Embargoed until Delivered

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503
www.whitehouse.gov/omb

TESTIMONY OF TONY SCOTT

UNITED STATES CHIEF INFORMATION OFFICER
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

February 25, 2016

Chairman Chaffetz, Ranking Member Cummings, and members of the Committee, I appreciate the opportunity to appear before you today to speak about the important issue of the Administration's recently announced changes to modernize and strengthen how the Federal Government performs and safeguards background investigations for its employees and contractors.

As you know, the Federal Government is responsible for issuing, handling, and storing important and sensitive data. We are also responsible for using this data as part of many different critical functions, one of which is the subject of today's hearing – the Federal Government's background investigations process.

As the world's technologies continue to evolve and our economy becomes ever more digitally connected, the Federal Government's tools, systems, and processes for managing this sensitive information and for conducting background investigations must also evolve. We must keep pace with technological advancement in order to anticipate, detect, and counter malicious attempts to breach Government systems, and to address threats posed by trusted insiders who may seek to do harm to the Government's personnel, property, and information systems.

Given the numerous Information Technology (IT) systems that are used across government, and the amount of data that is collected to conduct background investigations, confronting the cybersecurity threats to these systems and data is of particular interest to me in my role as the Federal Chief Information Officer (CIO). As CIO, I lead the OMB Office of E-Government & Information Technology (IT) (E-Gov), which is responsible for developing and overseeing the implementation of Federal IT policy. Even though my team has a variety of responsibilities, I will focus today's remarks on the Administration's response to increasing cybersecurity threats, and actions we are taking to improve the Government's background investigation process.

Governance of the Suitability and Security Clearance Processes

Beginning in 2008, the Suitability and Security Clearance Performance Accountability Council (PAC) was established through an Executive Order, comprised of the Office of Management and Budget (chair); the Director of National Intelligence (Security Executive Agent), the Director of the U.S. Office of Personnel Management (OPM) (Suitability Executive Agent), and the Departments of Defense (DOD), Treasury, Homeland Security, State, Justice, and Energy, the Federal Bureau of

Investigation, and other agencies. The inter-agency PAC oversees reforms to the processes that Federal agencies and the public rely on to ensure Federal employees, contractors or members of the armed forces are suitable for employment and can be trusted with access to facilities and sensitive information.

The PAC Security and Suitability Review

Last year, in light of increasing cybersecurity threats – including the compromise of information housed at OPM – the PAC initiated an accelerated inter-agency review of the Government's suitability and security clearance background investigation process. Its goals were to determine how to further secure the sensitive data collected as part of the background investigation process and to determine improvements that could be made to the way the Government conducts background investigations.

The review resulted in the announcement last month of a number of steps that the Administration is taking to improve the Government's background investigation process for Federal employees and contractors. I would like to highlight major actions we are taking with our partners in OPM, DOD, and ODNI as well as other PAC agencies.

The New Background Investigations Bureau

In order to create a more secure and effective infrastructure, the Administration will establish a new Federal entity, the National Background Investigations Bureau (NBIB), which will strengthen how the Federal Government performs background investigations. There are a number of organizational changes that will take time to implement but result in significant improvements over time:

- The head of NBIB will be Presidentially-appointed, unlike the current structure, where the head of FIS is a career employee of OPM.
- The head of NBIB will be a full member of the PAC, whereas currently OPM's Federal Investigative Services (FIS) is a subordinate component of OPM and is not an independent member of the PAC.
- While the NBIB will report to the OPM Director, it will also be accountable to the PAC and its customer agencies, and will receive policy direction from the Suitability and Security Executive Agents.
- NBIB will be headquartered in Washington D.C., rather than in Boyers, Pennsylvania, which will allow for enhanced coordination with its inter-agency partners.
- NBIB will have a dedicated senior privacy official to advance privacy-by-design as the new entity is stood up and new IT systems are developed.
- Not only will a cadre of inter-agency personnel help stand up the NBIB, but NBIB will also leverage the expertise of inter-agency personnel and customer feedback as part of its ongoing management.
- NBIB will have several inter-agency working groups with its customer agencies designed to ensure there is regular feedback incorporated into operational decisions.

