



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

**STATEMENT OF
KATHLEEN MCGETTIGAN
ACTING DIRECTOR
U.S. OFFICE OF PERSONNEL MANAGEMENT**

before the

**COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES**

on

**Improving Security and Efficiency at OPM and the National Background
Investigations Bureau**

February 2, 2017

Chairman Chaffetz, Ranking Member Cummings and Members of the Committee:

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Committee. Thank you for the opportunity for myself and my colleagues with me today to testify before the committee on the National Background Investigations Bureau (NBIB) transition, the security clearance process, and information technology (IT) security. As the Acting Director of the U.S. Office of Personnel Management (OPM), I can assure you we recognize how critical this is to the Federal government and to our national security. In keeping with our focus on modernizing the way that OPM carries out its important missions, OPM has worked to optimize the business processes surrounding background investigations. OPM has also taken aggressive measures to enhance the security of its IT systems, both within the NBIB and throughout OPM, accelerating an ambitious long-term IT security and modernization plan to upgrade the security of our systems and strengthen the agency's ability to respond to cyber incidents. OPM has also partnered with the Department of Defense (DOD) and other agencies to leverage government-wide knowledge, resources, and best practices.

Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management

February 2, 2017

The National Background Investigations Bureau

NBIB was established on October 1, 2016, and is the primary provider of background investigations for the Federal government. NBIB is designed with an enhanced focus on national security, customer service, and continuous process improvement to meet this critical government-wide need. Charles S. Phalen, Jr., the NBIB Director, has a long and distinguished career in multiple roles at senior levels in the Federal government and private industry with a focus on protecting our national security. His extensive experience includes serving in various capacities at the Central Intelligence Agency, including as the Director of Security, and with the Federal Bureau of Investigations as Assistant Director leading its Security Division.

NBIB conducts 95 percent of investigations across the government. Even those few agencies that have the statutory authority to conduct their own investigations, such as the Intelligence Community, rely on NBIB's services in some capacity. Its new organizational structure is aimed at leveraging automation, transforming business processes, and enhancing customer engagement and transparency. Through a strong partnership with DOD, NBIB will build a modern and secure IT system to comprehensively support the investigations process and enhance end-to-end processes across government. These efforts will ultimately improve the efficiency, cost effectiveness, and quality of the investigations across the Federal government.

As you are likely aware, in late 2014, OPM's market capacity for contract investigation services was drastically reduced by the loss of OPM's largest field contractor, resulting in an investigative backlog. This backlog was exacerbated by the cybersecurity incidents at OPM that were announced in 2015. Looking forward, it is an NBIB priority to address the investigative backlog while maintaining a commitment to quality and returning back to the level of performance realized from 2009 through 2014. NBIB, working with the Office of the Director of National Intelligence (ODNI), DOD and other customers, is focusing efforts in three primary areas. First and foremost, NBIB is working to increase capacity. NBIB hired 400 new Federal investigators in 2016, and NBIB recently awarded a new investigative fieldwork contract, increasing the fieldwork contractors from two companies to four. Work under the new contracts began on February 1, 2017. Second, NBIB is focusing on policy and process changes to add efficiencies, reduce level of effort, and maintain investigative quality. To support this effort, NBIB, working closely with the DOD and interagency partners, conducted a detailed business process reengineering effort and worked in collaboration with ODNI in its role as the Security Executive Agent to identify appropriate policy and process changes to help address the backlog. Third, NBIB has actively worked with customer agencies to prioritize cases and schedule those that are most critical to our national security and the mission needs of our customers.

**Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management**

February 2, 2017

Information technology also plays a central role in NBIB's ability to enhance the background investigation process. A key component of NBIB is to leverage DOD's cybersecurity expertise and resources to design, develop, and implement a modern and secure IT environment. While still in development, the new system, known as the National Background Investigation System (NBIS), is to be operated and maintained by DOD on behalf of NBIB. NBIB is encouraged by the significant progress DOD has made toward new capabilities that will improve the effectiveness and security of background investigations. Concurrently, the OPM Office of the Chief Information Officer (OPM CIO), in coordination with our interagency partners to include DOD and Department of Homeland Security (DHS), has aggressively pursued further improving the cybersecurity posture of the OPM network.

