OFFICE OF INSPECTOR GENERAL

Testimony of Inspector General John Roth

Before the Subcommittee on Transportation and Protective Security

Committee on Homeland Security

U.S. House of Representatives

“How Can the United States Secret Service Evolve to Meet the Challenges Ahead?”

Homeland Security

June 8, 2017
2:00 PM

DHS OIG Highlights

"How Can the United States Secret Service Evolve to Meet the Challenges Ahead"

June 8, 2017

Why We Did This

The inspections and audits discussed in this testimony are part of our ongoing oversight of the Secret Service. Our reviews are designed to ensure the efficiency and effectiveness of Secret Service operations.

What We Recommend

We made numerous recommendations in these reports. Our recommendations are aimed at helping the Secret Service improve its ability to execute its important mission.

For Further Information:
Contact our Office of Legislative Affairs at (202) 254-4100, or email us at
DHS-OIG.OfficeLegislativeAffairs@oig.dhs.gov

What We Found

This testimony highlights three of our recent reviews:

- *The Secret Service Has Taken Action to Address the Recommendations of the Protective Mission Panel* – We concluded that the Secret Service has clearly taken the Protective Mission Panel's recommendations seriously, but fully implementing changes and resolving underlying issues will require a multi-year commitment and depend heavily on adequate funding and staffing.

- *DHS Is Slow to Hire Law Enforcement Personnel* - From fiscal years 2011 through 2015, the Secret Service came close to meeting or met authorized staffing levels for Special Agents and Uniformed Division Officers, but significant hiring delays continued. The Secret Service has made changes to improve its law enforcement hiring process and shorten the amount of time it takes to hire personnel, but most of the changes are relatively new and their long-term success cannot yet be measured.

- *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data* – The Secret Service did not have adequate protections in place on sensitive case management systems. Although the Secret Service recently initiated steps to improve its IT management structure, it will take time to fully implement these improvements and demonstrate effectiveness.

DHS Response

DHS concurred with our recommendations.

Chairman Katko, Ranking Member Watson Coleman, and Members of the Subcommittee:

Thank you for inviting me here today to discuss our work relating to the United States Secret Service (Secret Service). We have conducted a number of investigations, audits, and inspections of Secret Service programs and operations and have made several recommendations. My testimony today will describe some of that work and discuss its implications.

Our most recent oversight of the Secret Service has focused on three key operational areas: the Secret Service's actions to address recommendations of the Protective Mission Panel, difficulty in hiring law enforcement personnel, and challenges protecting sensitive case management systems and data.[1] In general, the Secret Service has taken action to address the concerns and challenges identified by our office. Although we have seen encouraging progress, many of the implemented changes require long-term commitment and planning. We will continue to monitor the Secret Service's progress in implementing our recommendations over time.

The Secret Service Has Taken Action to Address Recommendations of the Protective Mission Panel

Following the September 19, 2014 White House fence jumping incident, the Secretary of Homeland Security established the Protective Mission Panel (Panel) to undertake a broad independent review of the Secret Service's protection of the White House Complex (WHC). The Panel made 19 recommendations in its December 2014 unclassified report. To address the Panel's findings and recommendations, we verified and evaluated actions the Secret Service has planned and taken since December 2014.

One of the Panel's major criticisms was that the Secret Service had never developed a budget process that articulated its mission or a corresponding staffing and budget plan to meet its needs. Historically, as its operational tempo has increased, the Secret Service has often solved short-term problems at the expense of long-term ones, such as deferring technology upgrades to pay for operational travel, or paying large amounts of overtime rather than fixing the hiring process. To cure this, the Secret Service developed a "mission-based

[1] *The Secret Service Has Taken Action to Address the Recommendations of the Protective Mission Panel*, OIG-17-10 (November 2016); *DHS Is Slow to Hire Law Enforcement Personnel*, OIG-17-05 (October 2016);*USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*, OIG-17-01 (October 2016).

budget" for fiscal year 2018,[2] which should start addressing many of the causes of equipment and personnel shortfalls.

We estimate that it will require the Secret Service to have about 8,225 personnel, known as "full time equivalents" (FTE) by 2022, up from the FY 16 level of about 6,500, in order to have sufficient personnel to conduct its mission, including the very critical element of training. We think that the President's request for FY 2018 for 450 more personnel is a step in the right direction, but will be insufficient to meet current needs. Inadequate workforce strength results in little or no training, mistakes due to workforce fatigue, decreased quality of work life, poor morale, and increased attrition. Until the Secret Service can hire and retain a workforce at or exceeding its workforce staffing models, this will continue to be a problem. Compounding this problem is Secret Service's inability to hire efficiently, as I discuss below.

