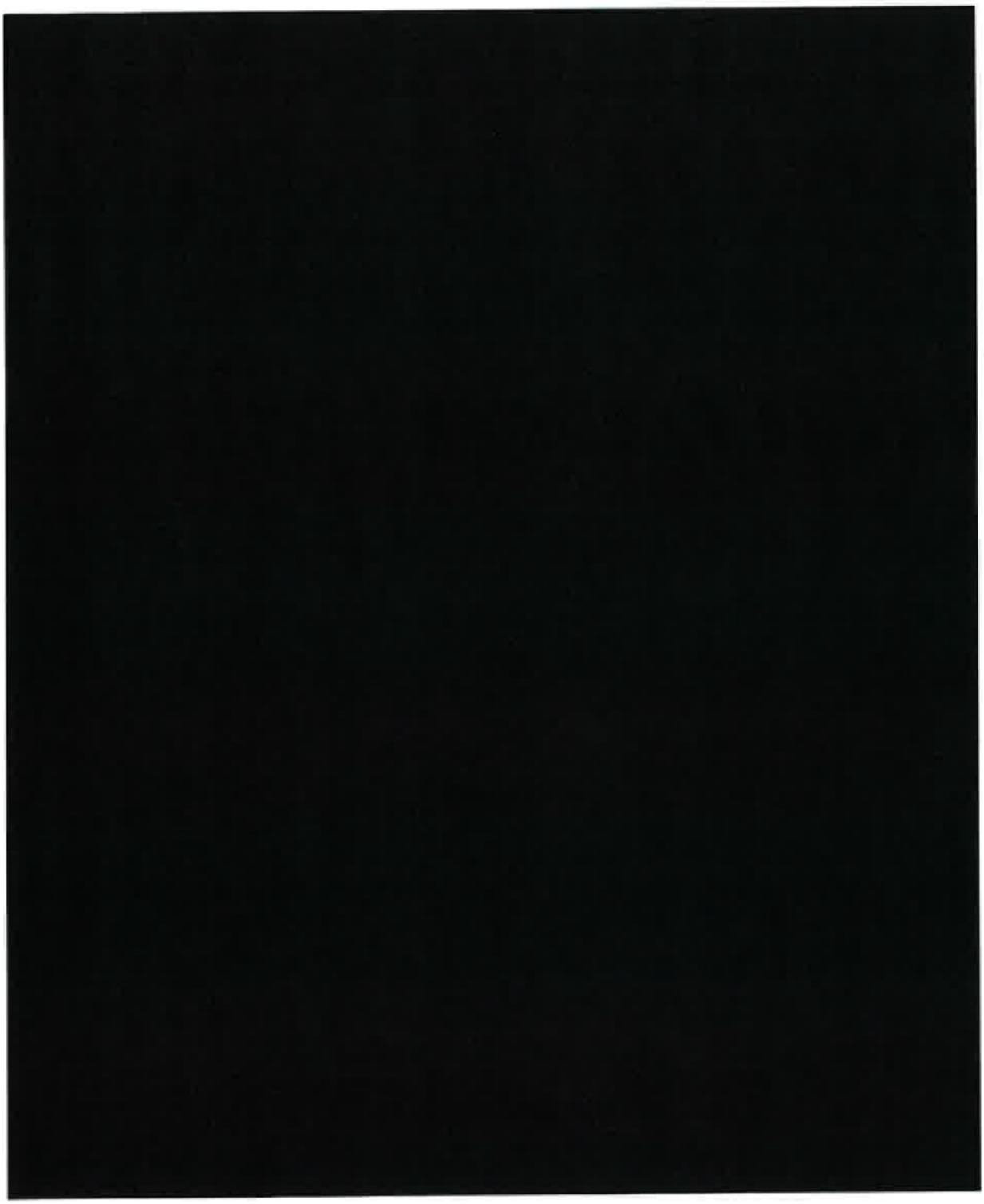
[redacted]

Documents that DIIA distributed to the Department during FYs 2014 and 2015 did not contain either of the warnings SOP [redacted] describes. For example, documents DIIA distributed to the Department during FY 2015 instead contained the following warning:

[redacted]

According to an official, the division changed its warning for disseminated material but did not update SOP [redacted] to include the revised warning. DIIA should change SOP [redacted] to reflect that change in procedures.

[redacted]



On-Call Schedule

SOP [redacted], August 4, 2011, requires that the DIIA supervisor ensure the division maintain an on-call schedule, provide each Intelligence Research Specialist with an up-to-date schedule, and provide PSB, the Dignitary Protection Division, the Investigations Division, Department Commanders, and the Command Center with up-to-date on-call schedules. A DIIA official stated that as of December 2015, the division had not completed an on-call schedule for at least 6 months because the Department always contacts the same DIIA official after hours regardless of the schedule. Without an official policy or schedule designating who is on call, there could be confusion about the appropriate individual within DIIA the Department should contact after hours. DIIA should revise SOP [redacted] to reflect the change in procedures.

