Testimony of Brook M. Colangelo

Chief Information Officer

Office of Administration

Executive Office of the President

Before the

House Committee on Oversight and Government Reform

May 3, 2011

Good morning Chairman Issa, Ranking Member Cummings, and distinguished Members of the Committee on Oversight and Government Reform. Thank you for inviting me to participate in this hearing on "Presidential Records in the New Millennium: Updating the Presidential Records Act and Other Federal Recordkeeping Statutes to Improve Electronic Records Preservation," and for your continued interest in the future of Executive Branch recordkeeping. As you consider potential changes to the Presidential Records Act and other federal recordkeeping laws, I am pleased to appear before you today to provide you with technical background information on the systems in place to maintain electronic records at the Executive Office of the President (EOP). I will also discuss our efforts to improve those systems and EOP information technology infrastructure as a whole.

Since January of 2009, I have been the Chief Information Officer (CIO) of the Office of Administration (OA). The OA was created by Reorganization Plan No. 1 of 1977 and formally established by Executive Order 12028 on December 12, 1977. OA's mission is to provide common administrative and support services to the EOP. I report to the Director of the OA, Cameron Moody, who has overall management responsibility for the OA. It is worth noting that OA's support role does not encompass developing policy options or articulating the Administration's views on legislative proposals.

The EOP is made up of components that advise and assist the President in carrying out his constitutional and statutory duties, including for example the White House Office (WHO), National Security Staff (NSS), Office of Management and Budget (OMB), United States Trade Representative (USTR), and OA itself. Some of these components are subject to the Presidential Records Act (PRA), while others are subject to the Federal Records Act (FRA). All EOP components, except the staff of the Executive Residence, are provided unclassified technology services by the Office of the Chief Information Office (OCIO). Throughout my testimony, I refer to these users and services as EOP users and EOP systems.

Some of the key functions that we provide are support of the EOP network; EOP email system; IT Service Desk, including support of business applications; management and protection of the EOP network against information security threats and risks; and operations and maintenance of the telecommunications infrastructure.

I understand that the Committee is exploring potential changes to the Presidential Records Act and other federal recordkeeping laws. My hope is that the technical background information I provide today, together with the legal and policy expertise offered by my colleagues at the National Archives and Records Administration (NARA), will aid the Committee's consideration of these potential changes. Because effective electronic records management rests upon a reliable and secure IT infrastructure, my testimony today will first provide an overview of the state of EOP IT infrastructure in January 2009 and the status of our IT modernization efforts. I will then discuss some current EOP systems and policies that directly relate to the management of electronic records. Of course, records management is an important consideration in OCIO's overall design and operation of EOP IT systems.

EOP Infrastructure in 2009

From the very beginning of this Administration, it was apparent that the EOP IT systems were struggling to maintain stable and secure operations due to aging infrastructure. We found that over 82 percent of IT assets (desktop computers, laptops, servers, etc.) were considered "end-of-life," which means that they were no longer supported by the original equipment

manufacturer. EOP enterprise software had not been upgraded in several years and was severely out of date. The EOP had a single data center and no viable plan or funding for a secondary, Disaster Recovery Data Center, which effectively puts the continuity of the EOP's systems in jeopardy.

The Administration faced several outages on the unclassified systems in January and February of 2009.

- **January 26, 2009 – Email down for 21 hours:** The EOP experienced a partial email service outage related to issues with Microsoft Exchange 2000. Roughly around 10:00 a.m. on January 26, an Exchange server crashed. This server was a newly-configured cluster (one of ten clusters overall) and had been built to support all the new staff of the Administration. An after action evaluation revealed that this outage was caused by the configuration of the server cluster but the EOP experienced further delays as a result of issues involving rebuilding the nine-year-old server technology. Once we brought the email back up for the new staff we quickly reallocated staff across the ten clusters.
- **February 3, 2009 – Email down for 1.5 hours:** The EOP experienced email service outages when the processor of the domain controllers reached capacity. The domain controller had a single processor and single core configuration which was a primary contributor to the incident. We rebooted the server to resolve the issue. Once stable, we rebuilt the troubled server and then added additional domain controllers for redundancy.
- **February 28, 2009 – Email down 7.5 hours and Network down 1.5 hours:** Again, the EOP experienced a partial email service outage related to the Exchange 2000 system. The EOP had a planned outage to replace a critical part of our Storage Area Network (SAN). The OCIO gracefully shut down the email servers but when the servers were brought back online one mail server crashed. An after action report revealed the root cause was the result of a critical file (called the hive) in the Windows Server registry being too large to load. The OCIO began monitoring the hive file from then on which improved the operations of the Exchange servers. On the same day, the EOP also experienced a network outage that was due to a failure in the core network switch. The redundant