The Panel also found — and we have confirmed through subsequent reviews — that the Secret Service has not kept pace with technological advancements. Instead of investing in cutting edge technology and driving research and development, the Secret Service has relied on outdated systems and equipment, with potentially dangerous consequences. For example, in our January 2016 report on the Secret Service's radio systems, we found that many radios were well beyond their recommended service life and that many manufacturers had stopped making several of the major system components, making repairs difficult.[3] Then, in April 2016, we reported that a confluence of technical problems with radios, security equipment, and notifications impeded the Secret Service's ability to apprehend an intruder who jumped over the North Fence and entered the White House in September 2014.[4] To update and enhance its technology, the Secret Service has committed funding to technology refreshes, is pursuing new technology, and has appointed civilians with specialized expertise to critical leadership roles, including Chief Information Officer and Head of the Office of Technical Development and Mission Support.

The Panel also asserted the Secret Service is insular and does not regularly learn from its external partners. To address the Panel's recommendations to engage with Federal and international partners, the Secret Service hosted more joint training exercises; sought to obtain periodic, outside assessments of the threats to and strategies for protecting the WHC; and engaged foreign protective services through events. However, the Secret Service has not yet

[2] U.S. Secret Service Fiscal Year 2018 Congressional Justification
[3] *U.S. Secret Service Needs to Upgrade its Radio Systems*, OIG-16-20 (January 2016).
[4] *2014 White House Fence Jumping Incident (Redacted)*, OIG-16-64 (April 2016).

evaluated these partnerships or established regular exchanges of knowledge, and staffing constraints limit joint training, as well as partner outreach. Leading the Federal protective force community, obtaining periodic outside assessments, and coordinating with international partners will require sustained support from Secret Service leadership and the flexibility to carry out these actions in the face of protective mission demands.

In short, the Secret Service has clearly taken the Panel's recommendations seriously, which it has demonstrated by making a number of significant changes.[5] Specifically, the Secret Service improved communication within the workforce, better articulated its budget needs, increased hiring, and committed to more training of its workforce. Additionally, using funding appropriated for Panel initiatives, the Secret Service began enhancing security and refreshing technology at the WHC. It has also begun working with stakeholders on plans to construct a new outer fence surrounding the WHC.

Nevertheless, there continues to be room for improvement, and we made five recommendations in our unclassified November 2016 report to further the Secret Service's progress in addressing the Panel's recommendations. That report makes additional recommendations that we believe will further strengthen the Secret Service. However, fully resolving underlying issues and implementing necessary changes will require a multi-year commitment and depend heavily on adequate funding and staffing. In addition, we recently issued a classified report reviewing the Secret Service's actions to address the Panel's classified recommendations.[6]

DHS Is Slow to Hire Law Enforcement Personnel

In October 2016, we issued a report on the results of our review of the law enforcement hiring processes at three components: U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Secret Service.[7] We identified several issues with all three components' law enforcement hiring processes. Today, I will focus on those we identified at the Secret Service.

From fiscal years (FYs) 2011 through 2015, the Secret Service came close to meeting or met authorized staffing levels for Special Agents and Uniformed Division (UD) Officers.

[5] *The Secret Service Has taken Action to Address the Recommendations of the Protective Mission Panel*, OIG-17-10 (November 2016).
[6] *The Secret Service Has Taken Action to Address the Classified Recommendations of the Protective Mission Panel* (Unclassified Summary), OIG-17-47 (March 2017).
[7] *DHS Is Slow to Hire Law Enforcement Personnel*, OIG-17-05 (October 2016).

Percentage of Secret Service Authorized Law Enforcement Positions Filled, FYs 2011–15

	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015
Special Agents	100%	97%	94%	100%	95%
UD Officers	100%	97%	93%	94%	87%

However, the Secret Service continues to be challenged by significant hiring delays. The table below shows the average number of days it took to hire Special Agents and UD Officers through job announcements issued in that fiscal year.

Secret Service Average Days-to-Hire, FYs 2011–15[8]

	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015
Special Agents	286	–	482	441	298
UD Officers	–	–	294	272	359

The Secret Service will be continued to be challenged by a lack of dedicated human resources staff, which lengthens the Secret Service's hiring process. At the end of FY 2015, for example, 32 percent of human resources positions at the Secret Service were vacant. Hiring freezes and attrition across the Department have also affected staffing levels of human resources personnel, resulting in a delay of applicant processing and hiring.

