UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Top Management Challenges Facing the United States Capitol Police

OIG-2018-02

October 2017

TABLE OF CONTENTS

Introduction

Annually, the Office of Inspector General (OIG) prepares a summary of the most significant management challenges facing the United States Capitol Police (USCP or the Department). The challenges reflect continuing vulnerabilities that OIG identified over the last several years as well as new and emerging issues the Department will face in the coming year. The Government Accountability Office (GAO) uses five criteria that reflect whether agencies met, partially met, or did not meet issues on its High-Risk Series—*Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others, GAO-17-317*, published February 15, 2017. The five criteria are:

- **Leadership Commitment** – Demonstrated strong commitment and top leadership support.
- **Capacity** – Agency with the capacity (that is, people and resources) to resolve risks.
- **Action Plan** – Corrective action plan defining the root cause and solutions as well as providing for substantially completing corrective measures, including steps necessary for implementing recommended solutions.
- **Monitoring** – Program instituted that would monitor and independently validate the effectiveness and sustainability of corrective measures.
- **Demonstrated Progress** – Ability to demonstrate progress in implementing corrective measures and resolving the high-risk area.

In 2016, OIG began using the above criteria to measure the Department's progress. Since our last report, the Department has shown solid, steady progress for the majority of its top management and performance challenges.

Of the five challenges on the 2017 list, at least four partially met all of the criteria for removal from the performance and management challenges. OIG narrowed Challenge One from 2017, *Interagency Communication, Coordination, and Program Integration Need Improvement,* to *Protecting and Securing the Capitol Complex*, because the Department strengthened how intelligence on terrorism, homeland security, and law enforcement information is shared and coordinated with its Federal, state, and local partners. *Challenge 5—Human Capital Management*—is still, however, in need of substantial attention. For FY 2018, Department challenges remain at five. Overall, progress has been possible through the concerted actions of the Chief of Police (Chief), the Chief Administrative Officer (CAO), and leadership and staff within the Department. This summary fulfills the OIG requirement under the *Reports Consolidation Act of 2000, Public Law 106-531*, to identify these management challenges, assess the Department's progress in addressing each challenge, and submit this statement to the Department annually.

Protecting and Securing the Capitol Complex (Challenge 1)

Protecting and securing the Capitol Complex from terrorists and weapons of mass destruction, while at the same time protecting Congress and its staff and welcoming the public, continues to be a major challenge. Like many departments within the Federal Government, USCP faces the challenge of coordinating programs for protecting people, facilities, and information. The Department has made solid and steady progress in strengthening interagency communication, coordination, and program integration with its partners—as demonstrated by USCP and its Federal and local partners in sharing intelligence information among protective service organizations on a real-time basis during June 14, 2017, shootings at the practice ballgame of congressional members as well as the 2017 presidential inauguration.

Source: abcnews.go.com.

Source: usatoday.com.

Source: cnn.com.

The Department revised its standard operating procedures to reflect changes in processes for its Division of Intelligence and Information Analysis and updated Memoranda of Understanding with the [redacted]

[redacted] as OIG recommended.[1] In addition, according to its *Strategic Plan for FY 2015-2019,* the Department employed smart policing with a transformational priority of implementing better internal and external communications as well as developing and integrating an enhanced operational planning capability. As a result of such efforts, we narrowed this challenge to protecting and securing the Capitol Complex.

While the progress is commendable, it does not mean USCP has eliminated all risk associated with coordinating and sharing terrorism-related information. It remains imperative that the Department and its partners continue their efforts. Continued oversight and attention is also warranted given the issue's direct relevance to homeland security as well as the constant evolution of terrorist threats and changing technology. OIG will continue to monitor this interagency coordination and communication, as appropriate, to ensure improvements are sustained.

As reflected in the recent attacks in Las Vegas, Alexandria, San Bernardino, and Orlando, protecting and securing the Capitol Complex from terrorists and weapons of mass destruction while protecting Congress and its staff is a major challenge for the Department. USCP must respond and deploy resources at a level of protection/security sufficient for scheduled or unanticipated events (such as demonstrations and suspicious packages) as well as changing and emerging threats on an open complex.

