UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Analysis of the
United States Capitol Police
Backup and Recovery Capabilities

Report Number OIG-2017-06

March 2017

~~*REPORT RESTRICTION LANGUAGE*~~

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

~~This report contains sensitive law enforcement material and is the property of the Office of the 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 Capitol Police Board, by them or by other agencies or organizations, without prior authorization by the Inspector General or the Capitol Police Board.~~

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. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and review of applicable documents.

We developed our recommendations based on the best knowledge available to OIG and discussed the 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, CPA, CFE
Inspector General

This page intentionally left blank

TABLE OF CONTENTS

Abbreviations and Acronyms

Continuity of Operations Plan	COOP
Fiscal Year	FY
Office of Information Systems	OIS
Office of Inspector General	OIG
Memorandum of Understanding	MOU
National Institute of Standards and Technology	NIST
Storage Area Network	SAN
Special Publication	SP
United States Capitol Police	USCP or the Department

EXECUTIVE SUMMARY

The United States Capitol Police (USCP or the Department) Office of Information Systems (OIS) administers the Department's backup and recovery process for most major systems. Each bureau and office develops its own Continuity of Operations Plan (COOP), which documents the essential functions of each bureau or office. The Mission Assurance Bureau collects the COOPs from each bureau or office and is responsible for the Department's overall COOP.

In accordance with our annual plan, the Office of Inspector General (OIG) conducted an analysis of the Department's backup and recovery capabilities for most major systems. The objectives of the analysis were to (1) review, analyze, and document policies and procedures for the data backup and recovery of USCP systems and applications, (2) observe operation of backup software and media, and (3) document USCP capability for recovering systems and applications within a defined recovery time objective.

The scope of the analysis included evaluation of controls, policies, and procedures during Fiscal Year (FY) 2016. In certain instances, we analyzed data from FY 2017 because it was the most recently available information at the time of our analysis. During our analysis, we became aware of other critical systems the Security Services Bureau and Command Center operate. Because those systems were outside of the scope of our analysis, we did not review the backup and recovery capabilities of the systems.

OIS had internal policies and procedures related to its backup and recovery process, namely, the [redacted] dated July 7, 2016, and the [redacted], dated September 20, 2013. However, the Department did not approve either of those directives. Without officially approved policy, the Department could not hold employees accountable for noncompliance with draft policies and personnel may not have been aware of their roles and responsibilities, which could have resulted in potential security control gaps.

[redacted]

According to the OIS COOP, the required recovery time objective for essential functions is [redacted]. That recovery time was tested on July 13, 2016, when power was lost at the primary data

center as a result of the janitorial staff accidentally activating the gaseous[1] fire suppression system. OIS successfully restored multiple critical systems at the backup data center before they could correct the power issue and all systems were back online at the primary data center within [redacted]. The incident demonstrated the ability of OIS to restore essential functions within their recovery time objective.

Several types of incidents could necessitate initiation of the recovery process. We believe that opportunities for improvement exist, which could help USCP recover should one of those incidents occur. For example, the Department did not have [redacted] USCP also did not develop a definition of a mission essential function. In addition, the Department did not have a fully developed COOP that encompassed all of its bureaus and offices. Finally, the Department did not have any memoranda of understanding with facility owners for locations it wanted to use as alternate work sites should a COOP scenario occur.

To develop more efficient and effective controls over the Department's backup and recovery process, ensuring security and support for business processes as well as the mission of USCP, we recommend that OIS formalize its internal policies and procedures. We also made other recommendations that, if implemented, would assist the Department in meeting its recovery time objectives in the event of an incident. See Appendix A for a complete list of OIG recommendations.

On March 9, 2017, OIG conducted an exit conference and on March 10, 2017, we provided a draft report to Department officials. We incorporated the Department's comments as applicable and attached their response to the report in its entirety in Appendix B.

Background

The United States Capitol Police (USCP or the Department) Office of Information Systems (OIS) backs up major systems. [redacted]

[1] USCP's primary data center employs an FM-200 fire suppression system that uses HFC-227ea (heptafluoropropane) gas to suppress fires.

OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with our annual plan, the Office of Inspector General (OIG) conducted an analysis of the Department's backup and recovery capabilities. The objectives of the analysis were to (1) review, analyze, and document policies and procedures of the data backup and recovery for USCP systems and applications, (2) observe operation of backup software and media, and (3) document the USCP capability for recovering systems and applications within a defined recovery time. The scope of the analysis included controls, policies, and procedures during Fiscal Year (FY) 2016. In certain instances, we analyzed data from FY 2017 because it was the most recently available information at the time of our analysis. During our analysis, we became aware of other critical systems the Security Services Bureau and Command Center operate. Because those systems were outside of the scope of our analysis, we did not review the backup and recovery capabilities of the systems.

