



Review of United States Capitol Police Insider Threat Capabilities

Report Number 2023-I-0007

December 2023

~~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 loaned to the recipient. It is not to be distributed outside the United States Capitol Police or any agency or organization receiving it 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 any agency or organization receiving it. It is to be returned to the Office of Inspector General or the Capitol Police Board.~~

TABLE OF CONTENTS

	<u>Page</u>
At a Glance	1
Background	1
Results	2
Conclusion	6
Appendices	7
Appendix A – Objectives, Scope, and Methodology	8
Appendix B – Abbreviations and Acronyms	9
Appendix C – Department Comments	10

At a Glance

In accordance with our *Annual Performance Plan Fiscal Year 2023*, the Office of Inspector General (OIG) conducted a review of United States Capitol Police (USCP or Department) Insider Threat Capabilities. Our objectives were to (1) assess the Department's Insider Threat capabilities and (2) compare those practices to those of partner agencies. Our scope included operations, existing policies, and procedures related to the Department's Insider Threat capabilities.

The Department did not have a comprehensive Insider Threat Program (ITP) and lacked controls for mitigating insider threat concerns. USCP had some decentralized activities that aligned with insider threat best practices and minimum standards defined by the National Insider Threat Task Force (NITTF) but did not have a responsible individual or entity for overseeing cumulative insider threat activities.

Background

In October 2011, the President issued Executive Order 13587 establishing the NITTF under joint leadership of the Attorney General and the Director of National Intelligence. The President directed that Federal departments and agencies with access to classified information establish insider threat detection and prevention programs, and the NITTF to assist agencies in developing and implementing these programs.

The NITTF defines a threat posed to U.S. national security by someone who misuses or betrays, wittingly or unwittingly, their authorized access to any U.S. Government resource as an insider threat. The threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

According to PoliceNet,¹ the Department's Office of Information Systems (OIS) provides USCP with information and technology products and services. OIS provides services in the following areas:

- Enterprise Applications
- Radio Services
- Systems Operations
- Voice and Data Services
- Program Management and Governance
- Information Security

PoliceNet states the Intelligence and Interagency Coordination Division (IICD) gathers and disseminates intelligence to the USCP workforce and external partners in support of the protection of Members of Congress and the Capitol Complex.

Major functions include:

- Serving as the principal point of contact within the Intelligence Community for all domestic and foreign intelligence impacting the security of the U.S. Congress.
- 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.

¹ PoliceNet is the Department's intranet.

- Collecting and analyzing all sources of intelligence to identify domestic and international threats to the U.S. Capitol, Members of Congress, congressional facilities, congressional employees, and the visiting public.
- Briefing USCP Commanders, the Capitol Police Board, and other members of the Department regarding emerging tactics and threats posed by various terrorist groups or individuals.
- Producing daily, weekly, and monthly finished intelligence products to inform department personnel, including senior commanders and units in the field.
- Conducting all-source research and analysis in support of ongoing investigations.
- Implementing and managing the Department's Personnel Security Program.

Results

The Department did not have a comprehensive Insider Threat Program (ITP) and lacked controls for mitigating insider threat concerns. USCP had some decentralized activities aligned with insider threat best practices and minimum standards defined by the National Insider Threat Task Force (NITTF) but did not have a responsible individual or entity to oversee cumulative insider threat activities.


Insider Threat Best Practices

Although practices created by the NITTF are applicable to the executive branch, OIG research into best practices identified NITTF as the subject matter experts and USCP

would benefit from adherence to NITTF standards. NITTF states that the task force has drawn together expertise from across the Government in areas of security, counterintelligence, and information assurance to develop the policies and standards necessary for the individual department and agency (D/A) to implement insider threat programs. Part of the NITTF effort involves hosting training and providing D/As with assistance to better educate their workforce to recognize potential insider threat activity, without creating an atmosphere of distrust. NITTF conducts assessments of the adequacy of insider threat programs within individual D/As. Through its interface with individual D/As, NITTF identifies and circulates best practices for detecting, deterring and mitigating emerging threats, and continues to assist D/As in troubleshooting issues.

Additionally, the NITTF established the detection of potentially malicious behavior involves authorized insider threat personnel gathering information from many sources and analyzing that information for clues or behavior of concern. The NITTF also asserted the importance to consider relevant information from multiple sources for determining if an employee's behavior deserves closer scrutiny, or whether a matter should be formally brought to the attention of an investigative or administrative entity, such as the Federal Bureau of Investigation or an agency's Inspector General.

