PRESIDENTIAL RECORDS IN THE NEW MILLENNIUM: UPDATING THE PRESIDENTIAL RECORDS ACT AND OTHER FEDERAL RECORDKEEPING STATUTES TO IMPROVE ELECTRONIC RECORDS PRESERVATION

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 3, 2011

Serial No. 112–45

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

70–518 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana
JOHN L. MICA, Florida
TODD RUSSELL PLATTS, Pennsylvania
MICHAEL R. TURNER, Ohio
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
CONNIE MACK, Florida
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
ANN MARIE BUERKLE, New York
PAUL A. GOSAR, Arizona
RAÚL R. LABRADOR, Idaho
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
JOE WALSH, Illinois
TREY GOWDY, South Carolina
DENNIS A. ROSS, Florida
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas
MIKE KELLY, Pennsylvania

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
EDOLPHUS TOWNS, New York
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
DANNY K. DAVIS, Illinois
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
CHRISTOPHER S. MURPHY, Connecticut
JACKIE SPEIER, California

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
ROBERT BORDEN, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

PRESIDENTIAL RECORDS IN THE NEW MILLENNIUM: UPDATING THE PRESIDENTIAL RECORDS ACT AND OTHER FEDERAL RECORDKEEPING STATUTES TO IMPROVE ELECTRONIC RECORDS PRESERVATION

TUESDAY, MAY 3, 2011

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 9:35 a.m., in room 2154, Rayburn House Office Building, Hon. Darrell E. Issa (chairman of the committee) presiding.

Present: Representatives Issa, McHenry, Jordan, Lankford, Amash, Buerkle, Gosar, DesJarlais, Guinta, Farenthold, Cummings, Maloney, Tierney, Clay, Connolly, and Murphy.

Staff present: Ali Ahmad, deputy press secretary; Robert Borden, general counsel; Molly Boyl, parliamentarian; Steve Castor, chief counsel, investigations; John Cuaderes, deputy staff director; Gwen D'Luzansky, assistant clerk; Adam P. Fromm, director of Member liaison and floor operations; Linda Good, chief clerk; Frederick Hill, director of communications; Ryan Little, manager of floor operations; Justin LoFranco, press assistant; Mark D. Marin, senior professional staff member; Ashok M. Pinto, deputy chief counsel, investigations; Jonathan J. Skladany, senior investigative counsel; Becca Watkins, deputy press secretary; John A. Zadrozny, counsel; Krista Boyd, minority counsel; Ashley Etienne, minority director of communications; Jennifer Hoffman, minority press secretary; Carla Hultberg, minority chief clerk; Lucinda Lessley, minority policy director; Amy Miller, minority professional staff member; Brian Quinn, minority counsel; Dave Rapallo, minority staff director; Suzanne Sachsman Grooms, minority chief counsel; and Mark Stephenson, minority senior policy advisor/legislative director.

Chairman ISSA. The committee will come to order.

Today we will hear testimony on the Presidential Records in the New Millennium: Updating the Presidential Records Act and Other Federal Recordkeeping Statutes to Improve Electronic Records Preservation.

We exist to secure two fundamental principles: first, Americans have a right to know that the money Washington takes from them is well spent and, second, Americans deserve an efficient, effective government that works for them. Our duty on the Oversight and Government Reform Committee is to protect these rights. Our solemn responsibility is to hold government accountable to taxpayers,

because taxpayers have a right to know what they get from their government. We will work tirelessly in partnership with citizen watchdogs to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy. This is the mission of the Government Oversight Committee.

Today's hearing concerns the status of executive branch compliance with the letter and spirit of the Presidential Records Act. The American people trust in the Presidential Records Act; they trust in this over 30-year-old piece of legislation to preserve for all time the records of each administration. Crafted in the aftermath of Watergate scandal, the act marked a major step forward in openness and transparency for the White House. By mandating the careful preservation of public accessibility of official records, the American people would have an accurate historical record of decisionmaking.

The purpose of this act is clear, but history moves on, technology moves on, and today we deal, without a doubt, with an administration who has to, by policy, attempt to implement modernization of an act that never envisioned Facebook and Twitter. This is not a new problem, but it is a growing problem. The Clinton administration first had the digital age, but ultimately seeing that email versus paper mail is substantially the same and when printed is identical made it relatively easy to comply with.

During the Bush administration, unfortunately, the move from Lotus Notes to Microsoft Exchange made us acutely aware that the quantity of digital information, if not lost but simply misstored, could end up costing us tens of millions of dollars to recover. In fact, the digital age is more complex and, if not handled correctly, is both more subject to loss of critical records and cost to preserve and recover them.

We on the committee have broad oversight and we try to do each part of government as best we can. But we do have limited special responsibilities. The Presidential Records Act falls to this committee. We take seriously that the decades that have gone by have caused an act fully understood to be very difficult to implement. We look forward to our witnesses helping us as we begin to craft the types of legislative reforms that will codify good policy that has been developed by multiple administrations and go beyond that to make it clear to the American people that all transactions appropriate and equivalent to the original ones captured will be captured in the digital age.

I now recognize the Ranking Member for his opening statement.

[The prepared statement of Chairman Darrell E. Issa follows:]

Full Committee Hearing

"Presidential Records in the New Millennium: Updating the Presidential Records Act & Other Federal Recordkeeping Statutes to Improve Electronic Records Preservation"

May 2, 2011

Rep. Darrell Issa, Chairman

Hearing Preview Statement

Tuesday's hearing of the House Committee on Oversight and Government Reform, entitled "Presidential Records in the New Millennium" will examine current federal recordkeeping laws and evaluate options for improving the rules governing the collection, storage, and preservation of official electronic communications and documents.

Since the passage of the Presidential Records Act 33 years ago, electronic media and information technology have proliferated across the federal government. Yet Congress has not undertaken a legislative effort to update the law and meet the demands of the digital information age. Three different presidents have issued executive orders to supplement the Presidential Records Act, but each has addressed issues relating to presidential privilege or the restriction of access to presidential documents. The classification of documents and rules of their collection, storage, and preservation, however, have remained unaltered since the Watergate era.