Conclusions

DIIA did not comply with guidance contained in several SOPs. Specifically, DIIA did not comply with SOPs regarding [redacted] and on-call schedules. As a result, non-compliance and outdated SOPs could have resulted in sharing DIIA information in an untimely, inaccurate, and careless manner. OIG, therefore, makes the following recommendations.

Recommendation 2: We recommend that the United States Capitol Police require that the Division of Intelligence and Information Analysis maintain copies of [redacted] as Department guidance (Standard Operating Procedure [redacted]) requires.

Recommendation 3: We recommend that the United States Capitol Police revise Standard Operating Procedures [redacted] to reflect any changes in processes for the Division of Intelligence and Information Analysis.

Opportunities to Use Resources in a More Efficient and Effective Manner

USCP may have opportunities to use resources in a more efficient and effective manner. USCP intelligence resources are decentralized and may result in fragmentation, overlap, and duplication. Although it partners with the [redacted]; USCP did not maintain the requisite MOUs. As a result, the Department did not have reasonable assurance that component analytic activities produced a product or resource investments in alignment with departmental priorities. [redacted] In the February 26, 2016 response to the draft report, the Department stated it will seek legal advice [redacted]

[redacted]

Intelligence Framework and Component Analysis Planning Process Are Not Functioning as Intended

USCP's intelligence framework and component analysis planning process did not function as intended. Specifically, the Department had decentralized intelligence resources throughout several USCP Bureaus and Divisions. While the responsibilities of DIIA are primarily intelligence related, other divisions within the Department regularly interact with or could benefit from increased interaction with DIIA on intelligence-related matters. To increase the efficiency of its intelligence resources, the Department should consider reorganizing those redundant functions into a single intelligence bureau.

TAS and IS-I regularly interact with DIIA on intelligence-related matters. TAS investigates threats to Congress and Directions of Interest. OSS refers threats and Directions of Interest to TAS. [redacted] The Department assigned a TAS agent to OSS. IS-I [redacted] investigates suspicious activity for any nexus to terrorism. [redacted]

TCD within SSB could benefit from increased interaction with DIIA on intelligence-related matters. TCD provides [redacted]

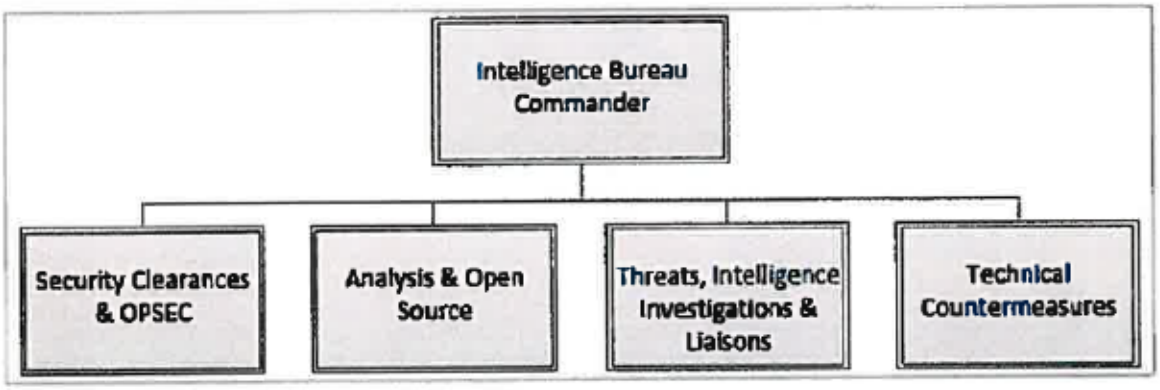
Reorganization and consolidation of these intelligence elements would increase the efficiency of its intelligence resources.

OIG Report Number [redacted] included a recommendation that the Department establish a formal Operational Security Program that incorporates appropriate guidance and industry best practices. The Special Security Section could be responsible for a formal operational security (OPSEC) program, however, officials stated the Department would need to reallocate additional resources to it as part of the reorganization.

[redacted]

[redacted] and develop more synergy throughout the Department. While OIG agrees with the Department's proposal to separate DIIA from PSB, the Department did not include all intelligence-related elements within the USCP reorganization. Integrating all of its intelligence-related elements such as the TAS, IS-I as well as TCD into a single bureau (as shown in Exhibit 3) would achieve greater collaboration and utilization of its intelligence resources.

