OFFICE OF INSPECTOR GENERAL

Testimony of Inspector General John Roth

Before the Committee on Oversight and Government Reform

United States House of Representatives

"Oversight of the Secret Service"

Homeland Security

November 15, 2016
10:30 AM

DHS OIG HIGHLIGHTS

Oversight of the Secret Service

November 15, 2016

Why We Did This

The inspections and audit 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 Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for inviting me here today to discuss oversight of the U.S. Secret Service.

Today, I would like to discuss the results of the Office of Inspector General's recent reviews, which touch on the Secret Service's efforts to reform its basic management functions to more effectively execute its mission. Our most recent work 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 each area, the Secret Service has taken action to address the concerns and challenges identified by our office and this Committee. 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.

The Secret Service has clearly taken the Panel's recommendations seriously, which it has demonstrated by making a number of significant changes, including several actions underway or nearing completion. Specifically, although managers need more training in encouraging, valuing, and responding to employee feedback, the Secret Service has improved communication within the workforce by providing a platform for employees to share ideas. Additionally, using funding appropriated for Panel initiatives, the

[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); and *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*, OIG-17-01 (October 2016)

Secret Service has begun enhancing security and refreshing technology at the WHC. Namely, it is working with stakeholders on plans to construct a new outer fence surrounding the WHC.

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 budget" for fiscal year 2018, which should address many of the causes of equipment and personnel shortfalls.

The Secret Service has also taken action or plans to act on the Panel's recommendations related to staffing, training, technology, leadership, and organization. However, fully implementing changes and resolving underlying issues will require a multi-year commitment and depend heavily on adequate funding and staffing. Further, some initiated or proposed actions have not yet resulted in desired outcomes. The Secret Service has increased hiring, but still struggles with staff retention. For example, the Secret Service hired 402 Special Agents between October 2014 and June 2016, but lost 420 Special Agents through attrition. During the same period, the Secret Service hired 342 Uniformed Division (UD) Officers but lost 312 UD Officers through attrition. Although training has been enhanced, it continues to be hindered by low staffing levels and high operational demands on the workforce.

To achieve its mission to protect the President and Vice President, their families, and the White House, the Secret Service must invest in cutting edge technology and drive research and development. At times in the past, the Secret Service's organizational structure and processes hindered its ability to carry out these tasks. Our January 2016 report on the state of the Secret Service's radio systems, for example, highlighted the fact that many were well beyond their recommended service life, and many manufacturers had stopped making several of the major system components, making repairs difficult.[2] Likewise, in our review of the March 4, 2015 alcohol-related incident at the WHC we noted that the video system there was installed in 2007 and, because of the limitations of the system and other reasons, video was not preserved for long periods of time.[3] We also found that the alarm at a residence of President George H.W. Bush was installed in 1993 and not replaced, even though in 2010 a Secret Service security expert determined that the alarm system had

[2] *U.S. Secret Service Needs to Upgrade its Radio Systems*, OIG-16-20 (January 2016)
[3] *Investigation into the Incident at the White House Complex on March 4, 2015* (May 2015)

exceeded its useful life.[4] Additionally, as we note below, the Secret Service data system known as the Master Central Index, which contained a variety of sensitive and essential information, was developed and implemented in 1984 and remained in use until 2015.

Recently, however, the Secret Service has empowered and professionalized the relevant offices and committed funding to technology refreshes and pursuing new technology. For example, it has made a non-law enforcement professional subject matter expert the head of the Office of Technical Development and Mission Support and established and assigned IT responsibilities to a non-law enforcement professional subject matter expert Chief Information Officer (CIO). Although the Secret Service has reorganized key budget and technology functions, emphasizing expertise and leadership experience, it has not yet elevated civilian leadership in the human resources area. Nor has the Secret Service found the ideal structure or placement in the component for the Uniformed Division.

The Panel 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 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.