Rather than employing one comprehensive automated applicant tracking system, the Secret Service uses two systems, which do not communicate with each other. The systems also require manual manipulation of data, making it difficult and cumbersome to process large numbers of applicants. In addition, applicants do not submit their Standard Form 86, *Questionnaire for National Security Positions* (SF 86), through the web-based, automated e-QIP system; instead they must email the document to Secret Service staff who print it out and review it manually. The electronic SF 86 only contains pages the applicant has completed, whereas the paper version is the entire 140-page document, including pages not completed. One Secret Service official described the process as a "paper mill," with boxes of applicant files filling an entire room.

The Secret Service has made changes to improve its law enforcement hiring processes and shorten the amount of time it takes to hire personnel, but most of the changes are relatively new and their long-term success cannot yet be measured. The Secret Service has established hiring events that allow applicants to complete several steps in the hiring process in one location. In FY

[8] Dashes indicate the Secret Service did not hire personnel that fiscal year.

2014, it took an average of 192 days to hire UD Officers who attended these events versus an average of 290 days for all other UD Officer applicants. In November 2015, the Secret Service created the Applicant Coordinating Center to further monitor applicant hiring, specifically during the polygraph examination, medical examination, and background phases of the process.

Despite improvements, the Secret Service continues to fall short of the Office of Personnel Management's (OPM) 80-day hiring goal. And while OPM's 80-day goal may be unrealistic in the law enforcement context because it does not account for additional steps in the law enforcement hiring process, the Secret Service also has failed to meet its own time-to-hire goals. In 2014, the Secret Service implemented a 118-day hiring target for its law enforcement applicants, but on average failed to meet this timeframe in FY 2014 and FY 2015 for both Special Agents and UD Officers. Although the Secret Service has improved its time-to-hire averages, it likely will never meet OPM's 80-day timeframe regardless of process improvements, and it will only be able to meet attainable internal targets.

Compounding these hiring challenges is that increased attrition requires increased hiring. For example, the Secret Service was able to hire 487 people between October 1, 2015 and end of June, 2016. This is an impressive accomplishment, but largely eviscerated by the fact that during the same period 439 individuals left the Service, resulting in a net gain of only 48 people.

We made five recommendations to the Department and components to improve the efficiency of law enforcement hiring practices, including that the Director of the Secret Service: (1) prioritize and dedicate full-time human resources, investigative, or polygraph personnel as needed; (2) establish an automated method to track applicants throughout the entire hiring process; and (3) adopt the e-QIP system for applicants to submit information for their SF 86 electronically. The Department and all three components concurred with our recommendations and are taking steps to address them. Based on the components' most recent responses to the final report, we consider all five recommendations resolved and open.

The Impact of Understaffing on the Secret Service

The inability to hire law enforcement personnel in a timely manner may lead to shortfalls in staffing, which can affect workforce productivity, as well as potentially disrupt mission critical operations.

During our review of the 2014 White House fence jumping incident, we found that staffing shortages for UD Officers led to excessive overtime, inadequate training, fatigue, low morale, and attrition.[9] An internal Secret Service report described similar effects on Special Agents. Similarly, during the course of an audit on Secret Service radio communications in 2015, we observed two UD officers sleeping at their posts. Fatigue from travel, overtime shifts, and long hours contributed to these incidents.[10]

Due to understaffing, the Secret Service relies on its UD Officers to work overtime and cancel days off and leave. In FY 2015, for example, UD Officers in the White House Branch worked an average of 22.9 overtime hours per pay period and worked 71.7 percent of days off. Working excessive overtime and having days off routinely canceled has a long-term negative impact on UD Officers' alertness and preparedness. Having to work exceedingly strenuous hours leads to fatigue, stress and low morale, which is unsustainable and results in attrition. Attrition in the Uniformed Division has been high; for example, in FY 2015, 152 UD Officers were hired but 169 left.

Additionally, due to the shortage in staffing many Secret Service personnel lack adequate training. Secret Service is not fully staffed to cover all shifts while others are in training. For Secret Service members a constant, rigorous, and innovative training regimen is a must because there is no room for error in their protective mission. A lack of training results in stale and degraded operational skills and could lead to incorrect or inadequate response during emergencies.

