UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Top Management Challenges Facing the United States Capitol Police Fiscal Year 2021

OIG-2021-04

January 2021

TABLE OF CONTENTS

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 fiscal year. Based on its High-Risk Series—*Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas, GAO-19-157SP*, dated March 2019—the Government Accountability Office (GAO) uses five criteria that reflect whether agencies met, partially met, or did not meet issues. 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 GAO 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 Fiscal Year (FY) 2020, additional progress is needed for the management challenges for FY 2021, 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.

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 welcoming the public continues to be a major challenge. In addition, during an unprecedented time with the outbreak of the coronavirus of 2019 (COVID-19) and the restrictions imposed resulting from the pandemic adds additional challenges to the Department in securing the Capitol Complex.

According to its *Strategic Plan FYs 2021-2025,* there are three essential aspects to ensuring the Department's ability to respond successfully, regardless of the challenges and complexities of the situation being addressed. They are: (1) a USCP sworn and civilian workforce instilled with the necessary specialized skills, capacity, and leadership support; (2) operational agility based on the best use of information and technology; and (3) strong partnerships across the law enforcement community. As a result of such efforts, we narrowed Challenge 1 to protecting and securing the Capitol Complex.

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 4, 2020, and the funeral of Representative John Lewis.

2020 State of the Union Address.
Source: Los Angeles Times.

Representative John Lewis – Lie in State at the United States Capitol.
Source: Washingtonian.

While commendable, such progress does not mean that 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 number of threats directed toward Members of Congress as well as increased social unrest, 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 of such events include mass demonstrations, the most recent election and inauguration, and suspicious packages, as well as changing and emerging threats within an open complex.

In several reports,[1] OIG made recommendations designed to increase the security of the Capitol Complex. For example, OIG recommended that the Department expand entry-level and in-service training related to pre-screening at various building access points.[2] Additionally, OIG made several recommendations regarding USCP's [redacted] 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 *Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, "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."

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

[1] *Assessment of the United States Capitol Police Pre-Screener Program,* Investigative Report Number 2019-I-0007, dated December 2019, *Follow-up Audit of the United States Capitol Police Canine (K-9) Program,* Report Number OIG-2020-08, dated March 2020, and [redacted]

[2] *Assessment of the United States Capitol Police Pre-Screener Program,* Investigative Report Number 2019-I-0007, dated December 2019.

[redacted]

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 2018, 2019, and 2020:

- *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.
- [redacted]

USCP has performed well in certain areas of information security. For example, the Office of Information Systems (OIS) conducted regularly scheduled and managed vulnerability scanning. Positive efforts help mitigate the risk to USCP's information security program, helping address conditions cited earlier. 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 types of 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 because those areas help build toward the security model of the future. The OIS Plan states, "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." In addition, according to the Department's FY 2021-2025 Strategic Plan, goal 3—Enhance information gathering, analysis, utilization, and dissemination—the Department will optimize and leverage the use of technology to enhance data analysis and information dissemination.

As previously stated, OIS developed and issued its strategic plan and closed several of the OIG recommendations made in cybersecurity related reports 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*	8 Report closed
OIG-2017-06	*Analysis of the United States Capitol Police Backup and Recovery Capabilities*	4
OIG-2017-08	*Analysis of the United States Capitol Insider Threat Detection Program*	5 Report closed
OIG-2018-09	*Analysis of the United States Capitol Police Monitoring of Internet Usage for Waste and Abuse*	2 Report closed

OIG-2019-06	*Analysis of the United States Capitol Police Email Security*	3 Report closed
OIG-2019-14	*Analysis of the United States Capitol Police Wireless Network and Devices*	4 Report closed
[redacted]	[redacted]	[redacted]

Source: OIG generated from its *Audits Recommendation Tracking System* for FY 2020.

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

Over the years, USCP has generally resolved 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 2019 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 2019. During FY 2020, USCP made significant improvements surrounding its internal controls related to payroll, and the FY 2020 Financial Statement audit report included an unmodified opinion on internal controls over payroll. However, one significant deficiency related to payroll remained during the FY 2020 audit.

  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 ensure 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. Objective 4.1.1 of the updated *Strategic Plan FYs 2021-2025* states that the Department will "Reaffirm through the established budgetary process that the USCP's Congressional budget justification remains balanced across all needs—workforce costs, technology expenditures, equipment, and other critical asset requirements." 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. 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.[4]

Human Capital Management Needs Improvement (Challenge 5)

In October 2020, the Department issued its *Human Capital Strategic Plan 2021-2025,* which is aligned with the Department's mission and directly supports the Department's *Strategic Plan FYs 2021-2015*. The Plan focuses on hiring, developing, and retaining the

[4] *Assessment of the United States Capitol Police Contractor Performance Monitoring*, Report Number OIG-2019-03, dated November 2018.

high-performing workforce needed to achieve its strategic goals. The Plan not only provides Department leaders and employees with the structure for fostering a workplace culture where employees are valued for their backgrounds, abilities, and ideas but also understanding their vital roles in achieving the Department's critical mission. 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, 2020, although Congress provided funding for a Department manpower workforce of 2,478, only 2,268 were assigned—with 210 sworn and civilian positions vacant. The vacancy level was the result of four factors: (1) in order to fiscally plan for the execution of FY 2021 operations without a final budget, the Department began reducing its sworn and civilian hiring in mid-March 2020 to ensure it could support onboard staffing strengths during a potential continuing resolution (CR) in FY 2021; (2) the onset of the COVID-19 pandemic in March 2020 resulted in the suspension of sworn training and limited the ability of the Department to process sworn and civilian applicants based on public health limitations; (3) the Department was faced with mandatory retirement benefit contribution increases starting in FY 2021 totaling $52 million that had to be absorbed during an FY 2021 CR; and (4) the Department experienced challenges finding highly qualified applicants for sworn and civilian positions who can meet employment suitability standards. Because FY 2021 began under a CR, the Department reduced its hiring efforts to meet its funded sworn and civilian staffing levels under a potential full-year CR, as well as fund noted increased benefits costs. OIG will continue to monitor those efforts.

As previously stated, auditors reported the processing of payroll as a material weakness in previous financial statement audits for a number of years prior to FY 2020. 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, the Office of Human Resources 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). During FY 2020, USCP made significant improvements surrounding its internal controls related to payroll, and the FY 2020 Financial Statement audit report included an unmodified opinion on internal controls over payroll. However, one significant deficiency related to payroll remained during the FY 2020 audit.

As experienced employees retire throughout the Department, they leave behind critical gaps in leadership and institutional knowledge. Those gaps 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 an effective human capital management program. The Department developed *Human Capital Strategic Plan 2021-2025*, which incorporates diversity and inclusion, recruitment and retention, performance management, and training and succession planning. The CAO believes that those actions will ensure the appropriate linkage to the Department's mission and operations as described in the Department's *Strategic Plan FYs 2021-2025*.

The Department must continue its efforts in addressing issues raised by auditors within the *USCP FY 2020 Financial Statement* audit report, as well as previous financial audit reports, regarding 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 monitoring such an effort.

OFFICE OF
INSPECTOR GENERAL
UNITED STATES
CAPITOL POLICE
INSPECTOR GENERAL