We made five recommendations to further the Secret Service's progress in addressing the Panel's recommendations. In addition to this unclassified report, we will be issuing a classified report focusing on our review of the Panel's classified recommendations. This Committee will receive a copy of the classified report once it is complete, and an unclassified summary will be posted on our public website.

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

[4] *Management Advisory – Alarm System Maintenance at Residences Protected by the Secret Service* (April 2015)

Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the Secret Service. We identified several issues with all three components' law enforcement hiring processes. Today, I will focus on those we identified at the Secret Service.

The good news is that from fiscal years 2011 through 2015, the Secret Service came close to meeting or met authorized staffing levels for Special Agents and UD Officers.

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. (A dash indicates the Secret Service did not hire personnel that fiscal year.)

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

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

A lack of dedicated human resources staff lengthens the Secret Service's hiring process. For example, Special Agents in field offices conduct polygraph examinations and background investigations as collateral duties, but it is difficult to complete these collateral duties because the Special Agents' primary investigative and protective functions take precedence. In FY 2015, the Secret Service's security clearance process, including polygraph examinations and background investigations, for UD Officers averaged 200 days. According to Secret Service officials, it takes even longer in an election year, such as this one, because of the Special Agents' increased operational tempo. Hiring freezes and attrition across the Department have also affected staffing levels of human resources personnel and delayed applicant processing and hiring. In the Secret Service, at the end of FY 2015, 32 percent of human resources positions were vacant.

Rather than one comprehensive automated system, the Secret Service uses two applicant tracking 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; 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 Department, CBP, ICE, and the Secret Service have all made changes to improve their 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 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 Office of Personnel Management (OPM)-established and its own time-to-hire goals. OPM's 80-day goal is unrealistic because it does not account for the additional steps in the law enforcement hiring process. 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 will likely not meet OPM's 80-day timeframe, regardless of process improvements, and it will only meet credible and attainable internal targets.

The inability to hire law enforcement personnel in a timely manner may lead to shortfalls in staffing, which can affect workforce productivity and morale, as well as potentially disrupt mission critical operations. In a previous OIG report we found that staffing shortages for UD Officers led to inadequate training, fatigue, low morale, and attrition.[5] An internal Secret Service report described similar effects on Special Agents.

We made five recommendations to improve the efficiency of law enforcement hiring practices. The Department and all three components concurred with our recommendations and are taking steps to address them. Based on the

[5] *2014 White House Fence Jumping Incident*, OIG-16-64 (April 2016)

components' responses to the draft report, we consider one recommendation unresolved and open and four recommendations resolved and open.

Our recommendation to prioritize and dedicate full-time personnel as needed is unresolved because we do not believe the Secret Service's plan to hire one additional polygraph examining investigator will substantially ease the burden of Special Agents who conduct polygraph examinations and background investigations as collateral duties.

Challenges Protecting Sensitive Case Management Systems and Data

Background

Last year, our office conducted an investigation regarding allegations of improper access and distribution of Chairman Chaffetz' personally identifiable information (PII) contained on the USSS 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*. [6]

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

In 1984, the Secret Service (USSS) developed and implemented the MCI mainframe application as an essential system for use by USSS 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 USSS mainframe and advised corrective action. According to USSS 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, USSS initiated the Mainframe Application Refactoring project in 2011. Four years later, USSS completed final disassembly and removal of the mainframe in August and September 2015 and migrated MCI data to the following five information systems:

[6] *Investigation into the Improper Access and Distribution of Information Contained Within a Secret Service Data System* (September 2015)

- 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.

Ineffective Systems and Data Management

Our audit disclosed that USSS 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, USSS had no reasonable assurance that mission-critical case management and investigative information was properly maintained and protected. Those relying on USSS 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) – USSS was operating IT systems without valid ATOs documenting senior-level approval to operate those systems. Lacking ATOs, USSS had no reasonable assurance that effective controls existed to protect the information stored and processed on these systems.

- Inadequate Access Controls – USSS 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 USSS 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 USSS' ability to detect unusual user

activities and/or provide appropriate response to potential or actual security risks, anomalies, or attacks. Such deficiencies significantly hindered USSS' 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.