In several reports,[2] OIG made recommendations designed to bolster Capitol Complex security. [redacted]

The Department agreed with OIG that USCP could civilianize posts traditionally staffed by sworn officers within its Command Center and Communications Section. In a June 29, 2017, Senate Committee on Appropriations Subcommittee on Legislative Branch FY 2018 Budget Hearing, the Chief testified that the Department had reviewed the duties performed by officers that could be converted to civilian and had begun efforts to reassign officers in areas that would better meet operational requirements.

To help ensure a secure and open environment that has ever-changing mission requirements, USCP relies on overtime,[3] as do other Federal law enforcement organizations. As of September 2017, the Department did not have enough officers to

[1] *Evaluation of the United States Capitol Police Division of Intelligence and Information Analysis,* Report Number OIG-2016-04, dated March 2016.

[2] *Analysis of United States Capitol Police Internal Post Assignments*, Report Number OIG-2016-08, dated June 2016 and [redacted]

[3] *Analysis of the United States Capitol Police Overtime*, Report Number OIG-2017-13, dated September 2017.

cover regularly scheduled tours of duty. According to Department officials, recruiting for the next 4 years will be at capacity in order to simply bring on new officers to keep up with the emerging protection requirements.

Recruitment and continued training will be vital to successfully achieve operational focus in these areas for the Department: [redacted] and (3) civilianizing various positions as part of a multi-year plan to bolster Capitol Complex security and protection of congressional members.

Strengthening Cybersecurity Strategies to Address Increasing Threats (Challenge 2)

The President and Congress have both indicated that cyber threats are one of the most serious economic and national security challenges facing our Nation and that America's economic prosperity in the 21st century will depend on cybersecurity.[4] Each year, the threats posed by cybercriminals evolve into new and more dangerous forms, while security organizations must continually develop methods to keep pace and thwart potential attacks. As security threats become increasingly sophisticated and more numerous, USCP faces the challenge of reevaluating and expanding traditional approaches to security information technology (IT) systems. The Department must work to fulfill existing requirements while also implementing new strategies to meet the additional security demands of mobile technology, cloud-based computing, and other technological developments.

The Department relies on information technology (IT) security and management systems and other networks to help carry out vital missions and public services. To ensure that appropriations are spent wisely and vital Government missions are not compromised, the Department should continually improve all areas of IT and cybersecurity infrastructures.

[4] High-Risk Series: *Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others* GAO-17-317: Published: Feb 15, 2017.

The Department must also ensure that systems deployed are cost effective and meet requirements. In an era of rapidly changing technology, the Department is challenged not only in managing systems but also collecting, using, and disseminating law enforcement sensitive information.

Based on concerns of USCP Oversight Committees, OIG conducted audits of USCP information security program during 2016 and 2017:

- *Performance Audit of the United States Capitol Police Public Web Sites and Web Applications*, Report Number OIG-2016-05, dated March 2016
- *Performance Audit of the United States Capitol Police Mobile Device Program*, Report Number OIG-2016-10, dated August 2016
- *Analysis of the United States Capitol Police Backup and Recovery Capabilities*, Report Number OIG-2017-06, dated March 2017
- *Analysis of the United States Capitol Police Insider Threat Detection Program*, Report Number OIG-2017-08, dated June 2017

We also followed up on a prior enterprise architecture audit[5] and addressed the Office of Budget and Management (OMB) IT and cybersecurity priorities. Our September 2015 audit of the Department's information security program uncovered several significant weaknesses in the overall approach to information security.

USCP was performing well in certain areas of information security. For example, the Office of Information Systems (OIS) conducted regularly scheduled and managed vulnerability scanning. While positive efforts help mitigate the risk to USCP's information security program, addressing the conditions cited earlier is imperative. Implementing an effective information security program will not be an easy or quick process but will require significant attention and support from USCP senior management.

Increased levels of threat throughout the Federal Government demonstrate the need to implement OIG recommendations and to continue enhancing the Department's ability to defend its systems and data against increased cybersecurity threats and protecting sensitive information such as PII and law enforcement data. The Office of Personnel Management and the Department of Commerce notified some USCP employees that hackers had obtained their PII during a breach of their systems. Ensuring the security of Federal information systems and cyber-critical infrastructures should protect the privacy of PII.

[5] *Independent Audit of USCP Enterprise Architecture*, Report Number OIG-2012-01, dated December 2011.