Many of the technologies in use today permit federal employees to easily bypass the tools and protocols designed to capture official communications and documents. Instant messaging and text-messaging devices, personal e-mail accounts, social networking websites, and other emergent technologies not only allow federal employees to communicate outside of official federal channels during business hours, but also are not stored or retained by federal recordkeeping authorities.

Press accounts have revealed that senior White House officials have used personal, non-government e-mail accounts to communicate about official business and to arrange meetings and conversations beyond reach of the Executive Office of the President. These developments serve to highlight the need for legislative reforms to update the Presidential Records Act and ensure that current and future generations of Americans have access to the critical information about their government.

###

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Mr. Chairman, first of all, before I begin, I would like to commend everyone who worked so hard for so long to bring Osama bin Laden to justice. I thank our military service members, our intelligence officials, our diplomatic corps, our law enforcement officials, and our Nation's leaders from both political parties. This was a sustained, unrelenting effort over a decade, and it shows that when America confronts its most daunting challenges, we can come together with a striking and inspiring unity of purpose.

The Presidential Records Act and the Federal Records Act are landmark open government laws that are based on a fundamental principle that Federal agencies must retain records of their official business. These include records that have historical value, as well as records that are important for administrative, informational, and evidentiary reasons.

The electronic age has brought new opportunities for making government work more effectively and efficiently on behalf of American taxpayers. It has also brought new challenges for ensuring that the Federal records are maintained properly.

Previous administrations have experienced problems preserving electronic records, particularly emails. During the Clinton administration, the email system experienced technical problems that resulted in lost emails. During the Bush administration, the White House conceded that it lost hundreds of days of official emails, and top officials routinely use their Republican National Committee email accounts for official business.

To address these problems, the current system now automatically preserves all emails from White House email accounts. In addition, White House computers block access to private email accounts like Gmail and Hotmail. Finally, if White House employees receive emails relating to official business on their personal accounts, they are directed to preserve those emails, either by forwarding them to their official accounts or by printing them.

As cutting-edge technologies continue to develop, they will create additional opportunities and challenges. Government officials can now communicate with each other and with the American public in new and creative ways through Facebook, Twitter, and other social media outlets. We want to encourage this kind of innovation. At the same time, we must ensure that records of official communications are preserved.

The Obama administration has worked closely with the National Archives to develop new policies relating to social media. To begin with, it has limited access to these platforms to a small fraction of White House employees. It has also worked with the National Archives to develop protocols to save official postings and samples of public comments in a manner that is consistent with its protocols for written correspondence.

As you know, Mr. Chairman, I always believe more can be done, so the question for today's hearing is whether we can improve the Presidential Records Act and the Federal Records Act. The clear answer from this side of the aisle is yes. On March 17, 2011, I introduced H.R. 1144, the Transparency and Openness in Government Act, a package of five bills that overwhelmingly passed the House last Congress with broad bipartisan support, including your

own, Mr. Chairman, and every Democratic member of this committee joined me, as an original cosponsor of this legislation.

H.R. 1144 includes electronic message preservation act which modernizes the Presidential Records Act and the Federal Records Act to ensure that the White House and agency emails are preserved electronically. Right now the law requires only that these records be saved; there is no requirement that they be saved electronically. This legislation had such bipartisan support last Congress that it passed the House by voice vote on March 17, 2010.

Since I introduced H.R. 1144 in March, a wide spectrum of open government groups has endorsed it. On April 18, 2011, a coalition of 17 organizations wrote to both of us seeking bipartisan support and prompt action in the House. They also said H.R. 1144, the Transparency and Openness in Government Act will enhance the effectiveness of Federal advisory panels, provide more access to Presidential records, secure electronic messages generated by administration officials, ensure donations to the Presidential libraries' open of the public record, and give the Government Accountability Office more teeth.

Mr. Chairman, although you declined to become an original cosponsor of this legislation back in March, I hope that you and I can work together on this issue in a productive way. With that, I yield back.

[The prepared statement of Hon. Elijah E. Cummings follows:]

Opening Statement
Rep. Elijah E. Cummings, Ranking Member

Hearing on "Presidential Records in the New Millennium: Updating the Presidential Records Act and Other Federal Recordkeeping Statutes to Improve Electronic Records Preservation"

May 3, 2011

The Presidential Records Act and the Federal Records Act are landmark open government laws that are based on a fundamental principle—that federal agencies must retain records of their official business. These include records that have historical value, as well as records that are important for administrative, informational, and evidentiary reasons.

The electronic age has brought new opportunities for making government work more effectively and efficiently on behalf of American taxpayers. It has also brought new challenges for ensuring that federal records are maintained properly.

Previous administrations have experienced problems preserving electronic records, particularly emails. During the Clinton Administration, the email system experienced technical problems that resulted in lost emails. During the Bush Administration, the White House conceded that it lost hundreds of days of official emails, and top officials routinely used their Republican National Committee email accounts for official business.

To address these problems, the current system now automatically preserves all emails from White House email accounts. In addition, White House computers block access to private email accounts like gmail and hotmail. And finally, if White House employees receive emails relating to official business on their personal accounts, they are directed to preserve those emails either by forwarding them to their official accounts or by printing them.

As cutting-edge technologies continue to develop, they will create additional opportunities and challenges. Government officials can now communicate with each other—and with the American public—in new and creative ways through Facebook, Twitter, and other social media outlets. We want to encourage this kind of innovation. At the same time, we must ensure that records of official communications are preserved.

The Obama Administration has worked closely with the National Archives to develop new policies relating to social media. To begin with, it has limited access to these platforms to a

small fraction of White House employees. It has also worked with the National Archives to develop protocols to save official postings and samples of public comments in a manner that is consistent with its protocols for written correspondence.

As you know, Mr. Chairman, I always believe more can be done. So if the question for today's hearing is whether we can improve the Presidential Records Act and the Federal Records Act, the clear answer from this side of the dais is "yes."

