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

TESTIMONY OF MARGARET WEICHERT
DEPUTY DIRECTOR FOR MANAGEMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE SUBCOMMITTEES ON
INFORMATION TECHNOLOGY AND GOVERNMENT OPERATIONS OF THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

March 14, 2018

Chairman Hurd, Ranking Member Kelly, Chairman Meadows, Ranking Member Connolly, and Members of the Subcommittees, thank you for the opportunity to appear before you today to discuss the state of Federal information technology (IT) in 2018.

In December, I had the pleasure of testifying before the Senate Committee on Homeland Security and Governmental Affairs. At that time, I discussed the broad range of disciplines that the Deputy Director for Management is charged with overseeing, including IT, Information Security, Human Capital Management, Finance, Accounting, Performance Management and Procurement. Today, as the newly sworn in Deputy Director for Management, I am working with our agency partners to drive necessary improvement in those disciplines, and I am excited to talk about one of those core areas – IT modernization – in depth.

Improving our technology infrastructure to enhance the quality, security, and impact of services we deliver to taxpayers is fundamental to bringing the Executive Branch into the 21st Century. To that end, next week we will be releasing the President's Management Agenda (PMA), of which IT modernization is one of three pillars. The PMA will set forth a long-term vision for an effective Government that better achieves its missions and enhances the key services upon which the American people depend. Modernization is the essential backbone of how Government serves the public in ways that meet its needs, while keeping sensitive data and systems secure and private. IT modernization efforts directly support the other two pillars of the PMA – modernizing the government workforce to align staff skills with evolving mission needs, and delivering transparency through data to increase accountability.

The Office of Management and Budget (OMB) has always played a critical role in Government IT modernization, and this has been a core competency of OMB since the establishment of the Office of E-Government and Information Technology in 2002. The importance of IT in delivering results to the public has substantially increased since then. This Administration has therefore doubled down on the commitment to technology modernization. The United States Digital Service (USDS), also housed in OMB, has added capabilities to pursue IT modernization.

And, on May 1, 2017, the President established the American Technology Council (ATC) via Executive Order (E.O.) No. 13794, to effectuate the secure and efficient use of IT across the Government, and to serve as a primary convening body between Government and industry to ensure that the Executive Branch is leveraging commercial technology and best practices. Just days later, on May 11, 2017, the President signed Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* to enhance cybersecurity risk management across the Government. OMB is the at the center of the work supporting both the American Technology Council and the implementation of Executive Order 13800, while driving performance and accountability for these initiatives across the Government.

Today I will talk about OMB's ongoing efforts to implement E.O. 13800, including the progress implementing the December 2017 *Report to the President on Federal IT Modernization*, as well as the work that OMB is doing to implement the Modernizing Government Technology Act and to oversee Federal cybersecurity.

IT Modernization Report

The American Technology Council published the Report to the President on Federal IT Modernization in December 2017. It recommends 50 crosscutting actions to improve the security posture of Federal agencies as they implement their IT modernization plans to address network consolidation/modernization and shared services. The Administration is making great progress toward implementing these actions, and the OMB team is collaborating with its interagency partners to reduce or remove barriers for agencies to leverage more modern, dynamic, commercially-available IT solutions. For example, OMB is actively working to identify efficient and effective service offerings for Cloud-based email and collaboration tools, which help facilitate the daily work of millions of Federal employees.

OMB is also developing policies to reduce agency reporting burdens and to securely deploy a modern IT infrastructure. We will be updating the policies governing the High Value Assets, Trusted Internet Connections, and Continuous Diagnostics and Mitigation programs, and revising the way we address identity management in the Federal Government. The goal is to better enable agencies to leverage dynamic, secure, and commercially available IT solutions by removing existing barriers. OMB will track the implementation of these policies through its management and budgetary oversight functions, and through the Modernize IT to

Increase Productivity and Security Cross-Agency Priority (CAP) goal that supports the forthcoming President's Management Agenda.

Implementation of the Modernizing Government Technology Act

The Oversight and Government Reform Committee has been instrumental in recent years in driving Federal IT modernization through its development of legislation such as FITARA and the DATA Act. Since it is Sunshine Week, a time where we celebrate open access to public information, I want to particularly recognize the influence the DATA Act has had in advancing Federal data transparency. We also greatly appreciate Chairman Hurd's introduction last year of the House version of the Modernizing Government Technology (MGT) Act, and the support that bill received from subcommittee members that contributed to its enactment as part of the FY 2018 National Defense Authorization Act. The MGT Act is designed to provide agencies flexible sources of funding required to meet high priority technology modernization goals. Successful implementation of this law is critical to the Administration's IT modernization agenda. In order to drive execution of the MGT Act, on February 27th OMB issued M-18-12, Implementation of the Modernizing Government Technology Act, describing actions agencies can take to utilize the Technology Modernization Fund (TMF) and the IT Working Capital Funds (WCFs) authorities. Together, the MGT provides additional flexibilities so

OMB and agencies have the financial resource mechanisms and technical expertise necessary to move the Government closer to leading industry practices in IT modernization. This will allow agencies to pivot their energy and attention away from traditional bureaucratic problems towards embracing technology opportunities, and will ultimately allow the Government to provide better, more secure, user-centered services to the American people.