The management issues related to Secret Service staffing are deeply embedded. These underlying problems are not subject to relatively quick fixes such as those applied to technical or structural problems. Overcoming these challenges will require diligence and the full commitment of Secret Service leadership. It is imperative, however, that the Secret Service tackles these more fundamental and persistent management issues or it risks being unable to respond adequately or accomplish its protective mission.

Challenges Protecting Sensitive Case Management Systems and Data

Background

In 2015, our office conducted an investigation regarding allegations of improper access and distribution of House Oversight & Government Reform Chairman

[9] *2014 White House Fence Jumping Incident*, OIG-16-64 (April 2016).
[10] *Management Alert – Secret Service Staffing and Scheduling Contributed to Officer Fatigue* (October 2015).

Chaffetz' personally identifiable information (PII) contained on the Secret Service mainframe, known as the Master Central Index (MCI). On September 25, 2015, we reported that 45 Secret Service employees had accessed Chairman Chaffetz' sensitive PII on approximately 60 occasions. The information, including the Chairman's social security number and date of birth, was from when he applied for employment with the Secret Service in September 2003. Of the 45 employees, only 4 had a legitimate business need to access this information. The others who accessed the Chairman's record did so in violation of the *Privacy Act of 1974*, as well as DHS policy and *USSS IT Rules of General Behavior*. [11]

During our investigation, we planned a follow-up audit to determine whether adequate controls and data protections were in place on the MCI.

In 1984, the Secret Service developed and implemented the MCI mainframe application as an essential system for use by Secret Service personnel in carrying out their law enforcement mission. An independent security review performed in 2007 by the National Security Agency (NSA) identified IT security vulnerabilities on all applications hosted on the Secret Service mainframe and advised corrective action. According to Secret Service personnel, a key deficiency of MCI was that once a user was granted access to the MCI, that user had access to all data within MCI — regardless of whether it was necessary for the user's role.

In response to NSA's review, Secret Service initiated the Mainframe Application Refactoring project in 2011. Four years later, it completed final disassembly and removal of the mainframe in August and September 2015 and migrated MCI data to the following five information systems:

- Field Investigative Reporting System (FIRS)
- Clearances, Logistics, Employees, Applicants, and Recruitment (CLEAR)
- Protective Threat Management System (PTMS)
- Electronic Name Check System (eCheck)
- Electronic Case Management System (eCase)

MCI disassembly and data migration occurred just a few weeks prior to the start of our audit in September 2015. As a result, we focused our audit on these five systems.[12]

[11] *Investigation into the Improper Access and Distribution of Information Contained Within a Secret Service Data System* (September 2015).
[12] *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*, OIG-17-01 (October 2016).

Ineffective Systems and Data Management

Our audit disclosed that Secret Service did not have adequate protections in place on the systems to which MCI information was migrated. Specifically, we found:

- Inadequate System Security Plans – These documents, which provide an overview of system security requirements, were inaccurate, incomplete, or in one case, nonexistent. As a result, Secret Service had no reasonable assurance that mission-critical case management and investigative information was properly maintained and protected. Those relying on Secret Service to protect their identities (e.g., informants) had no assurance against unauthorized access or disclosure of their information.

- Systems with Expired Authorities to Operate (ATO) – Secret Service was operating IT systems without valid ATOs documenting senior-level approval to operate those systems. Lacking ATOs, Secret Service had no reasonable assurance that effective controls existed to protect the information stored and processed on these systems.

- Inadequate Access Controls – Secret Service lacked access controls on the information systems we reviewed. Further, policies did not address the principle of least privilege, restricting system users to only those privileges needed for the performance of authorized tasks. According to Secret Service personnel, 5,414 employees had unfettered access to the MCI application data before it was retired. These deficiencies increased the likelihood that any user could gain unauthorized and covert access to sensitive information, compromising its confidentiality, integrity, and availability.

- Inadequate Audit Controls – These controls were not fully implemented, hindering the Service's ability to detect unusual user activities and/or provide appropriate response to potential or actual security risks, anomalies, or attacks. Such deficiencies significantly hindered Secret Service's ability to reconcile system events with the responsible individuals, rendering them unable to conduct appropriate incident response in the event of cyber security incidents or threats.

- Noncompliance with Logical Access Requirements – Secret Service had not fully implemented Personal Identity Verification (PIV) cards for logical access to Secret Service IT systems as required. Approximately 3 percent of privileged users and 99 percent of non-privileged users were not using PIV cards to access information systems, hindering USSS' ability to limit system and data access to only authorized users with a legitimate need.

