Testimony to House Committee on Oversight and Government Reform

Suzette Kent

Federal Chief Information Officer

Office of Management and Budget

July 25, 2018

Government Accountability Office's High Risk Cybersecurity Issues Report

Chairman Hurd, Chairman Meadows, Ranking Member Kelly, Ranking Member Connolly and Members of the Committees, thank you for having me here today.

Tomorrow will mark five months serving as the Federal Chief Information Officer (Federal CIO) within the Office of Management and Budget (OMB). In the short time in my role, I have had the great opportunity to learn from and work with a tremendous number of talented, driven, thoughtful, and passionate technology and cybersecurity professionals across the Federal Government. I am honored to be here today to talk with you and I appreciate participating in forums that draw attention and inspire actions toward improving federal cyber security. Advancement of our cyber security posture both at Agency level and across the government enterprise is one of the most important parts of my job.

My goal in being here today is to share with you some of the progress that has been made against the areas highlighted by GAO, but also to share what still must be done and engage your continued support against these objectives. I joined the Federal Government five months ago tomorrow from the Financial Services

industry where cybersecurity and data protection are at the core of industry capabilities. I bring that high bar of expectation to my role as Federal CIO.

As the Federal CIO, I am responsible for assisting Director Mulvaney in implementing OMB's statutory role per the E-Government Act of 2002 and the Federal Information Security Modernization Act of 2014 (FISMA).[1] These statutory roles include improving the management and operations of Federal civilian information technology systems and overseeing the information security programs of non-National Security Systems. It is important to note that the FISMA cybersecurity responsibilities for National Security Systems is delegated to the Director of National Intelligence and the Secretary of Defense. For those non-National Security Systems, the Office of the Federal CIO (OFCIO), executes OMB's statutory roles by developing and overseeing the implementation of policies and guidelines. OFCIO works with Federal civilian agency leadership to address information security priorities, collaborates with partners to develop cybersecurity policies, and conducts data-driven oversight of agency cybersecurity programs.

OMB's cybersecurity responsibilities under FISMA are addressed by three areas we focus on:

1. Developing and overseeing the implementation of cybersecurity policies and guidance for Federal civilian information technology systems.
2. Collaborating with agencies to protect federal civilian information technology systems and establishing a risk based approach to cybersecurity.
3. Ensuring that agencies are complying with federal cybersecurity policies and standards, in coordination with the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS).

In addition to these specific responsibilities, OMB works closely with our partners across government to ensure the security of the Federal civilian enterprise. This includes working with DHS, the National Security Council (NSC), Intelligence Community, Department of Defense (DoD), and others to respond to significant cybersecurity incidents and breaches. We also coordinate with agency Chief

[1] Public Law (P.L.) 113-283, FISMA Modernization Act of 2014 (2014), https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

Information Officers (CIOs) and Chief Information Security Officers (CISOs) to improve their ability to allocate resources to manage cyber risks within their department or agency. Improving communication, coordination, and implementation of the various roles and responsibilities set forth under FISMA is a critical task, and one I take very seriously as the Federal CIO, but it is only a part of this Administration's larger cybersecurity efforts.

We also collaborate with the Federal Inspectors General (IG) community to drive accountability and improve cybersecurity program performance across the government. We work closely with the IGs, CIOs, and CISOs. Throughout our collaboration, we work toward the same mission of securing Federal information and information systems. The improvements in Federal cybersecurity over the past few years, which GAO outlines in its most recent High Risk report, are a due to a culture of accountability and performance that we have enhanced with our oversight partners.

This Administration has made it a priority to improve our nation's cybersecurity. In May 2017, the President signed Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, (EO 13800)[2] to enhance cybersecurity risk management across the Federal Government. This executive order recognizes that the Government must promote the security of citizens' information and ensure that agencies consider cybersecurity as a vital element of their core missions and services, including the fundamental threat to mission and services posed by malicious cyber actors. The Executive Order also directed OMB, DoD, DHS, and the Director of National Intelligence, among other agencies to assess risks within their respective purviews, and develop action plans and strategies to mitigate those risks.

Pursuant to EO 13800, the White House published the Report to the President on Federal IT Modernization[3] (IT Modernization Report) in December 2017. In addition to surveying the state of Federal IT, the IT Modernization Report included 52 discreet, time-bound tasks focused on modernizing and safeguarding

[2] White House, Executive Order 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[3] American Technology Council, Report to the President on Federal IT Modernization (2017), https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf.