network switch was not set to auto failover and this caused an outage. The OCIO also repaired the network switch and later tested fail over.

Recently, on February 3, 2011, we experienced another outage, which I will discuss later in my testimony.

Realizing the state of the EOP systems, we pulled together a Modernization plan that focused on the areas most in need of improvement. In May of 2009, I briefed Congressional staff on the problems with EOP IT infrastructure and the EOP IT Modernization Program, and we later obtained funding to implement the plan.

IT Modernization Initiatives

The IT Modernization Program focused on three areas: Stabilizing the Core, Mobilizing the Workforce, and Optimizing the IT Systems. To Stabilize the Core, we focused on investing in the core infrastructure technologies. To help guide this effort, we hired an independent audit team to assess the network. Based on its findings we did the following:

- Upgraded the Core Network Switches;
- Upgraded the East & West Wing Network;
- Upgraded the Internet Service Protocol (ISP) – increased performance over 300 percent;
- Upgraded and expanded the use of Web Gateways, which I will discuss later; and
- Patched network gear and tested fail overs.

As part of Stabilizing the Core, we also modernized EOP Messaging. We upgraded from MS Exchange 2000 to MS Exchange 2007, which not only allowed for Exchange 2007's enhancements, but more importantly allowed for the implementation of Microsoft's Continuous Cluster Replication (CCR). This new clustering technology enabled the EOP to move from a two node cluster sharing one set of disks, to a two node cluster with independent disk storage. Additionally, we upgraded the BlackBerry Enterprise Servers to BES 5.0, simplified the overall

architecture, installed new/modern servers, and upgraded our Storage Area Network to a stable and expanded system.

We also began work on a Disaster Recovery Data Center, which I will discuss later in my testimony. To expand our core cyber security tools, we upgraded and expanded the vulnerability scanning system. We also created a malware analysis system and upgraded the EOP firewalls. In addition, we created the GOALIE Program. GOALIE stands for Government Operations and Lead for Inspection and Execution and is the name of a team of government staff stationed at our data center to verify the work of the OCIO's contractors and troubleshoot technical issues. All of these changes stabilized core EOP IT systems, which both enhanced EOP operations and reinforced the efficacy of our records management measures.

We also modernized the EOP network by Mobilizing the Workforce of the EOP. Prior to 2009, EOP staff had few resources that enabled them to work remotely, whether due to travel, efficiency, or in support of the continuity of government. Mobilizing the Workforce created a roadmap for staff to work remotely in a secure and records-managed environment. The highlights of this program include Secure Mobile Workstations, which are laptops that encrypt data at rest, and Remote Access using SSL VPN, which is a secure remote access and records-managed web portal allowing staff to work remotely. These measures directly enhanced EOP electronic records management. The Secure Mobile Workstations allowed employees working at home to utilize their secure, records-managed EOP computer rather than a personal computer. Additionally, for those circumstances where EOP staff do not have access to their Secure Mobile Workstation, the SSL VPN allows them to access their EOP desktop, files, and applications in a secure, records-managed environment.

The Modernization Program also Optimized IT Systems to improve our business agility and fully support the mission of the EOP. To that end, OCIO replaced the EOP's correspondence tool to ensure the correspondence team is able to respond to mail and email in a timely and effective manner. This upgrade resulted in more correspondence being captured and tracked electronically. We also updated the Congressional Visitors Tour System, which provided enhancements and has expanded the number of tours for Congressional Offices.