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

- Nature and type of network backups
- Controls related to the backup and recovery process
- Encryption of backed up data
- Testing of network backups
- Department Continuity of Operations Plans (COOP)

To understand backup and recovery capabilities, we reviewed the following guidance:

- [redacted], dated July 7, 2016
- [redacted], dated March 25, 2016
- [redacted], dated September 20, 2013

We also used National Institute of Standards and Technology (NIST) guidance. As a legislative branch entity, many laws and regulations that apply to executive branch agencies do not apply to USCP. We believe, however, that those laws and regulations not only represent effective guidance but are also best practices for USCP.

OIG conducted this analysis in Washington, D.C., from December 2016 through March 2017. We did not conduct an audit, the objective of which would be the expression of an opinion on

Department programs. Accordingly, we do not express such an opinion. OIG did not conduct this analysis in accordance with generally accepted government auditing standards. Had we conducted an audit and followed such standards, other matters might have come to our attention. On March 9, 2017, we conducted an exit conference. On March 10, 2017, we provided a draft copy of this report to Department officials for comment. We incorporated Department comments as applicable and attached their response to the report in its entirety as Appendix B. ~~This report is intended solely for the information and use of the Department, the Board, and USCP Oversight Committees and should not be used by anyone other than the specified parties.~~

RESULTS

Overall, USCP developed policies and procedures for system data backup and recovery. The Department did not, however, complete the formal approval process for guidance such as the [redacted] dated July 7, 2016, or the [redacted], dated September 20, 2013. Although the Department was able to recover the systems within the defined recovery time objective [redacted], as the OIS COOP defines, we believe there are several areas for improvement that could assist the Department in meeting its recovery time objectives should an incident occur.

OIS Backup and Recovery Policies and Procedures

We reviewed, analyzed, and documented guidance entitled [redacted], dated July 7, 2016; [redacted], dated March 25, 2016; and [redacted], dated September 20, 2013. Although OIS developed internal policies and procedures related to the backup and recovery process, the Department did not complete the appropriate approval process for certain policies. Specifically, OIS did not seek approval from the Department for either the policy entitled [redacted], dated July 7, 2016, or the [redacted], dated September 20, 2013.

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Controls PM-1 states,

> The organization: develops and disseminates an organization-wide information security program plan that: Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.

Without officially approved policy, the Department could not hold employees accountable for noncompliance with draft policies and personnel may not have been aware of their roles and responsibilities, which could have resulted in potential security control gaps.

Conclusions

The Department did not approve draft policies and procedures for ensuring the process for security and integrity of the backup and recovery of systems. The lack of official Department policies could have placed it at increased risk of not being able to restore critical systems. We, therefore, make the following recommendation.

Recommendation 1: We recommend that the United States Capitol Police review and approve the [redacted] dated July 7, 2016, and the [redacted] policy, dated September 20, 2013.

[redacted]

Conclusions

We observed the operation of the backup software and media. We did not note any reportable issues to address in this section, and therefore do not have any recommendations.

Recovering Data Within Defined Recovery Time Objective

According to the OIS COOP, the recovery time objective for essential functions [redacted]. That requirement was tested on July 13, 2016, when power was lost at the primary data center when janitorial staff accidentally activated the gaseous fire suppression system. OIS successfully restored multiple critical systems at the backup data center before it could correct the power issue,

and all systems were back online at the primary data center within [redacted]. The incident demonstrated OIS ability to restore essential functions within the required recovery time. We believe, however, that there are opportunities for improvement, which could assist USCP in recovering its systems within the defined recovery time objective in the event of an incident.

[redacted]

[redacted]

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control CP-9 states, "the organization protects the confidentiality, integrity, and availability of backup information at storage locations."

[redacted]

Department-Level Mission Essential Functions

[redacted], dated March 25, 2016, defines a COOP as, "A predetermined set of instructions and procedures that describe how an organization's mission essential functions will be sustained within [redacted] However, according to Department officials, USCP did not have defined core mission essential functions for the Department. Bureaus in the Department are generally aware of essential functions, but no Department-wide definition of a mission essential function exists and each bureau and office defines its own mission essential functions, which may not align with the business requirements for the Department as a whole.