High Value Assets (HVAs), promoting the consolidation of network acquisitions and management, and driving agencies to leverage commercial cloud solutions and cybersecurity shared services. OMB, in coordination with DHS, NIST, and the General Services Administration (GSA), has completed 37 of those 52 tasks, many ahead of schedule. We intend to complete the rest of the tasks on time and by the end of the year.

In addition to the IT Modernization Report, EO 13800 required OMB to develop the *Federal Cybersecurity Risk Determination Report and Action Plan*, which provides a comprehensive review of Federal agencies' cybersecurity programs to date. OMB and DHS conducted 97 agency risk management assessments to measure the sufficiency of agencies' cybersecurity capabilities and risk mitigation approaches. OMB found that agencies lack situational awareness of the threat environment, capabilities to detect intrusions and data exfiltration, and fundamental accountability for mitigating cyber risks across the enterprise. OMB is leveraging these findings to drive returns on investment across the $15 billion in Federal cybersecurity spending in terms of reducing risks to the Federal enterprise.

We are currently working on many other initiatives to drive stronger accountability and improvement in Federal cybersecurity. As the Chair of the Technology Modernization Board, I am working to administer the Technology Modernization Fund to drive high impact investments to reduce or upgrade outdated legacy systems and improve agency service delivery. We appreciate the $100 million investment by Congress in FY 2018 for this important initiative and we look forward to working with this Committee and the Appropriations Committees to secure more funding in FY 2019 to continue our modernization efforts and multiply the impact and scope of the projects the TMF can fund.

We are working with the White House and Federal agencies to implement Executive Order 13833, which clarifies and reinforces the authorities and provenance of agency CIOs in IT budgeting and making risk based determinations across agency IT investments. We are working with the Federal community to better understand agency issues and incorporate that into OMB guidance. We are expecting to deliver new, updated, iterative policies around securing high value assets, data center optimization, information security continuous monitoring, and

network optimization and performance in the coming months. These policies will allow the Federal government to make smarter, risk informed investment and leverage modern technologies and enable our agencies to be more agile, responsive, and secure – which are goals OMB, GAO, and Congress all share.

Cybersecurity is a core component of the President's Management Agenda (PMA). IT Modernization goals, but it is also embedded in the work we are driving under the Sharing Quality Services Goal, the Improving IT Spending Goal, and many other subgoals and strategies anchored throughout the entire PMA. Further, both the PMA and the recent Reshaping American Government in the 21st Century reorganization and reform plan include explicit strategies and milestones to retain, reskill, and modernize our Federal IT and cybersecurity workforce, because security is as much a personnel issue as it is a technology issue.

The Deputy Secretaries and other senior officials who make up the President's Management Council, as well as OFCIO, DHS, and additional agency leadership are committed to continuous improvement and excellence in these areas.

These success stories underscore the great work that has occurred and illustrate the work that remains before us. It is also critical to showcase the success stories across agencies and outside government to prove that we can be successful and share the path to success so that Agency teams can leverage the experiences of others and have the confidence of achievable goals. By successfully delivering on our agenda, we build trust with the American public, and our stakeholders in Congress and the Administration. In this regard, I was fortunate to take on my current role with a clear, focused agenda against which we can execute. My job is to build relationships, eliminate blockers, and focus time, money, and attention – where warranted and effective – to propel further success in these vital cybersecurity areas.

Cybersecurity must underpin everything we are doing with respect to acquiring, deploying, operating and maintaining information technology across the government. The threats to our Nation continues to increase as our systems become more interconnected and malicious tools become more available. We are working across Federal agencies and industry to drive a risk management culture and reduce the impact that cyber incidents can have on core government

functions. I look forward to working with Comptroller General Dodaro and GAO, and our other Federal partners to enhance the government's security posture.

Thank you again for inviting me here today. I look forward to answering your questions.

Suzette Kent currently serves as the Federal Chief Information Office at the Office of Management and Budget. Ms. Kent is an industry leader of large-scale business transformation using technology, for the world's most complex organizations. She was most recently a principal at EY and has been a partner at Accenture, consulting president at Carreker Corporation and a Managing Director at JPMorgan. Although technology change has been at the core of her professional career, retooling the workforce and creating new opportunities for people has been an essential element of efforts that she has led. She has served as an enterprise leader for organizational learning, diversity and inclusiveness, and career development at every organization in which she has worked. Ms. Kent has been a frequent speaker in global industry forums, publisher of thought leadership pieces and holds patents in banking processes.