When the TMF is funded, the interdisciplinary board of experts who oversee the fund will provide necessary resources to high-impact, mission-focused agency IT projects. OMB is working closely with agencies that wish to establish IT WCFs so they can utilize best practices generated as part of the TMF process to evaluate and fund agency IT modernization efforts that are agile, successful, and deliver meaningful change.

OMB itself must lead the way in ensuring that the money we spend on our own personnel and service -- whether it is USDS, the Office of E-Government, or our other cross cutting management offices -- delivers the type of results expected by our agency partners, Congress and the American people. We are also looking to make more strategic use of the IT Oversight and Reform (ITOR) fund to direct expenditures and personnel to our highest technology priorities and make sure that

lessons learned from interacting with agencies and helping them solve their problems informs our longer term policy development and modernization efforts.

USDS Support of Technology Modernization Efforts

Since 2014, USDS has been an OMB component that effectively enhances Government service delivery to the American people through technology and design. USDS is focused on improving and transforming the experience of Americans who interact with the Government online. This means more citizens are able to access more Government services online due to more streamlined and secure methods of identity verification. It means veterans receiving appeals responses in a more timely manner. This work can ultimately help rebuild Americans' trust in Government. In addition to its work with individual federal agencies, USDS delivers projects such as the TechFAR Hub, a website that brings industry best practices to federal digital service acquisition, helping the Federal government to build the knowledge it needs to modernize its procurement strategy.

Cybersecurity

Far-reaching cybersecurity incidents of 2017 demonstrate the potentially harmful impact that insufficient cybersecurity can have on our Nation. Hundreds of millions of Americans had their personally identifiable information (PII)

compromised in a series of private sector data breaches that exploited unpatched vulnerabilities at companies whose core services focus on safeguarding that very information. Tens of thousands of Federal employees and taxpayers also had their information compromised because of vulnerabilities in agencies' data and system protections. These incidents continue to demonstrate that effective cybersecurity requires any organization — whether it be a Federal agency or other public or private company — to identify, prioritize, and manage cyber-risks across its enterprise.

The President signed Executive Order 13800 in May 2017 to enhance cybersecurity risk management across the Federal Government. E.O. 13800 recognizes that the Government must ensure that it is able to properly secure citizens' information and that agencies can protect their systems even as malicious cyber actors seek to disrupt their services. Accordingly, E.O. 13800 requires every agency to conduct comprehensive reviews of their cybersecurity programs. The order also directs OMB, Department of Homeland Security (DHS), Department of Defense, Department of Commerce, and several other key agencies to review cybersecurity practices across the Government and critical infrastructure sectors. E.O. 13800 assesses the sufficiency of agencies' risk mitigation and acceptance choices and includes a plan for remediating cybersecurity performance gaps. In

implementing E.O. 13800, OMB determined that agencies lack sufficient situational awareness of the threat environment, capabilities to adequately detect intrusions and data exfiltration, and fundamental accountability for mitigating cyber risks across the enterprise.

While E.O. 13800 is part of the roadmap for securely modernizing Federal IT systems over the coming years, our Modernize IT Cross Agency Priority (CAP) goal will establish meaningful metrics that focus on cybersecurity capabilities that reduce cyber risks to agency missions, the most tangible return on investment that we can demonstrate. The CAP goal emphasizes long-standing efforts of OMB and DHS to enforce disciplined, risk-based, cyber practices across Government, and to help safeguard agency IT systems, including helping agencies to address critical vulnerabilities and implement multi-factor authentication. Progress to date is encouraging, but insufficient. Agencies endured 35,277 cybersecurity incidents in Fiscal Year (FY) 2017, a 14% increase over the 30,899 incidents that agencies reported in FY 2016. Modernizing our IT Infrastructure will reduce the risk of crucial services being disrupted. Toward this end, the $15 billion cybersecurity budget request submitted as part of the President's FY 19 Budget would fund investment in critical capabilities to safeguard agency IT assets and data. OMB's data-driven oversight of agency programs directly informed this request level.

Also essential are the current and future Federal workers needed to help implement these critical capabilities. The nation's growing challenges require a capable Federal technology and cybersecurity workforce that possesses the necessary knowledge, skills, and competencies to counter increasingly sophisticated and ever-changing threats. I am working with the Office of Personnel Management, DHS, the National Institute of Standards and Technology (NIST), and agencies across the Executive Branch on government-wide actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats.

Closing

In closing, OMB looks forward to working with Congress on IT modernization. Through our collaborative efforts, we will be able to improve Government services and cybersecurity. I thank the Subcommittees for holding this hearing, and for your commitment to IT modernization. I would be pleased to answer any questions you may have.