On March 17, 2011, I introduced H.R. 1144, the Transparency and Openness in Government Act, a package of five bills that overwhelmingly passed the House last Congress with broad, bipartisan support, including your own, Mr. Chairman. Every Democratic member of this Committee joined me as an original co-sponsor of this bill.

H.R. 1144 includes the Electronic Message Preservation Act, which modernizes the Presidential Records Act and the Federal Records Act to ensure that White House and agency emails are preserved electronically. Right now, the law requires only that these records be saved. There is no requirement that they be saved electronically. This legislation had such bipartisan support last Congress that it passed the House by voice vote on March 17, 2010.

Since I introduced H.R. 1144 in March, a wide spectrum of open government groups has endorsed the bill. On April 18, 2011, a coalition of 17 organizations wrote to both of us seeking "bipartisan support and prompt action in the House." They also said this:

> H.R. 1144, "The Transparency and Openness in Government Act," will enhance the effectiveness of federal advisory panels, provide more access to presidential records, secure electronic messages generated by Administration officials, ensure donations to presidential libraries are part of the public record, and give the Government Accountability Office more teeth.

Mr. Chairman, although you declined to become an original cosponsor of this legislation back in March, I hope you and I can work together on this issue in a productive way. Yesterday, I wrote you a letter requesting that you schedule a business meeting to mark up H.R. 1144. Given the wide bipartisan support for this bill, I think we could get this bill out of our Committee and on to the floor by Memorial Day.

Let me conclude by asking that both my letter to you, and the letter from the 17 open government organizations, be made part of the official hearing record. I look forward to working with you to move this legislation forward.

Contact: Ashley Etienne, Communications Director, (202) 225-5051.

Chairman ISSA. I thank the Ranking Member.

We now go to our witnesses.

The Honorable David S. Ferriero. I thank you for your testimony today on behalf of the National Archives and Records Administration. Your work there is critical to our understanding of where reform is necessary.

Mr. Gary Stern, General Counsel to NARA, Office of Archivist.

And Mr. Brook Colangelo is the chief information officer of the Executive Office of the President. I appreciate your being here today. As you know, we also wanted the policy team, but I know that you come with probably the most critical information for today, so I am pleased to have you here.

Pursuant to the rules of the committee, could you all rise to take the oath and raise your right hands?

[Witnesses sworn.]

Chairman ISSA. Let the record reflect that all witnesses answered in the affirmative.

Mr. Ferriero, as you know, you have been here before, we do the green, the yellow, the red. The important thing is that all of your statements are on the record, and although you may go on script, to the extent that you can add to what is already going in the record, not simply repeat it, we would appreciate it. With that, you are recognized for 5 minutes. Thank you.

STATEMENTS OF DAVID S. FERRIERO, ARCHIVIST OF THE UNITED STATES, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, ACCOMPANIED BY GARY M. STERN, GENERAL COUNSEL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION; AND BROOK COLANGELO, CHIEF INFORMATION OFFICER, OFFICE OF ADMINISTRATION, EXECUTIVE OFFICE OF THE PRESIDENT

STATEMENT OF DAVID S. FERRIERO

Mr. FERRIERO. Thank you and good morning, Chairman Issa and Ranking Member Cummings. Thank you for calling the hearing and for your continued attention to the management and preservation of government records. As you mentioned, General Counsel Gary Stern accompanies me this morning and will be available to answer questions from the committee.

I am pleased to appear before you today to discuss the work that NARA does to implement the government recordkeeping laws, the Presidential Records Act [PRA], and the Federal Records Act [FRA]. The Archives have been responsible for setting government-wide policy on how all Federal agencies manage their records since the enactment of the FRA in 1950.

The FRA, however, does not apply to the President, the Vice President, and those members of their staffs that advise and assist them. Nor does it govern recordkeeping by Congress and the Supreme Court.

The Presidential Records Act of 1978 established public ownership of all Presidential and vice Presidential records, but it vested all records management and authority entirely and exclusively with the incumbent president and vice president. The legislative

history of the PRA states that the president is encouraged to implement sound records management practices.

Because the PRA presumes that all Presidential records must be permanently preserved and transferred to the National Archives at the end of the president's administration, the act allows for comparatively straightforward records management policy; that is, the White House saves all Presidential records, with the exception of some publicly received bulk mail correspondence, where a sampling is saved, and all Presidential records are transferred to NARA when the president leaves office.

In 1994, the Clinton administration established the policy of preserving all White House email records with an electronic record-keeping system. The George W. Bush administration continued this policy. While both administrations experienced some problems, as you mentioned, preserving their emails, which required restoration projects, the overall concept of capturing and preserving electronic Presidential records in their entirety became the accepted practice. NARA staff has successfully transferred the electronic Presidential records of these two administrations, along with all other records into the National Archives.

Throughout the course of an administration, both I and my staff provide guidance and advice on matters affecting White House records management when invited to do so. In this administration, NARA staff meet regularly with staff in the White House Office of Administration and other Executive Office of the President components on electronic records issues and provide guidance as requested. For example, we have provided advice on the preservation of Presidential record material generated by the White House and posted on social media Web sites and we have provided sampling methodology for archiving those types of records.

NARA has testified several times before this committee on the continuing challenges that Federal agencies across the government have in managing and preserving electronic records under FRA. The FRA requires each agency to follow NARA's guidance and implement a records management program. We have developed an extensive set of regulations and guidance on how agencies need to manage their records.

At the beginning of this administration, President Obama issued a Presidential Memorandum on Transparency and Open Government. NARA has subsequently emphasized that the backbone of a transparent and open government is good records management.

To put it simply, the government cannot be open or accountable if it does not preserve and cannot find its records. In February 2011, we issued our second annual Records Management Self-Assessment Report with respect to how agencies manage electronic records. The report noted that records management programs at many agencies are at risk.

In September 2010, NARA also produced a report on Federal Web 2.0 Use and Record Value that noted the Web landscape is evolving so rapidly that if we neglect to address these issues, we risk losing the truly valuable materials created by the Federal Government. In that report we made several recommendations, which are included in my written testimony.