Leveraging DOD's Expertise

We recognize that creating a new investigations service provider does not, by itself, resolve the challenges we face in securing the investigative data and systems. Thus, in addition to the governance and organizational changes above, the Administration intends for NBIB's IT systems to be designed, built, secured, and operated by DOD, in accordance with NBIB requirements. This will leverage DOD's expertise in information technology and cybersecurity for processing background investigations and protecting against threats, will better protect the sensitive information used to effectively adjudicate investigations, and bring the fullest security resources to bear against increasingly sophisticated and evolving threats.

- This approach will leverage DOD's significant national security, IT, and cybersecurity expertise, incorporating security into the fundamental design of the systems, strengthening the security of the data environment, and providing robust privacy protections.
- To support this work, the President's Fiscal Year 2017 Budget includes $95 million within DOD's topline to that will be dedicated to the development of these IT capabilities.
- The PAC will also establish an inter-agency cybersecurity advisory group to provide advice and counsel on system development and threat mitigation.
- These efforts are consistent with OMB's direction to all Federal agencies to phase out the use of legacy IT systems where possible, and to begin using modern and emerging technology tools and capabilities to adequately secure mission functions, systems, and information.

Implementation

While these changes will take time to fully implement, the Administration has taken, and will continue to take, a series of actions to strengthen the background investigations process, including:

- In March, the Administration will have established a dedicated transition team headquartered in Washington D.C. to develop and implement a transition plan to: (1) stand-up the NBIB, (2) ensure that the transition timeline fully aligns with business needs, (3) transition the management of new investigation IT capabilities to DoD, (4) migrate the existing mission, functions, personnel, and support structure of OPM FIS to NBIB, and (5) provide continuity of service to FIS's customer agencies during the transition.
- By October 1, the Administration expects to establish the NBIB with the new governance and organizational structure described above, including absorption of FIS.
- By the end of 2016, we expect to begin delivering new, modern government-wide capabilities such as eApplication and eAdjudication that will greatly improve the effectiveness, efficiency, and security of key aspects of the background investigation process.
- By the end of 2016, the PAC and the Performance Improvement Council will also develop and implement outcome-based metrics that measure the effectiveness of the vetting processes.

Role of the Cybersecurity National Action Plan

More broadly, enhanced cybersecurity across all Federal Agencies will be strengthened by:

- Implementation of the Cybersecurity National Action Plan (CNAP), which builds on the security measures implemented in response to the 2015 cyber incidents (e.g., expanding strong

authentication; increasing scans; patching critical vulnerabilities; tightening privileged users policies and practices; identifying and securing high value assets; hiring a new senior OPM cyber and information technology advisor). The CNAP takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, and maintain public safety and economic and national security.

Summary

Over time, these actions will lead to tangible changes to the way we conduct background investigations for our trusted employees, military members and contractors. Indeed, these efforts – like other successful reforms in this important area – will span more than one Administration. We look forward to working with Congress to create a more secure, efficient, and effective Federal background investigations infrastructure. I thank the Committee for holding this hearing and I am pleased to answer any questions you may have.

Tony Scott, U.S. Chief Information Officer
Office of Management and Budget

Tony Scott is the third Chief Information Officer of the United States, appointed by President Obama on February 5th, 2015. Prior to his position in the White House, Mr. Scott led the global information technology group at VMware Inc., a position he had held since 2013. Prior to joining VMware Inc., Mr. Scott served as Chief Information Officer (CIO) at Microsoft from 2008 to 2013. Previously, he was the CIO at The Walt Disney Company from 2005 to 2008. From 1999 to 2005, Mr. Scott served as the Chief Technology Officer of Information Systems & Services at General Motors Corporation. He received a B.A. from the University of San Francisco and a J.D. from Santa Clara University.