



## **UNITED STATES CAPITOL POLICE OFFICE OF INSPECTOR GENERAL**

### **Top Management Challenges Facing the United States Capitol Police Fiscal Year 2020**

**OIG-2020-02**

**October 2019**



## TABLE OF CONTENTS

	<u>Page</u>
Introduction	1
Top Management Challenges for Fiscal Year 2020	2
Protecting and Securing the Capitol Complex (Challenge 1)	2
Strengthening Cybersecurity Strategies to Address Increasing Threats (Challenge 2)	3
Strong, Integrated Internal Control Systems Still Needed (Challenge 3)	6
Managing Federal Contracting More Effectively (Challenge 4)	7
Human Capital Management Needs Improvement (Challenge 5)	7

## Introduction

Each year, 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 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—*Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, dated March 2019. 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 steady progress for the majority of its top management and performance challenges.

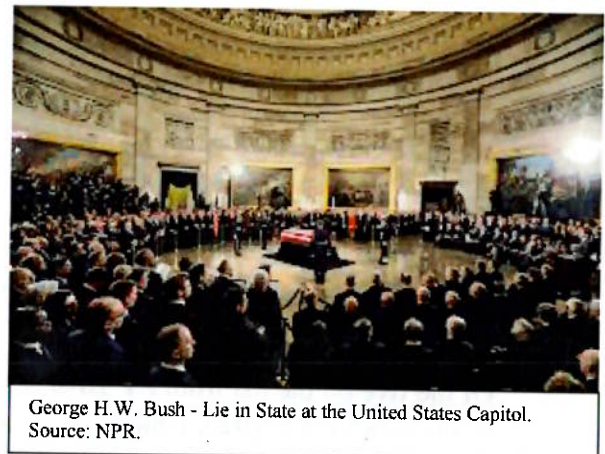
Of the five on the list from FY 2019, additional progress is needed for the management challenges for FY 2020, which remain at five. Overall, progress has been possible through the concerted actions of the Chief of Police (Chief), the Chief Administrative Officer (CAO), and leadership and staff within the Department. This summary fulfills the OIG requirement under the *Reports Consolidation Act of 2000, Public Law 106-531*, to identify the management challenges, assess the Department's progress in addressing each challenge, and submit this statement each year to the Department.

## Top Management Challenges for Fiscal Year 2020

### *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 consistent 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 the President’s State of the Union Address on February 5, 2019, and the funeral of George H.W. Bush. Additionally, in October 2019, USCP contained a pipe bomb at the Congressional Mail Facility and coordinated with a Federal partner to ensure that evidence was preserved to assist in identifying the suspect.



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 commendable, such progress does not mean USCP eliminated all of the risk associated with coordinating and sharing terrorism-related information, and the Department with its partners must continue their efforts. In addition, 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 increased amount of threats directed toward Members of Congress as well as increased mass shootings, 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. The Department must respond and deploy resources at a level of protection/security sufficient for scheduled or unanticipated events. Examples are mass demonstrations, concerts, and suspicious packages, as well as changing and emerging threats within an open complex.

In several reports,<sup>1</sup> OIG made recommendations designed to increase the security of the Capitol Complex. [REDACTED]

[REDACTED] Additionally, OIG made several recommendations for augmenting the Dignitary Protection Division.<sup>3</sup> In October 2019, the Department made organizational changes to better focus the intelligence capabilities of the Department by renaming and refocusing the Intelligence and Inter-agency Coordination Division. OIG will continue to monitor those efforts for addressing this management challenge.

---

### *Strengthening Cybersecurity Strategies to Address Increasing Threats* (Challenge 2)



According to GAO's High-Risk Series: *Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, dated March 2019, "Federal agencies and the nation's critical infrastructure are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being."

---

<sup>1</sup> *Analysis of United States Capitol Police Internal Post Assignments*, Report Number OIG-2016-08, dated June 2016 [REDACTED]

<sup>3</sup> *Follow-up Analysis of the United States Capitol Police Dignitary Protection Division*, Investigative Number 2019-I-0002, dated June 2019.



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 for meeting the additional security demands of mobile technology, cloud-based computing, and other technological developments.

The Department relies on IT security and management systems as well as 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.

The Department must also ensure that systems deployed are both cost effective and meet requirements. In an era of rapidly changing technology, the Department is challenged not only with 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 programs during 2017, 2018, and 2019:

- *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.
- *Analysis of the United States Capitol Police Monitoring of Internet Usage for Waste and Abuse*, Report Number OIG-2018-09, dated March 2018.
- *Analysis of the United States Capitol Police Email Security*, Report Number OIG-2019-06, dated March 2019.
- *Analysis of the United States Capitol Police Wireless Network and Devices*, Report Number OIG-2019-14, dated September 2019.

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 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 Personally Identifiable Information (PII) and law enforcement data.

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."