One of the fundamental challenges that agencies have in managing electronic records under the FRA, and what distinguishes them from records governed by the PRA, is the need to separate permanent records from temporary records. Electronic records management systems generally require significant user input to file individual records, resulting in few agencies managing and preserving their email records electronically.

Rather, most agencies simply rely on print-to-paper as their official records management policy for email and many other electronically created records. While the FRA still provides a viable statutory framework for managing Federal records, we believe that there could be ways to modernize the FRA to improve the management of electronic records.

Before closing, I do want to raise one critical but often overlooked point. Ultimately, responsibility for records management will always rest, to some degree, with individual Federal employees, no matter what systems are in place. That was true in an era of exclusively paper records and it remains true in an increasingly digital age.

As the Archivist of the United States, I have made the management preservation and future access to electronic records my highest priorities. Indeed, as part of the transformation process that I have initiated within NARA, we have set up our own records management laboratory to develop and test best practices. I am committed to working with Congress, the White House, and Federal agencies to do all that we can to improve electronic records management and preservation.

Mr. Chairman, this concludes my testimony. Thank you for your attention and I am happy to answer any questions that you have.

[The prepared statement of Mr. Ferriero follows:]

TESTIMONY OF DAVID S. FERRIERO

ARCHIVIST OF THE UNITED STATES

BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

ON

"PRESIDENTIAL RECORDS IN THE NEW MILLENNIUM: UPDATING THE PRESIDENTIAL RECORDS ACT AND OTHER FEDERAL RECORDKEEPING STATUTES TO IMPROVE ELECTRONIC RECORDS PRESERVATION"

MAY 3, 2011

Good morning Chairman Issa, Ranking Member Cummings, and members of the Committee on Oversight and Government Reform. Thank you for calling 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 attention to the management and preservation of government records. Our General Counsel, Gary M. Stern, accompanies me this morning, and will be available to answer questions from the Committee.

I am pleased to appear before you today to discuss the work that the National Archives and Records Administration (NARA) does to implement the government recordkeeping laws, i.e., the Presidential Records Act (PRA) and the Federal Records Act (FRA). We appreciate your interest in improving the rules governing the collection,

storage, and preservation of and access to official electronic communications and other documents.

The National Archives has been responsible for setting government-wide policy and direction concerning how all federal agencies manage their records since the enactment of the Federal Records Act in 1950. The FRA, however, does not apply to the President, the Vice President, and those members of their staffs that advise and assist them. Nor does it govern recordkeeping by the House, Senate, Supreme Court, and Architect of the Capitol.

Until 1978, there was no statutory provision that required the President, the Vice President, and their staffs to manage or preserve their records. Those materials were treated as the personal property of the President and Vice President, much in the same way that records of individual Members of Congress and Supreme Court Justices are currently treated. The Presidential Records Act of 1978, 44 U.S.C. chapter 22, established public ownership of all presidential and vice presidential records, but it vested all records management authority entirely and exclusively with the incumbent President and Vice President. The legislative history of the PRA states that "the President is encouraged to implement sound records management practices." H. Rep. No. 95-1487, at 4 (1978).

Because the PRA presumes that all Presidential records must be permanently preserved and transferred to the National Archives at the end of the President's Administration, the Act allows for comparatively straightforward records management policies – i.e., the White House saves all Presidential records, with the exception of publicly received correspondence, as discussed below. In 1994, the Clinton

Administration established the policy of preserving all White House email records with an electronic recordkeeping system. The George W. Bush Administration continued this policy. While both Administrations experienced some problems preserving their emails and had undertaken restoration projects, the overall concept of capturing and preserving electronic Presidential records in their entirety became the accepted practice. NARA staff have successfully transferred the electronic Presidential records of these two Administrations into the National Archives, which have been preserved and are currently available for search and access by NARA staff. The Obama Administration is also capturing and preserving its electronic Presidential records.

The National Archives has no formal regulatory or oversight authority over how an incumbent President performs his records management responsibilities while in office, except that the President must obtain the Archivist's written views before destroying any presidential record. See 44 U.S.C. § 2203(c). Nevertheless, throughout the course of an Administration, both I and my staff endeavor to provide our best guidance and advice on matters affecting White House records management when invited to do so. In this Administration, NARA staff meet regularly with staff in the White House Office, Office of Administration, and other Executive Office of the President components on electronic records issues and provide advice as requested.

In accordance with section 2203(c) of the PRA, NARA worked with the George W. Bush Administration to apply the "bulk mail" disposal authority granted since the Reagan Administration for low level public mail received by the President and the Vice President to electronically received public correspondence. This practice includes maintaining a small electronic sample for permanent preservation and transfer to NARA.

During the Obama Administration, NARA has also provided advice for the preservation of Presidential record material generated by the White House and posted on social media websites. In addition, NARA has provided a sampling methodology for the posted record comments on White House pages on Facebook and other social media websites.

To the extent that the Committee would like to examine specific revisions to the PRA, we would have to consult with the White House and the Department of Justice before offering Administration views due to the sensitive constitutional and separation of powers issues that are associated with Congressional regulation of the Presidential recordkeeping. I can say, however, that the Archives would welcome the opportunity to engage in a constructive dialogue with the Committee and the Administration over potential revisions to the PRA.

NARA has testified several times before this Committee on the continuing challenges that federal agencies across the government have in managing and preserving electronic records under the FRA. The FRA requires each agency to follow NARA's guidance and implement a records management program. Based on the statutory framework of the FRA, 44 U.S.C. chapters 21, 29, 31, and 33, we have developed an extensive set of regulations and guidance on how agencies need to manage their records.

At the beginning of his Administration, President Obama issued a Presidential Memorandum on Transparency and Open Government. NARA has subsequently emphasized that the backbone of a transparent and open Government is good records management. To put it simply, the Government cannot be open or accountable if it does not preserve – and cannot find – its records. In February 2011, we issued our second annual Records Management Self-Assessment Report for 2010. With respect to how

agencies manage electronic records, the report noted that records management programs in many agencies:

- Do not ensure that e-mail records are preserved in a recordkeeping system;
- Do not monitor staff compliance with e-mail preservation policies on a regular basis;
- Have policies that instruct employees to print and file e-mail messages;
- Consider system backups a preservation strategy for electronic records, and do not distinguish between saving and preserving electronic records;
- Consider compliance monitoring to be the responsibility of IT staff; and
- Are rarely or not at all involved with, or are excluded from altogether, the design, development, and implementation of new electronic systems.