In November 2012, the President issued the National Insider Threat Policy and the Minimum Standards through a Presidential Memorandum. NITTF minimum standards outline best practices for meeting and creating a comprehensive program that tracks, collects, and analyzes information to identify anomalous behavior in order for



departments and agencies to deter, detect, and mitigate insider threats.

USCP Insider Threat Activities

As previously stated, USCP had some decentralized activities that aligned with insider threat best practices but did not have a responsible individual or section for overseeing insider threat concerns. For example, OIS requires that employees complete an annual security awareness training module.

Although the Department did not have an ITP, a Department official stated that USCP did, however, perform some of the NITTF best practices and worked with the Department's leadership to identify a senior official responsible for the ITP, although to date one has not been identified.

Additionally,



Based on the NIST framework, 


USCP had Security Awareness training that met many of the requirements such as threat monitoring and a section of the course did address ITP reporting.

Within IICD, most reports and investigations are unclassified and IICD is not a producer of intelligence but a consumer of derivative intelligence.

IICD had employees temporarily assigned—detailees—to other agencies, including the Federal Bureau of Investigation. In addition, the detailees provided bi-weekly “high side-Top Secret” briefings. Such briefings include inter-department and leadership discussions.

The Protective Service Bureau (PSB) manages the clearances for its IICD section

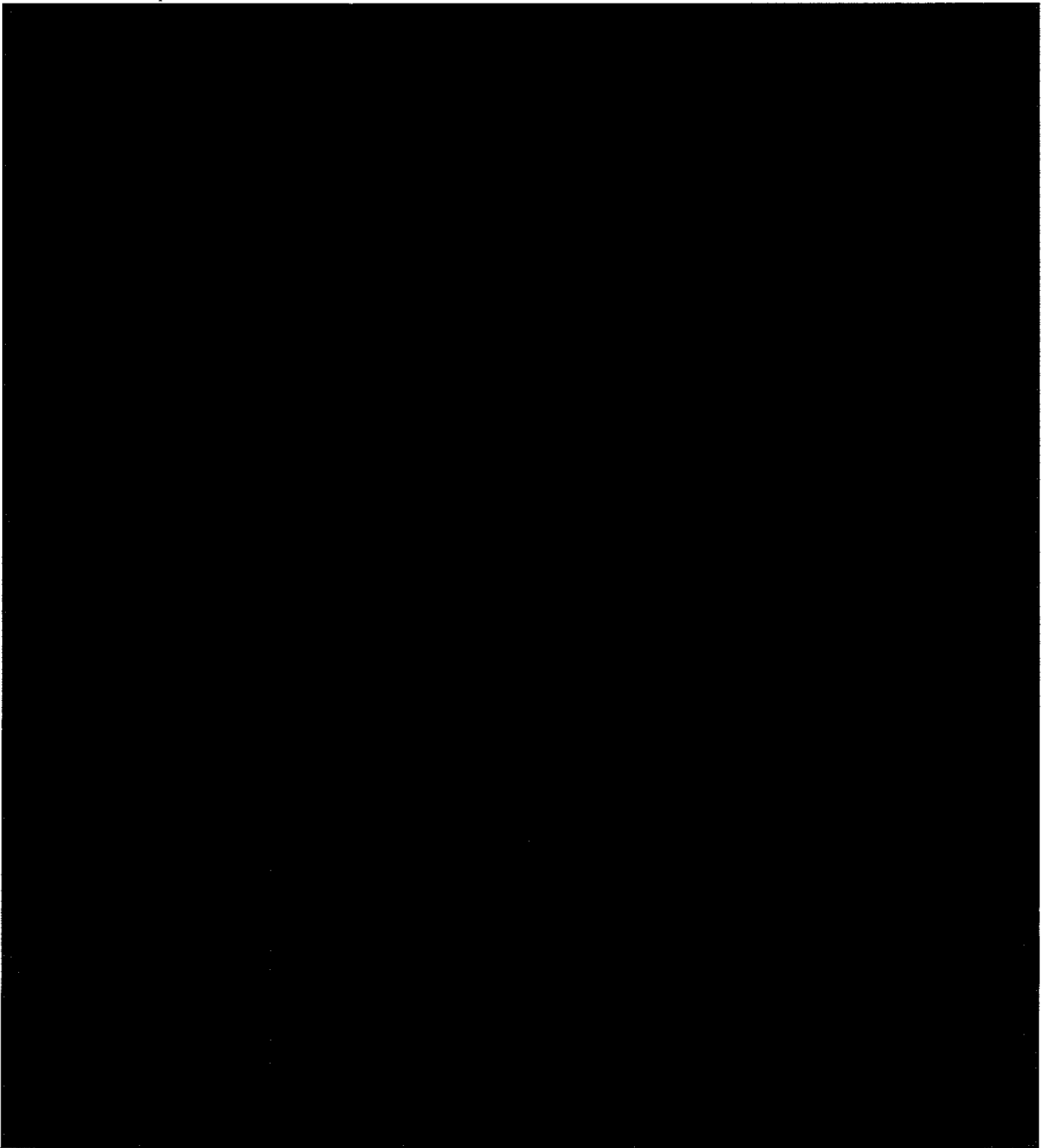
Additionally, the Department is in the process of recruiting a Security Manager. One of the initial tasks for the Security Manager will be to create Key Performance Indicators and publish those indicators throughout IICD. An Acting Security Manager is currently managing IICD sensitive compartmented information facility operations—but no new procedures have been added.