Department-Level Continuity of Operations Plan

According to NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control CP-2 Control Enhancement 1 states, "The organization coordinates contingency plan development with organizational elements responsible for related plans." USCP relies on each bureau to establish COOPs, and according to officials, the Department COOP does not encompass all of its bureaus. In addition, the [redacted] dated March 25, 2016, identifies COOP as an agency-wide document outlining the recovery process for OIS. According to the Mission Assurance Bureau and OIS officials, the above guidance is misleading as to the complete requirements of a successful COOP program. As a result, the guidance has led Department employees to believe that COOP is the

[redacted]

responsibility of OIS alone. Without establishing a Department-level COOP where the Department drives the priorities and requirements, each bureau and office will continue to define its own requirements. If activation of COOPs does occur, the Department may delay critical functions while resources work independently to continue individual bureau and office level functions.

Memorandum of Understanding for Alternate Work Locations

According to Department officials, USCP did not have a Memorandum of Understanding (MOU) with the various COOP locations and that some bureaus planned to [redacted] in the event headquarters and other USCP office locations are not available. NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control PE-17 states: "The organization (b) Assesses as feasible, the effectiveness of security controls at alternate work sites; and (c) Provides a means for employees to communicate with information security personnel in case of security incidents or problems." However, the Department lacks MOUs with facility owners that would allow them to use these facilities as COOP locations. Without documented agreements in place to use the alternate work locations, the locations may be unavailable, which could delay business continuity should the Department activate the COOP.

Conclusions

Although OIS demonstrated an ability to recover major systems within their recovery time objective during the incident that occurred on July 13, 2016, opportunities for improvement exist that could enhance the Department's ability to restore systems within recovery time objectives in the event of an incident. For example, [redacted]. In addition, USCP did not develop a Department-level definition of a mission essential function. The Department also did not have a fully developed COOP encompassing all Department bureaus and offices. Finally, USCP did not have an MOU with any facility owners for locations it planned to use as alternate work sites in the event of a COOP scenario.

Recommendation 2: We recommend that the United States Capitol Police consider acquisition and implementation of [redacted].

Recommendation 3: We recommend that the United States Capitol Police define Department-level mission essential functions. Once Department-level mission essential functions are established, we recommend each bureau align business priorities that satisfy mission essential function requirements. In addition, the United States Capitol Police should develop Department-level continuity of operations plan. Once the Department approves such a plan, each bureau must ensure that its plan aligns with the Department requirements.

Recommendation 4: We recommend that the United States Capitol Police revise [redacted], dated March 25, 2016, to

eliminate confusion regarding the Office of Information Systems responsibility for Department-wide continuity of operations.

Recommendation 5: We recommend that the United Stated Capitol Police establish a Memorandum of Understanding regarding [redacted]

APPENDICES

List of Recommendations

Recommendation 1: We recommend that the United States Capitol Police review and approve the [redacted], dated July 7, 2016, and the [redacted] policy, dated September 20, 2013.

Recommendation 2: We recommend that the United States Capitol Police consider acquisition and implementation of a [redacted].

Recommendation 3: We recommend that the United States Capitol Police define Department-level mission essential functions. Once Department-level mission essential functions are established, we recommend each bureau align business priorities that satisfy mission essential function requirements. In addition, the United States Capitol Police should develop Department-level continuity of operations plan. Once the Department approves such a plan, each bureau must ensure that its plan aligns with the Department requirements.

Recommendation 4: We recommend that the United States Capitol Police revise [redacted], dated March 25, 2016, to eliminate confusion regarding the Office of Information Systems responsibility for Department-wide continuity of operations.

Recommendation 5: We recommend that the United Stated Capitol Police establish a Memorandum of Understanding regarding [redacted].

DEPARTMENT COMMENTS

PHONE 202-224-9806

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

March 16, 2017

COP 170314

MEMORANDUM

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

FROM: Matthew R. Verderosa
Chief of Police

SUBJECT: Response to Office of Inspector General draft report *Analysis of the United States Capitol Police Backup and Recovery Capabilities* (Report No. OIG-2017-06)

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 *Analysis of the United States Capitol Police Backup and Recovery Capabilities* (Report No. OIG-2017-06).

The Department generally agrees with all of the recommendations and appreciates the opportunity to further improve upon the policies and procedures within the Office of Information Systems. The Department will assign Action Plans to appropriate personnel regarding each recommendation to achieve long-term resolution of each matter.