The Chairman has requested that our office investigate possible instances of the mishandling of PII at the Secret Service, including whether any other Member of Congress' PII has ever been improperly accessed or disseminated from a Secret Service database. Because the MCI database has been disassembled and dismantled, we are unable to conduct a historical audit regarding whether PII was mishandled during the time that the MCI was in use, between 1984 and August 2015. Due to the inadequate audit controls on the systems to which the MCI data and information was migrated, we also do not have the ability to review or investigate the potential mishandling of PII since August 2015. We have recommended that the Secret Service update its system policies, which would include updating policies for auditing system events, in order to address this deficiency.

- Noncompliance with Logical Access Requirements – USSS had not fully implemented Personal Identity Verification (PIV) cards for logical access to USSS 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, USSS had not designated a full-time component privacy officer reporting directly to the USSS Director. USSS privacy documentation was incomplete, out-of-date, or missing documented assessments on how privacy controls were implemented. USSS 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 USSS 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 USSS, or subjects of USSS investigations.

- Records Retention – USSS 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. We found that Chairman Chaffetz' 2003 application for employment with the USSS remained in both CLEAR and eCase, and therefore susceptible to unauthorized access. Collectively, the systems still contained records of the Chairman's name, social security number, race, the type of position to which he had applied, and the status of his application. USSS could not provide assurance that other applicants' records and corresponding PII had been properly expunged from CLEAR and eCase as well.

  The USSS Chief Records Officer concluded that the historical decision to retain these records for 20 years "was likely just precautionary" and the reasoning was no longer valid. We determined that Chairman Chaffetz' record and corresponding PII were deleted from CLEAR and eCase as of January 2016. That same month, USSS officials advised us that they were working towards implementing a new 2-year/5-year data retention protocol.

IT Management Has Not Been a USSS Priority

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

- Limited CIO Authority and Responsibility – Historically, the USSS CIO has not been effectively positioned to provide needed IT oversight. In 1988, USSS 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 USSS.

- Lack of Focus on IT Policy Management – Inadequate attention was given to keeping critical USSS IT policies updated. Key guidance had not been updated since 1992 when USSS 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, USSS 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 USSS hired a Deputy CISO that same month. Further, USSS 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. USSS 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 – USSS 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 USSS' employee population had completed the required IT security awareness training. USSS had a total of 6,307 Federal employees and 397 contractors.

Recent Steps to Improve IT Management

USSS 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 USSS 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 the Chairman's 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 USSS' ability to protect its employees, stakeholders, or the general public.

We made 11 recommendations to address the deficiencies identified in our report. The Secret Service Director concurred with each recommendation and outlined initial steps for corrective action. As part of our normal audit follow-up and resolution process, the Secret Service owes us a corrective action plan to address our recommendations within 90 days of the issuance of the report, which was formally transmitted to the Secret Service on October 7, 2016.

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. The Secret Service also needs to continue shortening the time it takes to hire law enforcement personnel, because delays in hiring may ultimately lead to staffing shortfalls, affect workforce productivity and morale, and potentially disrupt mission-critical operations. Finally, the Secret Service must manage its systems and information supporting its mission efficiently and securely. In December 2015, the Secret Service began to improve its IT program management, including centralizing all

IT resources under a full-time CIO and developing plans for an improved IT governance framework. Time will tell whether these improvements will effectively safeguard sensitive systems and data. We will continue to monitor the Secret Service's progress as it takes corrective actions to address vulnerabilities.

Our office will continue to help the Secret Service meet its critical mission through independent and objective audits, inspections, and investigations. In addition to our report on the classified Protective Mission Panel recommendations, we plan to publish several DHS-wide audits in FY 2017 that will include reviews of the Secret Service, including:

- A review of DHS components' use of force;
- A DHS-wide review of employee conduct and discipline;
- An audit to determine the effectiveness of polygraph examinations used by DHS; and
- A review of DHS controls over firearms and other sensitive assets.

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 Committee.