EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 22, 2013

STATEMENT OF STEVEN VANROEKEL
FEDERAL CHIEF INFORMATION OFFICER,
ADMINISTRATOR FOR E-GOVERNMENT AND INFORMATION TECHNOLOGY,
OFFICE OF MANAGEMENT AND BUDGET

BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

"Innovating with Less: Strategically Investing in Federal IT"

Good morning, Chairman Issa, Ranking Member Cummings, and Members of the Committee. Thank you for this opportunity to testify on the Administration's efforts to manage the Federal Government's investment in information technology (IT).

As I was finishing my undergraduate degree, the era of personal computing was just being set in motion, and within months of graduation, I was working for the Microsoft Corporation. Before joining Federal Government in 2009, I spent my entire post-college private-sector career at Microsoft, including three years as Speech and Strategy Assistant to Bill Gates, the corporation's co-founder, and most recently as Senior Director of the Windows Server division. I saw firsthand the power of technology and saw the incredible impact American innovation has on society.

During that nearly 20 years in the private sector, I woke up every day focused on improving and expanding core services and customer value, while also cutting costs. Although information technology is a small part of the Government's annual spending, it is at the core of almost everything we do. As such, we must ensure that the Government maximizes the return on its investment in Federal IT, drives innovation to meet customer needs, and establishes a trusted foundation for securing and protecting our IT assets.

As the Committee is aware, customer demand, fiscal austerity, and the interconnectedness of our digital world dictate that we must continually improve the way we procure, build, and manage Federal IT. The growth and pervasiveness of cloud computing, mobile devices, information, and social media are creating a demand for Government services that were once unforeseen. Expectations have reached a critical point even faster than anticipated.

Today, Americans pay bills online and buy plane tickets on smartphones. They expect us, through the use of technology, to provide the same quality of service they experience in their everyday lives. The Government must work to meet these expectations, efficiently and securely.

Eliminating duplicative IT, reforming Federal IT management, and streamlining service delivery were at the core of the Administration's first term IT agenda. Building on the progress of the last four years, my objective is to balance cost savings with innovation by continuing to cut costs while we invest in technology that securely serves the American people.

Strategic Priorities

The Administration must approach the strategic investment in IT through three priorities: innovating for the American people; improving our return on investment, or ROI; and advancing cybersecurity.

- **Innovate for the American People** – The value of Government programs rests upon their ability to positively impact the lives of Americans. Simply put, the American people must be at the center of every action we take, and each decision should be tied to a significant benefit for them. We should evaluate the success our IT investment by whether those efforts are meeting the public's needs. Those needs include simplifying the complexity of Government for the public. Additionally, the Government possesses a rich inventory of data. When utilized properly, with attention to privacy and security concerns, this data can create an incredible platform for innovation in the private sector while continuing to foster an increasingly important role for Government in the new data economy.

- **Improve the Return on Investment (ROI) of Federal IT** – To maximize our investment in IT, the Government must better manage the cost of providing IT services. Managing IT in an innovative way means consolidating redundant applications, systems, and services. It also means establishing common testing platforms to foster interoperability and portability so that we can build once and then use many times across the whole of Government. We must streamline the delivery of new infrastructure, and shift from asset ownership to service-orientation, which means that technology is delivered as a service – much like water or electricity – rather than built as a proprietary system. By culling from inefficiency and reinvesting in high ROI areas, we can drive innovation in government that creates efficient, mission-focused technology solutions.

- **Advance Cybersecurity** – The cybersecurity threat is one of the most serious national security, public safety, and economic challenges we face as a Nation. This issue requires creative solutions to address emerging and increasingly sophisticated threats, as well as

new vulnerabilities introduced by rapidly changing technology. To overcome these challenges, Federal agencies must improve cybersecurity capabilities to provide safe, secure, and effective mission execution and services to the American people, with a focus on accountability. Specifically, we must continue to implement initiatives such as the Cybersecurity Cross Agency Priority Goal, or CAP Goal, which is part of the Administration's broader performance management improvement effort, Federal Information Security Management Act, and the Federal Risk Authorization and Management Program (FedRAMP), and to continuously measure agency progress in improving information security performance.

In the near term, the Administration is using three strategic initiatives to measure and drive results in these areas. The first is the Administration's Digital Government Strategy—released last May – that is a comprehensive set of measures to deliver better digital services for the American people. The second is PortfolioStat, which is a tool agencies use to assess and improve the maturity of their IT portfolio management processes. The third is Cyberstat, which is a process that manages the security of our IT assets by identifying gaps and opportunities in agency cyber capabilities.

Digital Government Strategy

The Administration's Digital Government Strategy has three main objectives: (1) ensure the American people and an increasingly mobile workforce have access to high-quality, digital Government information and services anytime, anywhere, on any device; (2) ensure that in adjusting to this new digital world, the Government seizes the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways; and (3) unlock the power of Government data to spur innovation across our Nation and expand and enhance services available to the American people.