In September 2010, NARA also produced *A Report on Federal Web 2.0 Use and Record Value*, that noted "[t]he web landscape is evolving so rapidly that if we neglect to address these issues, we risk losing the truly valuable materials created by the Federal government. NARA and Federal agencies should be proactive in working together to understand these complexities and develop solutions." We made the following recommendations:

- Clarify how the Federal Records Act definition of a record applies to web 2.0 information.
- Mitigate public expectations of content longevity.
- Create a new General Records Schedule (GRS) item to provide dispositions for records created through clearly temporary uses of web 2.0 tools.
- Address transfer requirements for permanent web 2.0 records.
- Re-evaluate media neutrality as it applies to web records.

- Develop partnerships to identify best practices for capture and management of social media records.
- Integrate records management into agency social media policy.

One of the fundamental challenges that agencies have in managing electronic records under the FRA, and what distinguishes them from records governed by the PRA, is the need to separate records based on their retention and disposition requirements: i.e., permanent records from temporary, and long-term temporary records from short-term. Electronic records management systems generally require significant user input to file individual records, resulting in few agencies managing and preserving their email records electronically. Rather, most agencies still rely on print-to-paper as their official records management policy for email and many other electronically created records.

While the FRA still provides a viable statutory framework for managing federal records, we believe that, as a general matter, there could be ways to modernize the FRA to address more clearly the reality of managing electronic records. As Paul Wester, NARA's senior official responsible for government-wide records management, testified before this Committee last summer, we need to identify cost efficient ways to ensure that agencies manage electronic records electronically and transition away from printing and filing of e-mail and other electronic records. Without changing recordkeeping policies to reflect the current environment, while simultaneously also supporting the development and deployment of more robust electronic recordkeeping systems, the permanent record of our nation that is in electronic form will be compromised.

Given the special long-term preservation and access challenges associated with electronic records, NARA plans to identify how Federal agencies can be encouraged to

transfer preservation copies of permanently valuable electronic records to the National Archives as soon as possible, much earlier than the traditional 30 year time frame that the FRA sets out for paper records. Under existing authorities, agencies can retain permanently valuable records for more than thirty years or when no longer needed for agency business purposes. If NARA is not actively engaged with agencies to fully understand the electronic formats being used, then records may become at risk when they are eventually accessioned and the formats are no longer widely used. As part of its comprehensive review of records management practices, NARA plans to review options for mitigating this potential issue. Finally, NARA is exploring alternative ways to manage agency emails in what we hope will result in more user-friendly and cost effective approaches. We intend to begin piloting these approaches over the course of the next year.

Before closing, I do want to raise one critical but often overlooked point. Ultimately, responsibility for records management will always rest to some degree with individual federal employees, no matter what systems are in place. That was true in an era of exclusively paper records, and it remains true in an increasingly digital age. Although the development of automated email archiving systems like that used by the EOP enhance our ability to preserve key government records, updated records management policies and ongoing employee education and training remain key to sound records management practices.

I recognize the critical importance of finding solutions to the challenges faced with managing and preserving the ever increasing amounts of electronic records across the government and have made electronic records one of my main priorities as Archivist.

Indeed, as part of the transformation process that I have initiated within NARA, we are setting up our own records management laboratory to develop and test best practices, which we have already begun to do. I am committed to working with Congress, the White House, and federal agencies to do all that we can to improve electronic records management and preservation.

Mr. Chairman, this concludes my testimony. Thank you for your attention, and I am happy to answer any questions that may remain.

Chairman ISSA. Thank you, Mr. Ferriero.

Mr. Stern, I understand you don't have an opening statement. Do you have any comments at this time?

Mr. STERN. No. I will just defer until questions.

Chairman ISSA. Thank you.

Mr. Colangelo, you may proceed.

STATEMENT OF BROOK COLANGELO

Mr. COLANGELO. Good morning, Chairman Issa, Ranking Member Cummings, and distinguished members of this committee. Thank you for inviting me to participate in today's hearing on potential changes to the President Records Act and other records laws.

I am pleased to appear before you to discuss information technology systems in place for the Executive Office of the President and their impact on electronic records management. I have served as the chief information officer of the Office of Administration since January 2009. OA provides common administrative and support services to the components of the Executive Office of the President, including the White House Office, the National Security staff, and Office of Management and Budget. As CIO, I oversee all unclassified enterprise technology systems and services.

From the first days of the administration, it was clear that the EOP's IT systems were struggling to maintain stable and secure operations due to an aging IT infrastructure. Over 82 percent of our assets were end-of-life and no longer supported by their manufacturer. Enterprise software was severely out of date and had not been upgraded in years. The EOP had a single data center and no viable plan for a secondary disaster recovery. These flaws led to multiple email and network outages in the first 40 days of the administration.

We have devoted significant time and resources to modernizing the EOP IT systems in order to enhance stability, ensure security, and provide robust electronic records management. Among other initiatives, we have replaced network switches, overhauled our Internet connection, patched network gear, migrated to Exchange 2007, moved to BlackBerry Enterprise Server 5.0, increased and upgraded our storage area network, expanded our cybersecurity tools, and began to stand up a disaster recovery data center.

Amid these efforts, we have worked proactively to improve electronic records management while adapting to emerging technologies. Although past White Houses have struggled with email preservation, starting from the first day of this administration, email has been preserved through an automated archiving system that was procured by the Bush White House. We are now taking steps to upgrade or replace this system before it becomes outdated. We have also upgraded our email and BlackBerry servers to improve the reliability, and we are the first administration to begin archiving SMS text and pin-to-pin messages on EOP BlackBerry devices.

