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

April 22, 2015

Chairman Chaffetz, Ranking Member Cummings, members of the Committee, thank you for the opportunity to appear before you today. As some of you may know, I started my Office of Management and Budget (OMB) career just over two months ago, and I'm excited for the opportunity to speak with you today about OMB's role in Federal cybersecurity.

Before I begin, I would like to say that Federal cybersecurity oversight is one of my responsibilities as the Federal Chief Information Officer (CIO). As Federal CIO, I lead OMB's Office of E-Government & Information Technology (IT) (E-Gov). This office is responsible for: (1) developing and overseeing the implementation of Federal IT policy and (2) through the United States Digital Service, providing on-site expertise to agencies with high-impact public facing IT programs. During this Administration, E-Gov has been responsible for developing successful initiatives, like TechStat and PortfolioStat, which are focused on ensuring agency programs deliver value to customers. This is also the team responsible for leading the government-wide implementation of the Federal Information Technology Acquisition Reform Act (FITARA).[1] Although the objective of this law is to improve management of IT through strengthened CIO authorities, the law's impact on cybersecurity cannot be understated. CIOs with the proper authorities to manage IT will help ensure agencies are consistently applying cybersecurity policies and practices. Even though my team has a variety of responsibilities, I will focus my remarks on the team's work in Federal cybersecurity.

Strengthening Federal cybersecurity is one of the Administration's top priorities and a duty that I take very seriously. Having recently left a private sector CIO role, I can attest to the fact that having a strong cybersecurity program is critical to ensuring mission success. This is no different in the Federal government. Given the evolving threat landscape, it is imperative that we do everything in our power to ensure the security of government information and networks. In this interconnected world, we have to ensure that agencies, third-party contractors and vendors, and the citizens we serve all are protected from these threats. In my remarks today, I will provide you with an overview of OMB's role in Federal cybersecurity, a description of

[1] https://www.congress.gov/bill/113th-congress/house-bill/3979

recent events related to the cybersecurity of third-party contractors and vendors, and the steps OMB is taking to strengthen Federal cybersecurity practices.

OMB's Role in Federal Cybersecurity

To better understand OMB's role, I think it is important to provide a brief overview of the Federal cybersecurity landscape and the various offices involved. Under the Federal Information Security Modernization Act of 2014 (FISMA), the Director of OMB is responsible for Federal information security oversight and policy issuance for non-national security systems.[2] For national security systems, oversight and policy authority is delegated under FISMA to the Secretary of Defense for Department of Defense (DoD) systems and to the Director of National Intelligence for Intelligence Community systems. My testimony today will focus on OMB's role overseeing non-national security systems.

OMB executes its responsibilities in close coordination with its Federal cybersecurity partners, including the Department of Homeland Security (DHS) and the Department of Commerce's National Institute of Standards and Technology (NIST). FISMA clarifies DHS's role as the operational lead for cybersecurity of Federal civilian government systems. Specifically, the law gives DHS the authority to issue binding operational directives and to provide technical assistance to agencies. The law also states that Federal agencies are responsible for "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of: (1) information collected or maintained by or on behalf of the agency and (2) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."

Understanding the importance of this responsibility, OMB recently announced the creation of the first ever dedicated cybersecurity unit within the Office of E-Government & IT: the E-Gov Cyber and National Security Unit (E-Gov Cyber). The creation of the E-Gov Cyber Unit reflects OMB's focus on conducting robust, data-driven oversight of agencies' cybersecurity programs and on issuing Federal guidance consistent with emerging technologies and risks. This is the team behind the work articulated in the Fiscal Year (FY) 2014 FISMA report which highlighted both successes and challenges affecting Federal agencies' cyber programs. In FY 2015, the E-Gov Cyber Unit is targeting oversight through CyberStat reviews, prioritizing agencies with high risk factors as determined by cybersecurity performance and incident data. Additionally, the Unit is driving FISMA implementation by providing agencies with the guidance they need in this dynamic environment. The top FY 2015 policy priority of the team is updating Circular A-130, which is the central government-wide policy document that establishes agency guidelines on how to manage information resources. The E-Gov Cyber Unit is actively engaging with various stakeholders within the IT community to ensure the updated Circular provides agencies with guidance consistent with the latest technologies and best practices.

[2] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

Cybersecurity and Third-Party Contractors and Vendors

In 2014, several high profile cyber incidents across our nation made headlines for their scope, scale, and impact on victims. The Federal government was not immune to this threat activity. In 2014, cyber incidents impacted vendors responsible for conducting background investigations on behalf of the Federal government. In close partnership with DHS and appropriate agencies, OMB responded quickly and oversaw the government-wide response to mitigate the incidents, to include ensuring that relevant agencies notified potential victims in accordance with OMB guidance. During the response to these incidents, two things became clear: (1) third-party contractors and vendors were inconsistently implementing protections to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of government information and (2) Federal agencies did not have adequate contractual language, policy direction, or awareness of best practices to guide how contractors and agencies should respond to intrusions and/or actual breaches.

Steps Taken to Address Challenges

As part of the immediate response efforts, DHS worked closely with vendors that conduct background investigations, at their request, to ensure they had comprehensive controls in place to protect against future incidents. At the same time, OMB, in its policy and oversight role, took immediate action to address identified challenges. First, through the President's Management Council (PMC), OMB conducted a review of agencies' cybersecurity programs to identify risks and implementation gaps. Second, OMB directed an inter-agency effort to collect and disseminate contracting best practices to help agencies ensure the protection of sensitive government information.

The review conducted through the PMC allowed agencies and OMB to assess a broad range of cybersecurity risks ranging from how agencies identify and detect threats to agency policies and procedures for responding to incidents. As part of this review, agencies were directed to establish and initiate a process for identifying and reviewing relevant contracts to ensure compliance with Federal cybersecurity and privacy laws, OMB guidance, and NIST standards. The results of these reviews provided important context for both OMB and agencies and are being used to inform ongoing efforts to strengthen agency cybersecurity programs.

The inter-agency effort to collect and disseminate contracting best practices included direction from OMB to the Federal CIO Council and Chief Acquisition Officers (CAO) Council to provide recommendations to OMB for next steps to bolster cyber protections in Federal contracts. As part of this effort, OMB will address the need for:

- Formal guidance to agencies to implement new policy requirements;
- Updates to existing guidance or recommended inclusions in annual guidance documents; and
- Facilitation of best practices sharing through existing interagency forums.

In closing, I would like to say that securing our information in cyber space is the next great challenge for our country, but it is a challenge that I welcome. Ensuring the security of

information on the Federal government's networks and systems will remain a core focus of the Administration as we move aggressively to implement innovative protections and respond quickly to new challenges as they arise. In addition to our current strategy, we look forward to working with Congress on legislative actions that may further protect our nation's critical networks and systems.

I thank the Committee for holding this hearing, and for your commitment to improving Federal cybersecurity. I would be 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.