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 HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE
UNITED STATES SENATE

June 25, 2015

Chairman Johnson, Ranking Member Carper, members of the Committee, thank you for the opportunity to appear before you today. I appreciate the opportunity to speak with you about recent cyber incidents impacting Federal agencies.

I would like to start by highlighting a very important point of which you are already aware: both state and non-state actors who are well financed, highly motivated are persistently attempting to breach both government and non-government systems. And these attempts are not going away. They will continue to accelerate on two dimensions: first, the attack will continue becoming more sophisticated, and secondly, as we remediate and strengthen our own practices, our detection capabilities will improve. That means that we have to be as nimble, as aggressive, and as well-resourced as those who are trying to break into our systems.

Confronting cybersecurity threats on a continuous basis is our nation's new reality– a reality that I faced in the private sector, and am continuing to see here in my new role as the Federal Chief Information Officer (CIO). As Federal CIO, I lead the Office of Management and Budget's (OMB) Office of E-Government & Information Technology (IT) (E-Gov). My office is responsible for developing and overseeing the implementation of Federal Information Technology policy. Even though my team has a variety of responsibilities, I will focus today's remarks on cybersecurity.

OMB's Role in Federal Cybersecurity

Under the Federal Information Security Modernization Act of 2014 (FISMA), OMB is responsible for federal information security oversight and policy issuance. 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).

Additionally, OMB recently announced the creation of a dedicated cybersecurity unit within the Office of E-Gov & 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, monitoring and improving responses to major cyber security incidents, and 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 facing 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, including best practices for how to secure those resources.

Recent Cyber Incidents Affecting the Office of Personnel Management (OPM)

My colleagues will fully address the recent cyber incidents affecting the Office of Personnel Management (OPM). In terms of the role of OMB in responding to recent events, my office monitors very closely all reports of incidents affecting federal networks and systems. We use these reports to look for trends and patterns as well as for areas where our government-wide processes, policies, and other practices can be strengthened. We then update our guidance and coordinate with other agencies to ensure that guidance is implemented. And thanks to the good work done by this committee last Congressional sessions, the recently passed Federal Information Technology Acquisition Reform Act (FITARA) and our guidance associated with the legislation strengthens the role of the CIO in agency cybersecurity.

In this case, OPM notified OMB in April 2015 of an incident affecting data in transit in its network. OPM reported that they were working closely with various government agencies on a comprehensive investigation and response to this incident. We have been actively monitoring the situation and have been engaged in making sure that there is a government-wide response to the events at OPM.

Strengthening Federal Cyber Security Practices

To further improve Federal cyber infrastructure and protect systems against these evolving threats, last week OMB launched a 30-day Cybersecurity Sprint. The team is comprised of the Office of Management and Budget's (OMB) E-Gov Cyber and National Security Unit (E-Gov Cyber), the National Security Council Cybersecurity Directorate (NSC Cyber), the Department of Homeland Security (DHS), the Department of Defense (DOD), and other agencies. At the end of the review, the Government will create and operationalize a set of action plans and strategies to further address critical cybersecurity priorities and recommend a *Federal Civilian Cybersecurity Strategy*. This strategy will detail short, medium and long term steps that the Government should take to address current operational deficiencies and vulnerabilities as well as future care of our Federal IT infrastructure.

Key principles of the *Strategy* will include:

- *Protect*ing *Data*: Better protect data at rest and in transit.
- *Improving Situational Awareness*: Improve indication and warning.
- *Increasing Cybersecurity Proficiency*: Ensure a robust capacity to recruit and retain cybersecurity personnel.
- *Increase Awareness*: improve overall risk awareness by all users.
- *Standardizing and Automating Processes*: Decrease time needed to manage configurations and patch vulnerabilities.
- *Controlling, Containing, and Recovering from Incidents*: Contain malware proliferation, privilege escalation, and lateral movement. Quickly identify and resolve events and incidents.
- *Strengthening Systems Lifecycle Security*: Increase inherent security of platforms by buying more secure systems and retiring legacy systems in a timely manner.
- *Reducing Attack Surfaces*: Decrease complexity and number of things defenders need to protect.

As part of the effort, OMB instructed Federal agencies to immediately take a number of steps to protect Federal information and assets and improve the resilience of Federal networks.

Specifically, Federal agencies must:

- Immediately deploy indicators provided by DHS regarding priority threat-actor techniques, tactics, and procedures to scan systems and check logs.
- Patch critical vulnerabilities without delay and report to OMB and DHS on progress and challenges within 30 days.
- Tighten policies and practices for privileged users.
- Dramatically accelerate implementation of multi-factor authentication, especially for privileged users.

Summary

In closing, I want to underscore a critical point I made at the beginning of this testimony: both state and non-state actors are attempting to breach both government and non-government systems. And this problem is not going to go away. It's going to accelerate. Ensuring the security of information within 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 the actions we are taking, we also look forward to working with Congress on legislative actions that may further protect our nation's critical networks and systems. Providing Departments and Agencies with the proper legal authority along with the requisite funding are key steps to ensuring that our Federal civilian networks are adequately protected. I encourage you to continue working with the administration to move important, necessary cybersecurity legislation through Congress.

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.