Although we have explored an enterprise solution for archiving records created on social networks, due to a lack of a suitable enterprise solution, EOP components currently use a combination of automated and manual methods to archive these records. Finally,

we have installed a new content management system on the White House Web site that archives every change to the site.

These initiatives have improved electronic records management on the EOP IT systems. Additionally, we have made it easier for staff to work on those systems. We have deployed secure mobile workstations, enabling staff to work on EOP systems while traveling or at home. Staff also have secure Web-based access to EOP desktop and applications, enabling them to work in a records managed environment from any computer.

We also restrict EOP network access to Web sites that could pose risks to records management or security. This includes sites like Gmail, Yahoo Mail, Facebook, Twitter, along with instant messaging sites like AOL Instant Messenger from the EOP network. A limited number of staff have access to approved social networking sites for official business, but cannot access Web mail sites like Gmail or Instant Messaging. Staff who receive access and are subject to the President Records Act receive supplemental briefing on their records management obligations. We also restrict the ability of EOP personnel to connect personal devices to the EOP network.

These proactive IT measures are reinforced by EOP policies. Employees are instructed to conduct all work on EOP systems, including electronic communications, except in emergency circumstances when they cannot access the EOP systems and must accomplish time-sensitive work. Staff receive guidance that the PRA applies to work-related electronic communications on personal accounts and are instructed to take appropriate steps to preserve any records on their personal accounts such as forwarding those communications to their EOP account or copying their EOP account on outgoing emails.

Through these proactive measures, we hope to improve the EOP electronic records management and address the challenges presented by emerging technologies. I hope this background information and my written testimony aids the committee's consideration of potential changes to the President Records Act and other Federal recordkeeping law.

Mr. Chairman, I would be pleased to answer any questions.

[The prepared statement of Mr. Colangelo follows:]

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.

Chairman ISSA. Thank you. I recognize myself for 5 minutes at this time.

Mr. Colangelo, are any of these carried into the White House?

Mr. COLANGELO. IPads, sir?

Chairman ISSA. Yes.

Mr. COLANGELO. We have not deployed iPads for enterprise use.

Chairman ISSA. Are any of these carried into the White House? Have you ever seen one of these into the White House?

Mr. COLANGELO. Yes.

Chairman ISSA. So people carry a product which circumvents your entire system by going to the AT&T network on a daily basis in the White House, isn't that true? Nothing stops someone from using this or other wi-fi connected not to any wi-fi in the White House, but to AT&T, Verizon, Sprint systems, and they communicate freely from the White House to Gmail or any other account, isn't that true?

Mr. COLANGELO. Mr. Chairman, we have strong policy, along with enterprise technology, that captures our records on the EOP network.

Chairman ISSA. I heard you. Answer my question, please. If I take an app product into the White House, as I did last night for dinner, I have full communication capability; you don't block any Verizon, Sprint, AT&T, or T-Mobile. The fact is that people every day bring their private property into the White House and can Gmail, Hotmail and the like from within the White House, correct?

Mr. COLANGELO. Individuals are not restricted on what they bring into the White House on personal devices on the person.

Chairman ISSA. So someone, if they chose to, could be emailing back and forth to the DNC from the White House, and you would not have the ability to capture that, is that correct?

Mr. COLANGELO. We provide training and policy to staff.

Chairman ISSA. Please. I am asking only the technical questions because you don't make policy. I ask for the policy person; I was denied that person. So let's stick to straightforward. I am not after the President, I am not after the administration; I am after the changes in technology and whether or not we are equipped to deal with them.

Today there are hundreds of products in the old Executive Office, in the Treasury Building, and in the White House proper being used to communicate, whether you like it or not, to private emails. They're simply connected, is that correct?

Mr. COLANGELO. That is correct, sir.

Chairman ISSA. OK. We are not making an issue out of it; that is the reality of the last decade of changes. And hopefully our work here is not about the current occupant of the White House, but about an act that has survived multiple presidents with ever-changing challenges.

Mr. Ferriero, if someone were to produce a book 5 years from now and they had their Gmail records, their Microsoft Word documents, all of which were produced on private computers using the Cloud while they were sitting inside the White House or working as covered persons for the Office of the President, would you believe you're entitled to that source material under the Presidential Records Act?

Mr. FERRIERO. If that content was work for that administration, then, yes, that's a Presidential record.

Chairman ISSA. And don't most kiss-and-tell books that come out after a president is gone usually, but not always after, don't they basically talk about meetings, experiences and so on, and ultimately aren't they most often from information that is either written, typed, or in some other way captured during the time they are either employees of the White House or physically in the White House. That is just the reality of what we see post-president.

Mr. FERRIERO. Exactly. In fact, some of the heaviest users of our Presidential libraries' collections are former members of the administration.

Chairman ISSA. They have to supplement what they took with them. How do you propose, in a digital age, that we deal with those correspondence that occur? Ultimately, the President is both the head of the Armed Forces, the head of the administration, and the head of his party. How do we appropriately capture that which we should capture, not capture that which we shouldn't, by statute rather than policy?

Mr. FERRIERO. Well, as I said, the way the law is written, the control, unlike the Federal Records Act, the control of that content rests with the President and the Vice President. So the position that we have is guidance, is to provide guidance, and Mr. Stern meets with his colleagues from the White House on a regular basis to provide that kind of guidance and to understand how technology is being used in the White House.

Chairman ISSA. Are all of you comfortable that a "I will decide which one of my Gmails fits that based on my training" is sufficient?

Mr. STERN. Well, it is our view that both statutes, even though they are old and were written in a time of principally paper records, are all-encompassing; they include language about included, but not limited to, all formats and all. So any official communications involving their work are presumptively Presidential records regardless of what system they are used on. It is also our clear understanding from this administration and prior administrations that the policy is you must use the government systems.

Chairman ISSA. Policy but not the statute. And as we already heard, they do use non-government systems; otherwise, there wouldn't be a policy that when you send and receive on your Gmail, you forward it into the official system. By definition, you can't have it both ways; you can't say the policy is that you only use official and then the policy is on those many, many, many, many occasions in which you don't use the official, please forward for the record. Clearly, the policy is not getting the job done completely.