Continuing Modernization Efforts: Disaster Recovery Data Center

The next major priority in our IT Modernization Program is the creation of a Disaster Recovery Data Center. The need for this center is well illustrated by the EOP's most recent outage, on February 3, 2011. On that day, the EOP email and network were down for nine hours. This outage was caused by two cuts in different locations to the EOP Synchronous Optical Networking (SONET) ring that connects the campus to our data center. While the circumstances leading to the outage were highly improbable – two separate cuts were made by a utility company's tree-trimming crews approximately 2.5 miles apart – the event highlighted the necessity of having a redundant data center which could have been used to provide mission critical IT services under such circumstances. Our team worked with our provider, who repaired the network as quickly as possible. Nonetheless, if the EOP had a Disaster Recovery Data Center, this outage could have been avoided.

Indeed, all of the outages discussed above would not have happened or would not have been so significant if the EOP had a Disaster Recovery Data Center. In any of those cases, when a service failed at the primary data center, it would have picked up at the Disaster Recovery Data Center and there would not have been an outage. A Disaster Recovery Data Center is a best practice – most corporations as well as the House and Senate have such facilities.

Aware of the need for such a center, we sought funding to stand one up. That funding was approved in the EOP's IT Modernization Budget in FY 2010 and to date we have accomplished the following:

- We signed a lease in 2010 for space in an existing, already-operational Data Center;
- We have connected the EOP Network to our new Data Center; and
- We have set up the preliminary facility infrastructure, such as network racks, power and cabling to the rack.

Now we will start focusing on installing essential services – first with the base layer, active directory, then installing messaging and archiving services. OA is working to ensure that thorough security is in place to protect the staff and information systems of the EOP. An operational Disaster Recovery Data Center will further enhance EOP electronic records management by keeping core, records-managed EOP systems running without interruption and by reducing the risk that electronic records will be physically destroyed.

Information Security

Information security is also essential to supporting records management—if data is stolen, altered, or destroyed, there could be an impact on EOP record-keeping as well as EOP operations. Additionally, in an insecure environment, people will be less likely to store confidential information in electronic form, reducing the effectiveness of electronic record-keeping measures.

We have taken significant steps to secure the EOP IT infrastructure. The EOP's primary Data Center is a physically-secured facility with state of the art information security. It is contained in an underground building in a federal facility protected by multiple fences. It is protected by manned security 24/7 and has security cameras throughout which record activities at the entry points and other strategic locations. The EOP Disaster Recovery Data Center will have similar measures in place.

The EOP Information Security program utilizes advanced tools and techniques to protect staff and data. We have a Security Operations Center – SOC – which is staffed 24/7 and monitors enterprise IT security of the EOP. The SOC monitors inbound and outbound traffic for malicious content and activity. We use packet capturing systems to analyze traffic for known malicious communications.

The EOP unclassified enterprise network is protected by firewalls that enforce policy on all inbound and outbound communications. Finally, the security team also evaluates hardware and software for security vulnerabilities for use on the EOP network. A risk assessment is

performed on new systems to ensure that they will not adversely impact the EOP network. The primary purpose of these security measures is to protect the EOP network and the information stored on it, but they have the important secondary effect of reinforcing electronic records management policies.

I now want to discuss several EOP systems and policies that relate even more directly to electronic records management. I will discuss:

- Enterprise Controls and Social Networking Access Restrictions;
- Personal Device and Personal Electronic Communications Policy;
- Email Archiving;
- Additional Electronic Message Archiving; and
- Social Network Archiving.

Enterprise Controls and Social Networking Access Restrictions

The EOP utilizes enterprise-wide controls to restrict access to certain websites and code that could pose records management or security risks. To do this, the EOP utilizes an industry leading Commercial-Off-The-Shelf (COTS) anti-malware and web filtering solution that analyzes the nature and intent of content and code entering the EOP network. This solution blocks access to a wide range of websites based upon filtered categories. This blocking was in place in January 2009, but we devoted resources to upgrading it in the spring of 2009 as a part of the Modernization Program. We have since doubled the number of servers to ensure EOP is protected from malicious content.