As previously stated, OIS developed and issued a strategic plan and closed several of the OIG recommendations made in cybersecurity related reports as shown in Table 1.

**Table 1 – Information Technology Recommendations Implemented**

Report Number	Title	Number of Recommendation(s) Closed
OIG-2012-01	<i>Independent Audit of USCP Enterprise Architecture</i>	5 Report closed
[REDACTED]	[REDACTED]	[REDACTED]
OIG-2016-05	<i>Performance Audit of the United States Capitol Police Web Site and Web Applications</i>	4 Report closed
OIG-2016-10	<i>Performance Audit of the United States Capitol Police Mobile Device Program</i>	8 Report closed
OIG-2017-06	<i>Analysis of the United States Capitol Police Backup and Recovery Capabilities</i>	4
OIG-2017-08	<i>Analysis of the United States Capitol Police Insider Threat Detection Program</i>	5 Report closed
OIG-2018-09	<i>Analysis of the United States Capitol Police Monitoring of Internet Usage for Waste and</i>	2 Report closed

	<i>Abuse</i>	
OIG-2019-06	<i>Analysis of the United States Capitol Police Email Security</i>	3 Report closed
OIG-2019-14	<i>Analysis of the United States Capitol Police Wireless Network and Devices</i>	0

Source: OIG generated from its Audits Recommendation Tracking System for FY 2019.

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

Over the years, USCP has tended to resolve individual issues rather than strengthening the underlying systemically weak controls causing the issues. 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.

- **Internal Controls** – In the *USCP FY 2018 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. Those issues were repeated from FY 2010 through FY 2018.

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. In FY 2019, the CAO implemented a dedicated team that will review and revise the Department's internal control directive as well as routinely review established internal controls and program operations throughout each fiscal year. Further, the Department formally established an Internal Controls and Risk Management Division to insure that this effort results in meaningful outcomes related to internal controls.

- **Budget** – The Department still needs to ensure that formulation and execution of the budget are integrated with its strategic and business planning. The Department



believes its efforts to develop a revised strategic plan that aligns to its mission and is meaningful to its workforce will better integrate its budget justification to its established strategic goals and objectives. OIG will continue to monitor this effort.

---

### ***Managing Federal Contracting More Effectively (Challenge 4)***

Agencies throughout the Federal Government have increasingly relied on contractors for executing missions. In FY 2019, the Department spent about \$90.7 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. Additionally, the Department must ensure that contracting officers and contracting officer representatives received certification training as required in order to ensure that proper internal controls can be maintained with the program.

OIG made recommendations designed to help the Department manage contracting more effectively. For example, OIG recommended that the Department collect performance data for contractors and track that information in a system that can be utilized by decision makers.<sup>4</sup>

---

### ***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, 2019, although Congress provided funding for a Department manpower workforce of 2458, only 2,295 were assigned—with 163 sworn and civilian positions vacant. The vacancy level resulted from two factors: (1) in order to fiscally plan for the execution of FY 2020 operations without a final budget, the Department began reducing its sworn and civilian hiring in mid-March 2019 to ensure it could support onboard staffing strengths during a potential continuing

---

<sup>4</sup> *Assessment of the United States Capitol Police Contractor Performance Monitoring*, Report Number OIG-2019-03, dated November 2018.

resolution; especially during a fiscal year when the Department must support operations to protect political conventions and pre-inauguration planning, and (2) the Department experienced challenges finding highly qualified applicants for sworn and civilian positions who can meet employment suitability standards. Because it is operating in FY 2020 under a continuing resolution, the Department must reduce its hiring efforts to meet its funded sworn and civilian staffing levels under a potential full-year continuing resolution. OIG will continue to monitor those efforts.

As previously stated, auditors have reported the processing of payroll as a material weakness in previous financial statement audits for a number of 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 "Workbrain" System* (OIG Report Number 2012-04.)

As experienced employees retire throughout the Department, they leave behind critical gaps in leadership and institutional knowledge, which can 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 CAO has advised OIG that the Department developed a draft human capital plan that incorporates diversity and inclusion; recruitment and retention; performance management; and training and succession planning. The CAO believes that incorporating those actions will ensure the appropriate linkage to the Department's mission and operations as described in Department strategic plan that is currently under revision.

The Department must continue its efforts in addressing issues raised by auditors within the *USCP FY 2018 Financial Statement* audit report, as well as previous financial audit reports, regarding employee and/or supervisor's failures to certify or approve bi-weekly timesheets timely and noncompliance with employee clock usage policy.

The Department implemented a revised performance management system designed to provide more meaningful goals and objectives for employees that link performance to the

Department's overall strategic goals. Such a link will ensure that the leadership goals of the Department are carried throughout all layers of the Department. The key to successful implementation of the new process will be the effective training of supervisors and employees on the linkage and the meaningful application of performance expectations into daily operations. OIG will continue to monitor the effort.