Exhibit 3 – Example Organization Chart for an Integrated Intelligence Bureau



Source: OIG generated.

Lack of Memoranda of Understanding with Partner Intelligence and Law Enforcement Agencies

Although USCP partners with other intelligence and law enforcement agencies—including [redacted], USCP did not maintain the requisite MOUs. OIG requested the MOUs from PSB, Office of General Counsel (OGC) and Office of Human Resources (OHR) officials. After a considerable amount of time, OGC and OHR were able to provide a MOU for [redacted]. However, the Department could not provide MOUs for the other liaison positions. As a result, the Department did not have reasonable assurance that component analytic activities produced a product or resource investments in alignment with departmental priorities.

Department Not Maximizing Open Source Section Resources

[redacted] In the February 26, 2016 response to the draft report, the Department stated it will seek legal advice [redacted]

Conclusions

Opportunities exist for the Department to use its limited intelligence resources in a more efficient and effective manner. The Department should consider reorganizing its intelligence resources into a single bureau. USCP did not maintain MOUs with Federal intelligence agencies. As a result, the Department did not have reasonable assurance that component analytic activities produced a product or resource investments in alignment with departmental priorities. [redacted] Considering the February 26, 2016, Department response to the OIG draft report, we revised Recommendation 6. Accordingly, OIG makes the following recommendations.

Recommendation 4: We recommend that the United States Capitol Police (1) establish a strategic intelligence framework and priorities and use them to inform analytic activities, and (2) establish mechanisms for evaluating workforce initiatives and use results to determine any needed changes.

Recommendation 5: We recommend that the United States Capitol Police maintain the Memoranda of Understanding for its liaisons to ensure reasonable assurance that component analytic activities produce a product and resource investments are aligned with supported departmental priorities.

Recommendation 6: We recommend that the United States Capitol Police request a legal opinion from the Office of the General Counsel regarding the current Department of Justice and other legal standards [redacted]

APPENDICES

Listing of Recommendations

Recommendation 1: We recommend that the United States Capitol Police update and formalize standard operating procedures for the Division of Intelligence and Information Analysis addressing all of its Sections including threat assessments, the "Open Source Newsletter," and security clearances.

Recommendation 2: We recommend that the United States Capitol Police require that the Division of Intelligence and Information Analysis maintain copies of [redacted] as Department guidance (Standard Operating Procedure [redacted]) requires.

Recommendation 3: We recommend that the United States Capitol Police revise Standard Operating Procedures [redacted] to reflect any changes in processes for the Division of Intelligence and Information Analysis.

Recommendation 4: We recommend that the United States Capitol Police (1) establish strategic intelligence priorities and use them to inform analytic activities and (2) establish mechanisms for evaluating workforce initiatives and use results to determine any needed changes.

Recommendation 5: We recommend that the United States Capitol Police maintain the Memoranda of Understanding for its liaisons to ensure reasonable assurance that component analytic activities produce a product and resource investments are aligned with supported departmental priorities.

Recommendation 6: We recommend that the United States Capitol Police request a legal opinion from the Office of the General Counsel regarding the current Department of Justice and other legal standards [redacted]

DEPARTMENT COMMENTS

UNITED STATES CAPITOL POLICE
OFFICE OF THE CHIEF
119 D STREET, NE
WASHINGTON, DC 20510-7218

February 26, 2016

COP 151263

MEMORANDUM

TO: Ms. Fay F. Ropella, CPA,CFE
Inspector General

FROM: Kim C. Dine
Chief of Police

SUBJECT: Response to Office of Inspector General (OIG) draft report on *Evaluation of the United States Capitol Police Division of Intelligence and Information Analysis* (OIG-2016-04)

The purpose of this memorandum is to provide the United States Capitol Police's response to the recommendations contained within Office of Inspector General's draft report *Evaluation of the United States Capitol Police Division of Intelligence and Information Analysis* (OIG-2016-04).

The Department agrees with recommendations 1-5. With regard to Recommendation 6, the Department is aware that the Office of the General Counsel has provided advice in the past regarding [redacted] activities and techniques. However, given the dynamic nature of this technological area of [redacted] and its legal implications, the Department requests that the recommendation state: "We recommend that the United States Capitol Police request advice from the Office of the General Counsel regarding the current Department of Justice and other legal standards [redacted]

As always, we appreciate the opportunity to work with the OIG to further improve upon current policies and procedures currently in place. The Department will assign Action Plans to appropriate personnel regarding each recommendation 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,

Kim C. Dine
Chief of Police

cc: Matthew R. Verderosa, Assistant Chief of Police
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 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