- Lack of Privacy Protections – Despite National Institute of Standards and Technology and DHS privacy protection requirements, Secret Service had not designated a full-time component privacy officer reporting directly to the Secret Service Director. Secret Service privacy documentation was incomplete, out-of-date, or missing documented assessments on how privacy controls were implemented. Secret Service had not published component-specific policies and procedures to comply with DHS policy. Also, responsible system owners and security personnel (i.e., Information System Security Officers) were unaware of their responsibilities for documenting and implementing privacy protections on Secret Service systems. Ineffective privacy leadership and practices increased the likelihood of serious breaches to PII, resulting in identify theft or worse, personal harm to employees, their families, informants working for Secret Service, or subjects of Secret Service investigations.

- Records Retention – Secret Service retained job applicant data on information systems longer than was relevant and necessary, in violation of the *Privacy Act of 1974*. Many "rejected" and "no longer interested" applications were more than 5 years old, including records up to 14 years old. In January 2016, Secret Service officials advised us that they were working towards implementing a new 2-year/5-year data retention protocol.

IT Management Has Not Been a Priority

The systems and data management problems we identified can be attributed to a lack of Secret Service priority on IT management. Specifically, our audit disclosed:

- Limited CIO Authority and Responsibility – Historically, the Secret Service CIO has not been effectively positioned to provide needed IT oversight. In 1988, Secret Service established the Information Resources Management Division (IRMD) to manage and support the investigative and protective operations and associated administrative functions of the agency from an IT perspective. In 2006, senior management decided to remove the incumbent CIO from heading IRMD and put a Special Agent in his place. The Special Agent, with limited IT management and leadership experience, became responsible for a technology division with a diverse portfolio of IT services, programs, acquisitions, and operational elements. In a culture in which Special Agents are reluctant to relinquish control, the split contributed significantly to a lack of IT leadership and inability to build a strong technology program within the Secret Service.

- Lack of Focus on IT Policy Management – Inadequate attention was given to keeping critical Secret Service IT policies updated. Key guidance had not been updated since 1992 when Secret Service was part of the Department of the Treasury. Outdated IT policies leave the organization hindered in its ability to implement and enforce IT system security requirements.

- Key IT Leadership Vacancies – Key positions responsible for the management of IT resources and assets were not filled. Some vacancies lasted for almost one year; other vacancies still existed at the time of our audit. For example, for almost a year, from December 2014 to November 2015, Secret Service lacked a full-time CIO. An acting Chief Information Security Officer (CISO) departed in September 2015; as of January 2016 the position was still vacant although the agency hired a Deputy CISO that same month. Further, Secret Service did not have a full-time Information System Security Manager, critical to ensuring that the organization's information security program is implemented and maintained.

- Vacant IT Staff Positions – As of December 2015, OCIO reported having 139 employees and 58 vacancies, which is a staff vacancy rate of 29 percent. Secret Service relied heavily on contractors to fill IT security positions rather than on Federal employees, as background checks for contractors did not require polygraphs. However, contractor Information System Security Officers felt they were not getting sufficient guidance to perform their responsibilities.

- Inadequate IT Training – Secret Service personnel did not receive adequate IT training. For example, not all employees and contractors completed mandatory IT security awareness, specialized role-based training, or privacy training. As a result, many employees lacked knowledge of their specific roles and responsibilities. For fiscal year 2015, we found that only 85 percent of Secret Service's employee population had completed the required IT security awareness training.

Recent Steps to Improve IT Management

Secret Service recently initiated steps to improve its IT management structure, which may give more priority to the leadership, policies, personnel, and training needed to ensure protections for sensitive systems and data. Specifically, in December 2015, the Secret Service Director announced component-wide that the new CIO was put back in charge of IRMD, giving him control of all IT assets. Additionally, five new divisions were established to delineate OCIO functions.

These changes are initial steps to address the various IT deficiencies we identified. However, it will take time for these improvements to be fully implemented and demonstrate effectiveness. Until then, the potential for incidents similar to the breach of Chairman Chaffetz' information in March 2015 remain. Any loss, theft, corruption, destruction, or unavailability of Law Enforcement Sensitive data or PII could have grave adverse effects on Secret Service's ability to protect its employees, stakeholders, or the general public.

We should not underestimate the challenges ahead. While the Secret Service has made substantial gains in securing its networks, according to the self-assessment scoring required by the Federal Information Security Management Act, it still needs to work on securing that each of its IT systems is properly authorized and protected from external threat.