PortfolioStat

Last year, I launched PortfolioStat, which instituted a forum for agency stakeholders to collectively examine targeted outcomes, strategy, and overarching management processes to identify opportunities for improvement. This effort resulted in ambitious, forward-looking strategies that, if implemented, will save the Government from spending $2.5 billion over the next three years by consolidating duplicative systems, buying in bulk, and ending or streamlining off-track projects. In 2013, the Administration will continue to drive comprehensive performance and management evaluations so that agencies may better manage and improve the maturity of their IT portfolios. PortfolioStat demonstrates that there continues to be opportunity for agencies to focus on terminating redundant, outdated or otherwise low value investments to free up resources to fund emerging priorities.

CyberStat

CyberStat is a review process focused on improving agency cybersecurity performance as part of the Cybersecurity CAP Goal. The Cyber CAP Goal measures agency progress in implementing the three priority cybersecurity capabilities of continuous monitoring, trusted Internet connections, and strong authentication with Homeland Security Presidential Directive 12 (HSPD 12) personal identity verification cards. These reviews provide the opportunity for agencies to identify cybersecurity capability areas where they may be facing challenges (such as technology, organizational culture, internal process, or human capital/financial resource challenges), as well as prospects and strategies to improve cybersecurity performance.

Over the long term, the Administration, along with the Federal IT community will focus on opening our data, making use of lightweight emerging technologies, and adopting modular development methodologies, consistent with system security and privacy controls, to allow us to further increase the quality of Federal services while curbing costs.

Additionally, we recognize that agencies are at different levels of progress in terms of how they are using and managing technology. Rather than attempt to force-fit all agencies into the same solutions, we must begin with flexible frameworks that enable all agencies to innovate.

Results through Innovation

Innovation must become the central tool to drive strategic investment in Federal IT. There are many initiatives across Government that illustrate how, over the long term, we can more efficiently and effectively manage IT. Today, I want to highlight three examples of initiatives aligned with the strategic priorities in IT

Open Data. The information maintained by the Government is a national asset with tremendous potential value to the public, entrepreneurs, and to our own Government programs. The Administration's innovation agenda includes multiple initiatives that will open Government data to enhance information exchanges, interoperability, and public release (subject to valid restrictions) while enabling the public, including private sector entrepreneurs, to leverage open government data to create jobs and provide better services for the American people. We are already seeing new companies and new services being built around utilizing newly-available Government data. For example, in the last year, the online real estate services Trulia and Zillow made initial public offerings. The service these companies provide would not be possible without the government data that underlies the two websites.

IT-as-a-Service. Through the advent of cloud computing, the IT community now has a scalable and transparent way to purchase and provide services, enabling agencies to transform how the organization leverages technology by pivoting away from the old model of buying IT as an asset.

The technology "as-a-service" model allows agencies to buy only what they need and to share services more effectively across organizational silos. For example, the Department of Homeland Security (DHS) Office of the Chief Information Officer has stood up multiple "as a service" technology platforms, including email as a service, customer relationship management as a service, and business intelligence as a service, that each component of DHS can leverage without investing or building proprietary solutions of their own. This model allows DHS components to save time and money and instead focus their human capital on the varied and important missions across the Department.

Continuous Monitoring. Continuous monitoring is an integral part of an enterprise-wide risk management process that allows agencies to establish the context of their risk management programs, and subsequently assess, respond to, and monitor risk on an ongoing basis. As the world becomes increasingly interconnected, we must prepare to confront a host of new threats that evolve in real time.

These three examples are a small sample of many across the Federal Government where a strategic investment in innovation is driving better management of Federal IT. These initiatives, and the many other IT gains attained by this Administration, were achieved while lowering overall expenditures on Federal information technology.

Conclusion

In challenging times, we must tap into underutilized human capital, technology, information, and other resources, picking up the pieces to transform them into something completely new. Rather than use the current fiscal situation as an excuse to reduce services, the Administration views it as an opportunity to cut inefficiencies and invest in innovation that will drive better service, efficient spending, and more vigilant security.

As a general matter, the Federal Government has shifted its mindset from building proprietary and highly customized systems to adopting a vision of innovating with less. I appreciate the work this Committee has done in this area—as you know, the magnitude and importance of these efforts requires all of us to continue to work together.

Thank you for the opportunity to appear today and I look forward to our discussion.

Steven L. VanRoekel, Federal Chief Information Officer and Administrator, Office of Electronic Government, Office of Management and Budget

Steven was appointed as the second United States Chief Information Officer by President Obama on August 5th, 2011. Prior to his position in the White House, Mr. VanRoekel served as the Executive Director of Citizen and Organizational Engagement at the United States Agency for International Development (USAID) and as Managing Director of the Federal Communications Commission (FCC). At the FCC, Mr. VanRoekel oversaw all operational, technical, financial, and human resource aspects of the agency. He also led the FCC's efforts to introduce new technology and social media into the agency.

Prior to joining government in 2009, Mr. VanRoekel spent his entire career at Microsoft Corporation, including a stint as Speech and Strategy Assistant to Bill Gates, the corporation's co-founder, and most recently as Senior Director of the Windows Server division. He received a B.A. in Management of Information Systems from Iowa State University.