STATEMENT OF INSPECTOR GENERAL MICHAEL A. BOLTON
UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Committee on House Administration
United States House of Representatives
July 16, 2019

Good morning and thank you for the opportunity to appear before the Committee on House Administration to discuss Oversight of the United States Capitol Police. My name is Michael A. Bolton. I am the Inspector General for the United States Capitol Police (USCP or Department). I have been with the Inspector General's office since 2006 and was appointed as the Inspector General in January 2019.

I would like to thank the Committee for its sustained and unwavering support of the United States Capitol Police, Office of Inspector General (OIG). The OIG is dedicated to ensuring that the Department, Board, and Committees are accurately informed of audit and investigative reviews through the submission of our independent reports. These comprehensive reports serve the Department in achieving the goals of their mission in providing a financially responsible operation as well as, a safe and secure environment for all members, staff, public employees, and visitors to the Capitol complex. However, none of this would be possible without the support of Congress and that of the Capitol Police Board. We very much appreciate our discussions with you and your staff about our work and future projects. These discussions have provided us with a regular opportunity to provide the Committee with important updates about our activities, challenges and focus.

The Inspector General Act establishes for most agencies an OIG and sets out its mission, responsibilities, and authority. The unique nature of the IG function can present a number of challenges for establishing and maintaining effective working relationships. To work most effectively together, the agency and its OIG need to clearly define what each considers a productive relationship and then consciously manage toward that goal in an atmosphere of mutual respect.

By providing objective information for promoting Government management, decision-making, and accountability, OIG contributes to the agency's success. OIG is an agent of positive change, focusing on eliminating waste, fraud, and abuse, and on identifying problems and recommendations for corrective actions by agency leadership. OIG provides the agency, Board, and Congress with objective assessments of opportunities to be more successful. Although not under the direct supervision of the Chief, OIG must keep the Board and Congress fully informed of significant OIG activities. Given the complexity of management and policy issues, OIG and the agency may sometimes disagree on the extent of a problem and the need for and scope of corrective action. However, such disagreements should not cause the relationship between OIG and the agency to become unproductive.

The Office of Inspector General is comprised into three areas of responsibility: Audits, Investigations, and Administration. Audits examines the economy and efficiency of USCP programs and operations, including program results, compliance with applicable laws and regulations, and fair presentation of financial reports. OIG conducts audits which are accomplished in accordance with generally accepted government auditing standards (GAGAS) published by the Comptroller General of the United States.

Investigations utilizes specific law enforcement authorities, tools, and techniques to conduct investigations and prevent fraud, waste, and abuse in the programs and operations of USCP. Investigative work is intended to result in appropriate actions to resolve allegations and to prevent and deter future instances of illegal or fraudulent acts or misconduct. In addition, Investigations conducts systematic and independent reviews and investigations of operations. Reviews are generally focused on management and internal controls and investigations are generally in response to allegations of employee misconduct or mismanagement issues. Furthermore, Investigations maintains the OIG Hotline, a confidential channel for complaints or concerns about violations of laws or regulations, gross waste of funds, abuse of authority, or mismanagement.

Administration ensures that the people, money, technology and equipment, and policies are in place so that OIG can function efficiently and effectively. Responsibilities include asset management; budget formulation and execution; human resources; workplace training; information technology; and policy preparation for OIG. Administration also facilitates OIG's planning and reporting activities and prepares crosscutting documents on OIG accomplishments.

I recently hired a new Assistant Inspector General for Investigations, a former United States Secret Service Special Agent with an extensive background in Protective Operations, Training, Internal Investigations, and Inspections. I also promoted an internal OIG employee to the position of Assistant Inspector General for Audits, who is not only a Certified Public Accountant, and a Certified Fraud Examiner, but is also s experienced and knowledgeable regarding Cybersecurity (IT) matters. In addition, because of FY 2019 budget request, I hired an Attorney Adviser/Auditor as a dual-purpose position to provide legal counsel and conduct audit work within the OIG. These highly qualified employees will provide the OIG and the Department with a fresh look at the various challenges that face the Department in the coming years.

Annually, the OIG prepares a summary of the most significant management challenges facing 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— *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 solid, steady progress for the majority of its top management and performance challenges.

The top Management Challenges facing the Department are: (1) Protecting and Securing the Capitol Complex, (2) Strengthening Cybersecurity Strategies to address increasing threats, (3) Strong Integrated Internal Control Systems, (4) Managing Federal Contracting more effectively, and (5) Human Capital Management.

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.

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 Department of Homeland Security and the Federal Bureau of Investigation as OIG recommended. 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. Because of such efforts, we narrowed this challenge to protecting and securing the Capitol Complex.

While 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.

In several reports, OIG made recommendations designed to bolster Capitol Complex security. For example, OIG recommended that the Department expand its counter surveillance (pre-screening) program by including committee hearings as well as outside entry points such as garages. Counter surveillance can be used as a tool for detecting and preventing disruptions as well as providing additional security.

The Congress has 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. 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.

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.

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, 2018, although Congress provided funding for a Department labor workforce of 2,363, only 2,283 were assigned-with 80 sworn and civilian positions vacant. The vacancy level resulted from two factors: (1) in order to fiscally plan for the execution of FY 2019 operations without a final budget (signed into law September 21, 2018), the Department began reducing its sworn and civilian hiring in mid-July to ensure it could support onboard staffing strengths during a potential continuing resolution: and (2) the Department experienced challenges finding applicants for civilian positions who can meet employment suitability standards. Because it is operating in FY 2019 under a full appropriation, the Department has resumed its hiring efforts to meet its funded sworn and civilian staffing levels. OIG will continue to monitor these efforts.

The Department recently implemented a revised performance management system designed to provide goals that are more meaningful as well as, 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. The Department is in the process of formulating their Strategic Plan for FY 2020 and beyond, to achieve its mission and to ensure that diversity, inclusion, equity and associated data analytics are at the forefront for the Department and employees. In addition, OIG will continue to review the Department's compliance with laws, regulations, policies and procedures related to Discipline as the Department moves forward in this ever-changing environment.

Of the five challenges on the FY 2018 list, at least four partially met all of the criteria from the performance and management challenges. OIG narrowed Challenge 1 from 2018, *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 attention. For FY 2019, 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.

Thank you for the opportunity to appear before you today. I would be very happy to answer any questions the Committee may have at this time.