The EOP restricts access to websites by blocking categories of websites that are defined by the content filtering service. This service is updated on a daily basis by the vendor and will also restrict access to websites and files that are identified as malicious. Sites that are blocked include known web-based email services like Yahoo Mail and Gmail, known social network sites like Facebook and Twitter, as well as known instant messaging services like AOL Instant Messenger and Skype. Blocking these sites has the unfortunate effect of making it more difficult for EOP personnel to communicate with family and friends while working often long hours in

the office, but these measures are necessary from a security perspective and strongly reinforce EOP policy that work-related communications should take place on the EOP email system. The EOP network also blocks several other categories of sites for the protection of the EOP network.

A limited number of EOP staff (slightly more than seventy, less than two percent of active EOP accounts) have workstations with access to certain social network websites for official business. Before receiving access to these social network sites, users subject to the PRA receive a supplemental legal briefing on their records management responsibilities. Once users are authorized, they are placed in a separate access policy from general users and are identified by their computer.

Only a limited number of websites are accessible to users on the approved access list. Most are social networking sites like Facebook and Twitter. But sites like Gmail, Hotmail and Yahoo Mail are still blocked, along with messaging services like AOL Instant Messenger and Skype. To be sure, some of the approved sites do offer services similar to web-based email or messaging, which is why PRA personnel receive the supplemental legal briefing before obtaining access. Before a site is added to the approved access list, the addition is approved by IT security and legal personnel.

Personal Devices and Personal Electronic Communications Policy

Through technical measures and as a matter of policy, OCIO restricts EOP employees from connecting personal electronic devices to the EOP network. This protects the security of the network and the information stored within it. It also draws a clear line between work and personal equipment.

EOP employees in both PRA and FRA components receive information on applicable record-keeping requirements. EOP employees are instructed to conduct all work-related communications on their EOP email account, except in emergency circumstances when they cannot access the EOP system and must accomplish time sensitive work. In such situations, EOP employees are instructed to take the appropriate steps to preserve any presidential or federal

records on their personal accounts, for example by forwarding those communications to their EOP account or copying their EOP account on outgoing email.

Email Archiving

As this Committee knows, previous Administrations have faced substantial technical challenges in archiving EOP emails. However, as a result of initiatives undertaken by the Bush White House, from the very first day of the current Administration, the EOP has been able to rely on an automated system that archives email sent and received on the EOP system. This system utilizes EMC's EmailXtender, which is a Commercial-Off-The-Shelf product. EmailXtender archives inbound and outbound email messages in near real time and in original format with attachments, whether sent or received from EOP computers or EOP BlackBerries. The system also provides an archive with robust access control and audit capabilities. In simple terms, EmailXtender operates by bifurcating emails sent and received through the EOP network. An email sent to an EOP account bifurcates once it enters the EOP system, with one copy of the email going to the EOP user's mailbox and the second copy being archived within EmailXtender. When an email is sent by an EOP user, one copy is received by the recipient and the second copy is again archived within EmailXtender. I should note that EmailXtender is reaching end of life and will eventually be no longer supported by the vendor and become obsolete. Due to that fact, OA is currently exploring an upgrade or replacement of the EmailXtender system to ensure that OA's archiving system remains compliant.

Additional Electronic Message Archiving

As I have said, EOP policy requires EOP staff to conduct work-related communications on their EOP email account. However, in order to facilitate security alerts or other urgent communications in the event of an emergency that disables the EOP email system, EOP BlackBerry devices do have the capability to send and receive other forms of electronic communication. Specifically, EOP BlackBerry devices have the capability to receive SMS text messages over the Verizon network and send and receive PIN-to-PIN messages over Research in Motion's BlackBerry network. These alternative forms of electronic communication have been

proven to work during past emergencies like the Terrorist Attacks on September 11th. For these types of emergency scenarios, the Bush administration enabled SMS text and PIN-to-PIN functionality on EOP BlackBerry devices, and this policy has continued.

There was, however, no system in place to archive SMS text or PIN-to-PIN messages sent and received using EOP devices. Along with the other initiatives I discussed previously, I am happy to report that, after exploring the technical options, OCIO now has systems in place to archive SMS text and PIN-to-PIN messages sent or received using EOP BlackBerry devices by pulling those messages directly from the servers they are transmitted over. OCIO began archiving PIN-to-PIN messages in November of 2010 and SMS text messages in early March of 2011. Although this does not alter EOP policies requiring work-related communications to take place on the EOP email system, these initiatives to improve our recordkeeping systems will ensure that emergency communications sent over either system will be archived.