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,

Matthew R. Verderosa
Chief of Police

cc: Steven A. Sund, Assistant Chief of Police
Richard Braddock, Chief Administrative Officer
[redacted] USCP Audit Liaison

Nationally Accredited by the Commission on Accreditation for Law Enforcement Agencies, Inc.

This page intentionally left blank

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

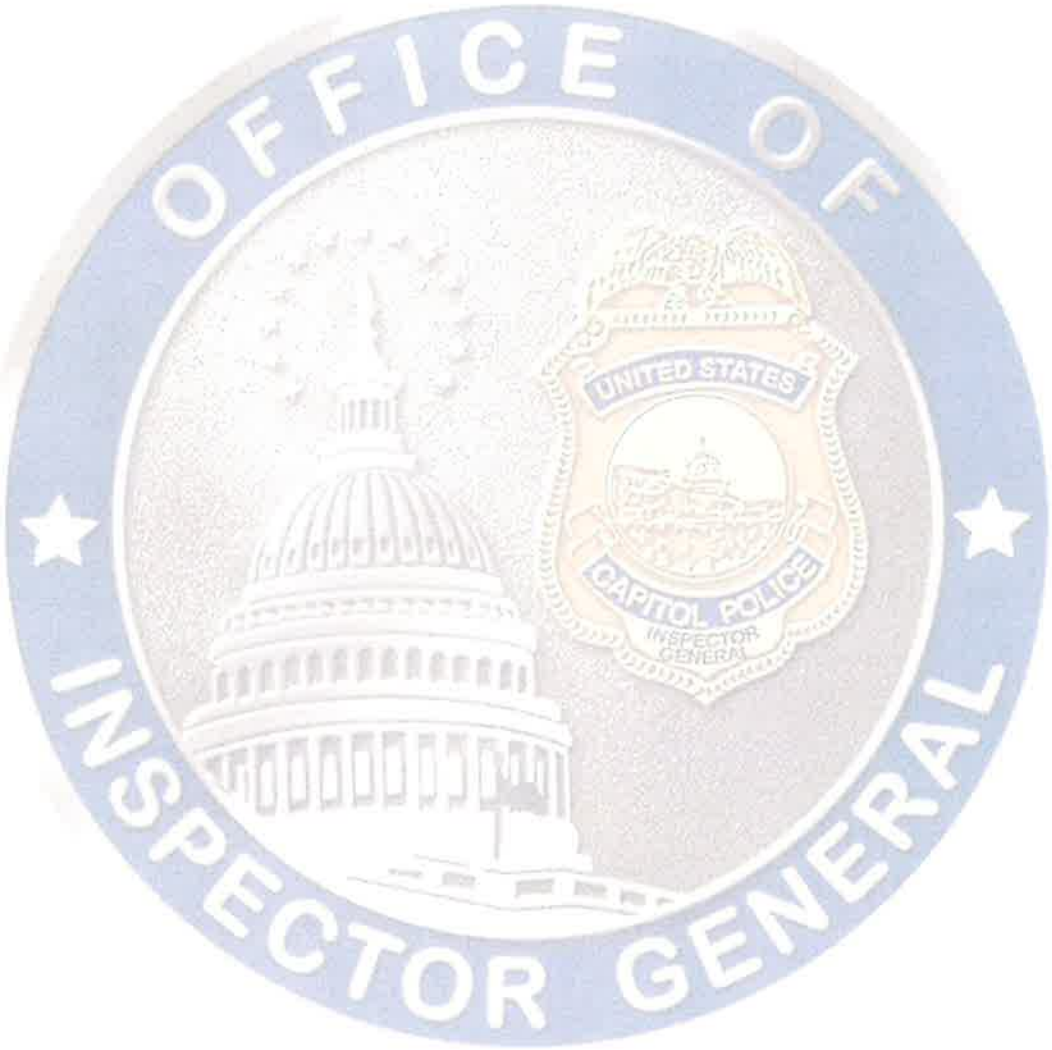
Write us:
United States Capitol Police
Attn: Office of Inspector General
499 South Capitol St. SW, Suite 345
Washington, DC 20510

Or visit us:
499 South Capitol Street, SW, Suite 345
Washington, DC 20003

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

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

Additional Information and Copies:
To obtain additional copies of this report, call OIG at 202-593-4201.


OFFICE OF
INSPECTOR GENERAL
UNITED STATES
CAPITOL POLICE
INSPECTOR GENERAL