Mr. STERN. And I guess the question is does that occur often, or our understanding is it can occur in emergency situations and the like, and whether it occurs on a regular basis, we are not aware of that.

Mr. FERRIERO. But let me answer your question.

Chairman ISSA. Please.

Mr. FERRIERO. Your question was are you comfortable. No, I am not. Any time there is human intervention, then I am not comfortable.

Chairman ISSA. Thank you.

Mr. Cummings.

Mr. CUMMINGS. Thank you very much.

We can agree that Federal employees should not use personal email to conduct official business, I think. Is that right, gentlemen?

Mr. FERRIERO. They can if they forward that communication to their official email.

Mr. CUMMINGS. OK. However, there are many times when using personal email might be necessary. For example, in the event of a natural disaster or a terrorist attack, communicating on official email may be impossible, would you agree?

Mr. FERRIERO. Agree.

Mr. CUMMINGS. Mr. Colangelo, in your testimony you describe several instances where the White House system experienced email outages, is that correct?

Mr. COLANGELO. That is correct.

Mr. CUMMINGS. Certainly, it should be made clear to employees that it is their responsibility to forward any records created on their personal email to their official email.

Mr. Colangelo and Mr. Ferriero, we don't want employees to just stop performing their duties in the White House or agency email system if it goes down, do we? We don't want that to happen if the agency system goes down, in other words, for them to stop doing business.

Mr. FERRIERO. Exactly.

Mr. CUMMINGS. So under that circumstance you want to make sure that they preserve whatever records they had.

Currently, the White House blocks access to personal email on White House computers. Employees are prohibited from even connecting personal electronic devices to the EOP network, is that correct?

Mr. COLANGELO. That is correct.

Mr. CUMMINGS. Yet, some still promote the false notion that White House employees are sitting around all day on their personal iPhones, accessing these personal email accounts to evade the Presidential Records Act and the Federal Records Act.

Mr. Colangelo, what more could be done? I suppose Federal agencies could ban employees from carrying personal cell phones at work. They could do that, couldn't they?

Mr. COLANGELO. That is more of a policy question, Congressman; I am a technologist.

Mr. CUMMINGS. And do we really want to create such an extreme big brother mentality like this?

Mr. Ferriero, what else could we do?

Mr. FERRIERO. The evolving guidance that we are working on in this particular administration is a good indication of how the system should work in a healthy environment. As I said, the control is with the White House and the quality of the product depends upon the relationship with the administration.

Mr. CUMMINGS. But you are not stopping the use of personal email. In other words, do you think it is a good idea to require all Federal employees to stop using any personal email as a condition of Federal employment?

Mr. FERRIERO. There are instances as you describe when that is the only solution, and, as far as I am concerned, that should be the guidance; you use your personal connections when you don't have access otherwise.

Mr. CUMMINGS. OK.

Mr. FERRIERO. And you ensure that record then gets transferred to your official email.

Mr. CUMMINGS. So obviouisly there are extreme and ridiculous proposals designed to make a point. At its most basic level, compliance with recordkeeping laws comes down to employees making decisions, is that right?

Mr. FERRIERO. That is the human element I was talking about.

Mr. CUMMINGS. Yes. And, Mr. Ferriero, isn't there inherently some level of discretion that must be allowed to ensure that employees can comply with the law while also doing their jobs, is that right?

Mr. FERRIERO. That is right.

Mr. CUMMINGS. Now, last year you applauded our legislation, the legislation that I spoke of about in my opening statement, did you not?

Mr. FERRIERO. I did.

Mr. CUMMINGS. And you supported it with great enthusiasm, did you not?

Mr. FERRIERO. I did.

Mr. CUMMINGS. And why is that?

Mr. FERRIERO. Because it points us in the right direction in terms of how we deal with our electronic records, and it also raises the consciousness of Congress about the importance of records, which is a real problem that I have inherited as Archivist of the United States.

Mr. CUMMINGS. So would you agree with me that would be a giant step in the right direction?

Mr. FERRIERO. It points us in the right direction, I agree.

Mr. CUMMINGS. And is there anything that you would like to see added to that legislation?

Mr. FERRIERO. One of the things that worries me most is the retention issue. The way the Federal Records Act is currently written, we are still in a 1950's paper mode, where many agencies have a 30-year retention policy for their records. Thirty years in an electronic environment is incredibly dangerous.

Mr. CUMMINGS. Mr. Chairman, I failed in my opening statement to ask that the letter that I mentioned with regard to what I sent to you a while back, in March, with regard to our legislation and the Transparency Act and then the letter I sent to you yesterday just be a part of the record. I ask unanimous consent.

Chairman ISSA. The first one, without objection, so ordered. The one yesterday was on this subject?

Mr. CUMMINGS. Yes, yes. Just asking for a markup.

Chairman ISSA. Oh, of course. Then without objection, so ordered.

[The information referred to follows:]

May 2, 2011

The Honorable Darrell E. Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am writing to request that you schedule as soon as possible a Committee business meeting to consider and vote on H.R. 1144, the Transparency and Openness in Government Act. As you know, H.R. 1144 is a package of five bills that overwhelmingly passed the House last Congress with broad, bipartisan support. I introduced H.R. 1144 on March 17, 2011, along with every Democratic member of the Committee. Although you declined to become an original cosponsor at that time, you supported all five underlying bills last Congress. Since the Committee has nothing scheduled this Thursday, I propose that we use this day to pass this legislation out of our Committee and send it to the floor.

Since I introduced this legislation in March, it has been endorsed by a wide array of open government organizations. On April 18, 2011, a coalition of 17 organizations sent a letter to you and me expressing their strong support for the bill. Their letter stated: "Our undersigned groups strongly support H.R. 1144, which we believe will make the government operate with more transparency and accountability."[1] The letter also said: "We hope we can work with you to ensure bipartisan support and prompt action in the House."[2]

Tomorrow, the Committee will hold a hearing on updating the Presidential Records Act and other federal recordkeeping statutes. H.R. 1144 directly addresses this critically important issue. Title IV of the bill is the Electronic Message Preservation Act, which would modernize the Presidential Records Act and the Federal Records Act to ensure that the White House and federal agencies preserve emails and other electronic messages. This legislation had such significant bipartisan support last Congress that it passed the House by voice vote during Sunshine Week on March 17, 2010. Representative Bilbray gave a strong statement in support of this bill during the floor debate. He stated:

---

[1] Letter from John W. Curtis, Ph.D. et al. to Chairman Darrell E. Issa and Ranking Member Elijah E. Cummings (Apr. 18, 2011).