Social Network Archiving

I also wanted to briefly raise the issue of archiving government records created on social networks. Currently, the management of this material is handled on a component-by-component basis within the EOP—OCIO does not provide an enterprise solution. During the summer and fall of 2009, OCIO did explore whether it would be possible to offer an enterprise solution, issuing a Request for Proposal for an automated solution to archive government records created on publicly-accessible websites like Facebook and Twitter. We learned from that process that the technology in this area had not matured enough to offer a sufficiently comprehensive, reliable, and affordable solution, and consequently ended the procurement after reviewing the bids that had been submitted.

Consequently, the records management of these social media records is handled on a component-by-component basis, rather than by OCIO. For example, I am aware that the White House Office utilizes a combination of traditional manual archiving techniques (like saving content in an organized folder structure) and automated techniques (such as Real Simple Syndication (RSS) feeds and Application Programming Interfaces (APIs)) to archive records

created by the White House on social network sites like Facebook and Twitter. Should technological solutions develop that allow OCIO to offer an enterprise-wide solution to archiving this material, we will certainly pursue those possibilities as we have other initiatives to improve management of electronic records at the EOP.

With respect to the archiving of government records on personal social network accounts, EOP policy requires staff to conduct work-related communications on their EOP account. And as I have described, social networks and similar sites are blocked from the EOP network. Staff have also received guidance that the Presidential Records Act applies to work-related electronic communications over both official and personal accounts, which includes social networks.

In conclusion, OA has made significant progress in improving the quality, security, and reliability of the EOP's information technology systems, and in upgrading the EOP's records management capabilities, building on the Bush Administration's important work to develop a reliable email archiving system. We look forward to continuing those efforts as we stand up a Disaster Recovery Data Center and encounter emerging technologies. I hope that this technical background information will be helpful to the Committee's consideration of potential changes to the Presidential Records Act and other federal record-keeping laws. In closing, I would also add that it is essential that we continue to invest in the operation and modernization of EOP IT infrastructure to avoid problems similar to those that have occurred in the past. Thank you for your continued support.

Mr. Chairman, this concludes my statement. Thank you for this opportunity, and I would be pleased to answer any questions that remain.

Brook Colangelo
Chief Information Officer (CIO), Office of Administration
Executive Office of the President (EOP)

Brook Colangelo is the Chief Information Officer (CIO) for the Office of Administration in the Executive Office of the President (EOP). Mr. Colangelo manages the unclassified enterprise technology that supports the EOP, including the White House and President of the United States.

Upon his appointment, he created a strategic plan to stabilize, mobilize and optimize the EOP's IT infrastructure. He moved EOP employees off of desktop computers and onto secure mobile work stations. His foresight on this critical workforce need was put to the test when the Washington Metropolitan Area was immobilized for a week due to the 2010 blizzard. While the federal government was closed, the new mobile work stations and other tools allowed 60 percent of EOP employees to get online and complete mission critical functions, ensuring that White House operations continued.

Mr. Colangelo previously worked as the CIO of the Democratic National Convention Committee, where he successfully managed an interactive Convention and led a green technology initiative to reduce the Committee's carbon footprint. He also served as the Information Technology Project Manager for the American Red Cross' Hurricane Recovery Program (HRP), which was dedicated to helping rebuild lives from the devastation of Hurricanes Katrina, Wilma and Rita. Prior to that, Mr. Colangelo served as the Director of Technology for QRS Newmedia Inc, a dynamic communications and consulting firm in Washington, DC. Mr. Colangelo has experience in the IT management of a wide range of projects, including technology and telecommunication construction, application and web development, and renovation of technology infrastructure.

Mr. Colangelo earned a Bachelor of Arts degree from the George Washington University and is a certified Project Management Institute (PMI) project manager. He is a recipient of Federal Computer Week's The Federal 100 and InformationWeek's first-ever compilation of the top 50 CIOs in federal, state, and local government.