Role of the Office of the Chief Information Officer

OPM has worked to strengthen the infrastructure and security of not only NBIB, but also OPM's entire technology ecosystem. This effort is being led by OPM's new CIO, David DeVries, who joined OPM in September 2016. Mr. DeVries had previously been the DOD Principal Deputy CIO and has a strong relationship with his former agency that facilitates coordinating the implementation of NBIS. Indeed, as the Federal government modernizes how it does business, OPM has focused on embracing new tools and technologies to deliver optimum customer service and enhance the security of the information we house. In a rapidly changing and increasingly interconnected digital world, it is important for agencies to develop the best possible defenses and safeguards.

Over the past eight months, OPM has successfully begun to roll out its program for implementation of the Federal Information Technology Acquisition Reform Act and enhanced the agency's infrastructure in ways that will help OPM support its cybersecurity initiatives and strategies, ensure its IT programs run more efficiently and securely in supporting the OPM business lines, and better utilize limited resources.

OPM has enhanced its cybersecurity efforts from multiple angles: through the addition of cybersecurity tools and security updates; through staff and agency-wide training; through hiring critical personnel; and through collaboration with OPM's interagency partners. For example, in Fiscal Year 2016, OPM implemented 100 percent multi-factor user authentication for access to OPM's network, via the use of the "Personal Identity Verification" (PIV) card. This capability and enforcement provides a powerful barrier to our networks and information stores from individuals who are not authorized to have access. OPM is in the process of expanding this to agency applications to further increase the security of our systems. In 2016, OPM launched two major IT system compliance initiatives that resulted in all major IT systems having current ATO (Authority to Operate) and network segmentation.

Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management

February 2, 2017

As the Federal government's personnel agency, OPM recognizes that cybersecurity is not just about technology, but is also about people and, to that end, in addition to strengthening its technology, OPM has added seasoned cybersecurity and IT experts to its already talented team. OPM has hired a number of other new senior IT leaders, and realigned and centralized its cybersecurity program and resources under the Chief Information Security Officer (CISO), a primary responsibility of which is to take the steps necessary to secure and control access to sensitive information. OPM also hired Information System Security Officers (ISSOs) in Fiscal Year 2016 to support all of OPM's major information systems.

OPM is continuing to leverage and utilize its interagency partnerships and the expertise of the IT and cyber communities across government. OPM strengthened its threat awareness by enrolling in multiple information and intelligence sharing programs. OPM was one of the first agencies to participate in DHS's Einstein 3A program, and was one of the first agencies in the Federal government to fully implement Phase 1 of DHS's Continuous Diagnostics and Mitigation program. These initiatives allow agencies to detect and prevent cyber-attacks, and continuously identify and proactively mitigate cybersecurity threats and vulnerabilities that might arise.

The cybersecurity incidents at OPM provided an important catalyst for accelerated change across the Federal government. OPM met the challenge and greatly appreciates the collaborative spirit with which its interagency partners across government continue to work with us every day. Embracing modernization can help save taxpayer dollars, improve critical programs, and mitigate security risks in a world of continually evolving threats. OPM and DOD will continue to collaborate on the development of a state-of-the-art IT system for NBIB. By investing in IT systems across functions, we can drive more effective, efficient, and data-driven accomplishment of work across a variety of missions.

Conclusion

The necessary key partnerships and plans have been developed to build out the NBIB and improve the security and efficiency of OPM's IT systems. We created a coordinated strategy to transition the investigative program to an organizational model that fosters innovation, focuses on customer service, and leverages interagency expertise. These structural and process improvements, in coordination with our partners, will enable us to improve timeliness and reduce the investigative backlog. In parallel, we are working closely with DOD's CIO to build the information systems capabilities to support this activity for now and the future. This productive partnership will enable an effective and secure information environment as a government-wide solution. Equally productive is the CIO's holistic approach, which ranges from bringing on new qualified personnel to adopting new tools and procedures that enhance the security of OPM's networks and data for all of OPM's lines of business, including NBIB.

**Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management**

February 2, 2017

Thank you for the opportunity to testify before you today, and we welcome any questions you may have.