According to the USCP OIS *Information Technology (IT) Strategic Plan for FY 2017-2021*, issued October 20, 2016, USCP recognizes the vital role of IT and radio communications as well as providing the necessary visibility and support to those IT initiatives. The plan reflects the Government-wide direction of leveraging cloud technologies, supporting the growing mobile workforce, and moving to a more efficient IT operation. The OIS plan also acknowledges building its security posture and prioritizing gaps and vulnerabilities is essential as it builds toward the security model of the future. "Educating every USCP employee about the potential threats and the role of the OIS security organization is paramount to protecting systems, data, and information. The OIS must secure and strengthen the IT infrastructure that enables information sharing to support the Department and its trusted partners."

Studies and surveys, including our audits,[6] showed that mobile devices drive productivity and most Federal organizations are encouraging mobility among employees. Use of mobile devices in the workforce has risks, however, and has increased the urgency and importance of security. The Department has made progress toward building a secure IT operation and partially met the criteria for removal. For example, as previously stated OIS developed and issued a strategic plan and closed all OIG recommendations in three reports and fully implemented four recommendations from other reports during FY 2017 as shown in Table 1.

Table 1 – Information Technology Recommendations Fully Implemented

Report Number	Title	Number of Recommendation(s) Closed
OIG-2012-01	*Independent Audit of USCP Enterprise Architecture*	5 Report closed
OIG-2015-10	*Performance Audit of the United States Capitol Police's Fiscal Year 2015 Information Security Program*	4 Report closed
OIG-2016-05	*Performance Audit of the United States Capitol Police Web Site and Web Applications*	4 Report closed
OIG-2016-10	*Performance Audit of the United States Capitol Police Mobile Device Program*	1
OIG-2017-06	*Analysis of the United States Capitol Police Backup and Recovery Capabilities*	2
OIG-2017-08	*Analysis of the United States Capitol Insider Threat Detection Program*	1

Source: OIG generated from its *Audits Recommendation Tracking System* for FY 2017.

[6] *Performance Audit of the United States Capitol Police Public Web Site and Web Applications*, Report Number OIG-2016-05, dated March 2016 and *Performance Audit of the United States Capitol Police Mobile Device Program*, Report Number OIG-2016-10, dated August 2016.

Strong, Integrated Internal Control Systems Still Needed (Challenge 3)

USCP managers are responsible for controlling the programs they oversee through internal control systems that bring about desired objectives, such as administering programs correctly and making payments accurately. Those internal controls consist of the policies, procedures, and organizational structures that collectively determine how a program is implemented and how requirements are met. In essence, internal controls are the tools managers use for ensuring that programs achieve intended results efficiently and effectively. They provide for program integrity and proper stewardship of resources. Because systemic control flaws can yield systemic program weaknesses—for example, unrealized objectives and improper payments—managers must continually assess and improve their internal control systems. Once a widespread deficiency is identified, managers must fix the problem before it undermines the program. Over the years, USCP has tended to resolve individual issues rather than strengthening the underlying systemically weak controls causing the issues.

- **Internal Controls** – In the *USCP FY 2016 Financial Statement* audit report, the independent auditor rendered an adverse opinion on the effectiveness of internal controls and reported a material weakness related to payroll processing. Those issues were repeated throughout FY 2010 through FY 2016.

  The CAO included compliance with internal controls into the performance plans for executives within the Office of Administration, along with self-risk assessments (as part of the Department's Force Development Program) and a 5-year schedule of control reviews starting in 2017. The step is important for ensuring that the internal controls program for the Department is given the appropriate attention within critical mission support functions that have the potential for fraud, waste or abuse.

- **Budget** – The Department still needs to ensure that formulation and execution of the budget are integrated with its strategic and business planning. The Department established a Performance Improvement Team designed to link the following activities for Force Development: Strategic Planning, Management and Planning, Communication, Leadership Capacity, Performance-Based Operations, and Learning and Sharing Knowledge, and other associated duties. According to USCP officials, implementation of the Department's new strategic plan allows the Department to begin integrating the Department's strategic goals and objectives with the Force Development Budget Process.