A Department official stated IICD lacks an ITP.

[REDACTED]. Other agency’s policies for document management are followed, although no repository for directives and any related process or program exists.

The following chart details aspects of NITTF standards that the Department has met or not established. Of the Department’s 22 ITP areas reviewed, the department had 1 area fully operational, 1 area was in the Initial Operating Stage, 9 areas were in the Initial Development or Infancy Phase, and 11 areas were either not in place or not started.

Task Force Requirements Reviewed



Conclusion

The Department did not have an Insider Threat Program for meeting the minimum standards set by the NITTF. However, USCP did have pre-existing insider threat-related controls and activities that met some of the minimum requirements. Thus, OIG makes the following recommendations.

Recommendation 1: We recommend that the United States Capitol Police formally designate an official responsible for overseeing insider threat concerns.

Recommendation 2: We recommend that the Department develop a comprehensive insider threat program that adheres to National Insider Threat Task Force minimum standards.

APPENDICES

Objective Scope and Methodology

In accordance with our *Annual Performance Plan Fiscal Year 2023*, OIG conducted a review of USCP Insider Threat Capabilities. Our objectives were to (1) assess the Department's Insider Threat capabilities and (2) compare those practices to those of partner agencies. Our scope included operations, existing policies, and procedures related to the Department's Insider Threat capabilities.

To accomplish our objectives, we conducted interviews with Department officials and reviewed USCP documentation related to insider threat capabilities. To research best practices, OIG reviewed National Insider Threat Task Force (NITTF) guidance and interviewed NITTF members.

We conducted this assessment in Washington, D.C., from March 2023 through August 2023. 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.

Abbreviations and Acronyms

Department/Agency	D/A
Employee Assistance Program	EAP
Intelligence and Interagency Coordination Division	IICD
Insider Threat Program	ITP
National Institute of Standards and Technology	NIST
National Insider Threat Task Force	NITTF
Office of the Inspector General	OIG
Office of Information Systems	OIS
Protective Service Bureau	PSB
Sensitive Compartmented Information Facility	SCIF
United States Capitol Police	USCP or Department

Department Comments



PHONE: 202-224-6806

UNITED STATES CAPITOL POLICE

OFFICE OF THE CHIEF
119 D STREET, NE
WASHINGTON, DC 20510-7218

December 15, 2023

COP 230537

MEMORANDUM

TO: Ron Russo
Inspector General

FROM: J. Thomas Manger
Chief of Police

SUBJECT: Response to Office of Inspector General draft report *Review of the United States Capitol Police Insider Threat Capabilities* (Report No. OIG-2023-I-0007)

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 *Review of the United States Capitol Police Insider Threat Capabilities* (Report No. 2023-I-0007).

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 Insider Threat Program. 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 "J. Thomas Manger".

J. Thomas Manger
Chief of Police

cc: Ashan M. Benedict, Assistant Chief, Protective and Intelligence Operations
Sean P. Gallagher, Assistant Chief, Uniformed Operations
Jason R. Bell, Assistant Chief, Standards and Training Operations
Magdalena Boynton, Chief Administrative Officer
[REDACTED] Program Manager/Audit Liaison