Previous Allegations of Employee Misconduct

Over the past several years, as part of our independent oversight effort, we have investigated various incidents involving allegations of misconduct by Secret Service employees.[13]

For example:

- We investigated allegations that, in April 2012, during preparations for President Obama' visit to Cartagena, Colombia, Secret Service agents solicited prostitutes and engaged in other misconduct. As part of our investigation, we conducted 283 interviews of 251 Secret Service personnel. Based on our interviews and review of records, we identified 13 Secret Service employees who had personal encounters with female Colombian nationals consistent with the misconduct reported. We determined that one of the female Colombian nationals involved in the incident was known to the Intelligence Community. However, we found

[13] *See, e.g. Investigation Into the Improper Access and Distribution of Information Contained Within a Secret Service Data System (September 2015); Investigation Into the Incident at the White House Complex on March 4, 2015 (May 2015); Allegations of Misuse of United States Secret Service Resources (October 2014).*

no evidence that the actions of Secret Service personnel had compromised any sensitive information.

- We reviewed the actions of two Secret Service agents who on the evening of March 4th, 2015, had entered an area of the White House Complex that had been secured as a result of a suspicious package. We concluded that it was more likely than not that both agents' judgment was impaired by alcohol. We found that, notwithstanding their denials, both agents were observed by uniformed officers as "not right," and "not making sense," had just spent the previous five hours in a restaurant/bar in which one ran up a significant bar tab, and that they drove into a crime scene inches from what the rest of the Secret Service was treating as a potential explosive device and which, under different circumstances, could have endangered their own lives and those of the UD officers responding. While each agent had a duty to report the incident to his superior, neither did do so. We found that their failure to do so reflected either poor judgment or an affirmative desire to hide their activities.

The Secret Service has certainly taken steps to address these and similar challenges, but not always successfully. These persistent challenges may not be easy to resolve through expeditious action, such as suspending employees and issuing new guidance. They may require more fundamental change that addresses the root cause of the misconduct.

As a result of the Cartagena incident, in December 2013, we issued a report on our review of the Secret Service's efforts to identify, mitigate, and address instances of misconduct and inappropriate behavior. In our report, we described a situation in which many employees were hesitant to report off-duty misconduct either because of fear that they would be retaliated against or because they felt management would do nothing about it.[14] For example, in response to one survey question, 56 percent of electronic survey respondents indicated that they could report misconduct without fear of retaliation, meaning that almost half of the workforce may have feared retaliation for reporting misconduct.

As a result of our findings, , the Secret Service created a table of penalties for determining appropriate corrective, disciplinary, or adverse actions for common offenses and established a centralized process within headquarters for determining and implementing discipline for employee misconduct.

[14] *Adequacy of USSS Efforts to Identify, Mitigate, and Address Instances of Misconduct and Inappropriate Behavior*, OIG 14-20 (December 2013).

Ongoing OIG Oversight of the Secret Service

Our office will continue to help the Secret Service meet its critical mission through independent and objective audits, inspections, and investigations. We plan to publish several DHS-wide audits in FY 2017 that will include reviews of the Secret Service, including:

- DHS' Use of Polygraphs in the Hiring Process Audit: We are conducting a Department–wide audit of the use of polygraphs and USSS is part of that audit. The purpose of this audit is to determine whether DHS' polygraph examinations are an effective tool for screening new employees during the hiring process.

- DHS Conduct & Discipline: We are currently conducting a Department-wide audit of DHS' disciplinary processes, which focuses on the depth and breadth of employees' perceptions and attitudes about misconduct and the application of discipline, DHS' established rules of conduct, and the application of discipline across the Department.

Conclusion

The Secret Service's statutory responsibility to protect the President, other dignitaries, and events, as well as investigate financial and cyber-crimes to help preserve the integrity of the Nation's economy, leaves little, if any, room for error. As our audits and inspections have demonstrated, to achieve its mission, the Secret Service needs to continue working to improve its operations and programs. Although it has planned and taken actions to address the Protective Mission Panel's recommendations, fully implementing changes and resolving underlying issues will require the Secret Service's sustained commitment and depend heavily on adequate funding and staffing. We will continue to monitor the Secret Service's progress as it takes corrective actions to address vulnerabilities.

Mr. Chairman, thank you for inviting me to testify here today. I look forward to discussing our work with you and the Members of the Subcommittee.