Managing Federal Contracting More Effectively (Challenge 4)

Agencies throughout the Federal Government have increasingly relied on contractors for executing missions. In FY 2017, the Department spent about $62 million on goods and services, which requires proper internal controls. The work of GAO and agency OIGs clearly demonstrate that Federal agencies often confront interrelated challenges. Those challenges include separating wants from needs, executing acquisition programs within available funding and established timeframes, using sound contracting arrangements with appropriate incentives and effective oversight, assuring that contractors are used only in appropriate circumstances and play proper roles, and sustaining a capable and accountable acquisition workforce. The Department must fully implement controls and procedures for purchase cards, travel cards, and acquisitions so contracting officers and contracting officer representatives adequately award, administer, and oversee procurement actions so contractors comply with the terms of the agreements.

The Department hired additional procurement staff, which resulted in improved contract administration and oversight. In addition, the Department provided refresher training for contracting officer representatives and appropriation law training for applicable personnel. However, effective internal controls are especially critical with new and major procurements. The Department should continue improving management of its acquisition processes and procedures, especially sole-source solicitations, in accordance with applicable principles of law and authorities. The Department also updated its acquisition policy and supporting procedures that adopt the intent and spirit of the *Federal Acquisition Regulation*. The Department has taken steps to fully implement the new procedures and realign Procurement directly under the CAO.

To follow up on areas of concern, OIG conducted an audit[7] of the Department's Purchase Card Program. The audit revealed that the Department did not design internal controls and processes in a way that would ensure successful implementation and administration over its Purchase Card Program. The Department's purchase card guidance[8] was outdated and

[7] *Performance Audit of the United States Capitol Police Purchase Card Program*, OIG-2017-11, dated August 2017.

[8] [redacted], September 20, 2011, and Standard Operating Procedure (SOP) [redacted], August 22, 2011.

inconsistent and did not provide sufficient monitoring and oversight for compliance. As a result, numerous non-compliance issues were brought to light.

OIG made eight recommendations, which the Department agreed to fully implement. The Department scheduled training for purchase cardholders and approval authorities for October 2017.

Human Capital Management Needs Improvement (Challenge 5)

Although making progress in improving human capital operations during the past year, the Department sometimes lacks the basic management capabilities needed to effectively and efficiently implement new programs and policies. The Department faces new and more complex challenges, including budget constraints, recruitment and training of new officers, and evolving security threats. As of September 30, 2017, although Congress authorized the Department a manpower workforce of 2,314, only 2,191 are assigned—with 123 sworn and civilian positions vacant as a result of of budget constraints.

As previously stated, auditors have reported the processing of payroll as a material weakness in previous financial statement audits for more than 6 years. As a result of findings related to the Department's time and attendance process, the Chief and CAO requested that OIG assist in further determining the adequacy, effectiveness, and efficiency of USCP policies, procedures, and internal controls over the Department's time and attendance processes and system. As of September 30, 2017, OHR had fully implemented all of the nine recommendations from the audit entitled *Agreed-Upon Procedures of USCP Time and Attendance* [redacted] *System* (OIG Report Number 2012-04.)

As experienced employees retire throughout the Department, they leave behind critical gaps in leadership and institutional knowledge, which could adversely affect the Department's ability to carry out its diverse responsibilities and missions and effectively respond to urgent issues. Critical to the success of transformation are agency employees, its human capital, and effective human capital management programs. Before implementing any human capital reforms, the Department must demonstrate that its human capital systems at a minimum meet certain conditions, including the following: (1) a strategic human capital planning process that links Department human capital efforts to mission and critical program goals; (2) capabilities for designing and implementing a new human capital system effectively; (3) a modern, effective, credible, and validated performance management system that provides a clear line of sight between individual performance and organizational outcomes; and (4) adequate safeguards that will ensure fair and equitable treatment of employees.

The Department must continue its efforts in addressing issues raised by auditors within the *USCP FY 2016 Financial Statement* audit report, as well as previous financial audit reports, regarding leave balance discrepancies within multiple human capital systems, and educating timekeepers and employees on proper time and attendance practices. In addition to issuing a new [redacted] in collaboration with the release of the upgraded [redacted] system, the Department continues to update staff on the new features of the system. According to the CAO, the Department has developed a corrective action plan to address this matter by the close of the calendar year 2017 leave year.

The Department must continue its plan to revise its performance management system and provide more meaningful goals and objectives to employees that link performance to the Department's overall strategic goals. The linkage will ensure that the leadership goals of the Department are carried throughout all layers of the Department.

Source: akc.org

OFFICE OF
INSPECTOR GENERAL
UNITED STATES
CAPITOL POLICE
INSPECTOR GENERAL