[2] *Id.*

> Madam Speaker, this is a classic example of trying to work together to open up the system, allow the transparency that the American people are demanding, and I strongly support its intention and its execution.[3]

Mr. Bilbray emphasized the bipartisan cooperation that led to House passage of the bill last Congress. He stated:

> Madam Speaker, I would like to close by thanking the ranking member and full committee chairman for allowing the minority to participate in the formation of this bill. There are so many committees that aren't allowing the minority to participate. I think this is really a nice example of the cooperation that I think the American people want to see and don't see enough of. I want to thank the chairman and ranking member for allowing us to participate in the process.[4]

Additionally, the Archivist of the United States, David Ferriero, issued a statement in support of this legislation. He stated:

> The Government cannot be open and accountable if it does not preserve—and cannot find—its records. I applaud the leadership of Chairman Towns and Representatives Hodes, Issa, Clay, and McHenry on this important issue of managing and protecting the records of our Government.[5]

Title II of H.R. 1144 also would improve the Presidential Records Act by ensuring that presidential records are released in a timely manner. This title incorporates the Presidential Records Act Amendments, which passed the House last Congress by a vote of 359 to 58 on January 7, 2009. This legislation would establish a process for handling executive privilege claims by requiring the current president and former presidents to raise any objections to the release of records within 90 business days. The bill also would make clear that the right to claim executive privilege must be made personally by the current or a former president.

During consideration of the Presidential Records Act Amendments on the House floor last Congress, you made this statement strongly supporting the bill:

---

[3] U.S. House of Representatives, Debate on H.R. 1387 (Mar. 17, 2010).

[4] *Id.*

[5] National Archives and Records Administration, *National Archives Supports Goals of H.R. 1387 – The Electronic Message Preservation Act* (Mar. 17 2010) (online at www.archives.gov/press/press-releases/2010/nr10-74.html).

> I want to thank the chairman today because as we bring three votes from our committee, each of these was shared with the other in consultation, each of them was agreed were necessary and could be moved in a timely fashion today. Each of them will be presented to our conferences as noncontroversial, and in fact, ones that should pass unanimously or near unanimously. This is a great start.[6]

H.R. 1144 also includes several other provisions to improve the transparency of the executive branch. Title I of the bill would incorporate the Federal Advisory Committee Act Amendments, which would make federal advisory committees more transparent and accountable and close loopholes in the implementation of the Act. The Federal Advisory Committee Act Amendments passed the House last Congress by a vote of 250 to 124 on July 26, 2010. This bill received bipartisan support on the floor. For example, Representative Jo Bonner made this statement:

> H.R. 1320 provides strong protections against conflicts of interest and robust transparency into the workings of these committees. The bill also closes a loophole that many agencies were using to get around financial disclosure requirements and ethics requirements for members of those committees. I commend Mr. Clay, Chairman Towns, Ranking Member Issa, and other distinguished members of the committee for their hard work and desire to make the Federal Government more transparent and open and accountable to the American people.[7]

Title III of H.R. 1144 incorporates the Presidential Library Donation Reform Act. This bill would increase the transparency of presidential libraries by requiring organizations that raise funds to build those libraries to disclose information about their donors. This legislation passed the House last Congress by a vote of 388 to 31 on January 7, 2009. During debate on the House floor, you expressed your support for this legislation, stating:

> Madam Speaker, I join with the chairman in recommending swift passage through the House for at least the third time. This bill has passed under multiple authors, both Republican and Democrat. It is, by nature, one in which we believe we are appropriately asserting a daylight requirement on past and future Presidents and would certainly hope that we would view this bill as noncontroversial in most areas.[8]

Title V of H.R. 1144 is the Government Accountability Office Improvement Act. This bill would strengthen GAO's authority to access agency records and to pursue litigation if access is improperly denied. This bill passed the House last Congress by voice vote on January 13,

---

[6] U.S. House of Representatives, Debate on H.R. 35 (Jan. 7, 2009).

[7] U.S. House of Representatives, Debate on H.R. 1320 (July 26, 2010).

[8] U.S. House of Representatives, Debate on H.R. 36 (Jan. 7, 2009).

2010. During the House floor debate, Representative Luetkemeyer explained the importance of this legislation. He stated:

> Madam Speaker, Congress looks to the GAO to assist with the investigative and oversight functions vested in the legislative branch. This bill is intended to increase the effectiveness of GAO by ensuring that the agency is not unnecessarily restricted in its efforts to secure necessary information when performing these necessary and important functions. I urge my colleagues to support this legislation.[9]

H.R. 1144 is a strong open government bill, and its five component bills garnered wide bipartisan support in the last Congress. There is no reason we should not pass this legislation out of our Committee this week and on to the floor for consideration by the full House as soon as possible. Moving this legislation will send the message that this Committee is committed to working in a bipartisan manner to make the federal government more transparent and accountable.

Sincerely,

Elijah E. Cummings
Ranking Member

[9] U.S. House of Representatives, Debate on H.R. 2646 (Jan. 13, 2010).

H.R. 1144, TRANSPARENCY AND OPENNESS IN GOVERNMENT ACT
Rep. Elijah Cummings, Ranking Member
Committee on Oversight and Government Reform

H.R. 1144, the Transparency and Openness in Government Act, strengthens several core open government laws. The Act incorporates the text of five bills that previously passed the House of Representatives with broad, bipartisan support. Collectively, these reforms will enhance accountability and provide the public with greater access to government information.

Making Advisory Committees More Transparent and Accountable.
Title I makes federal commissions more transparent and accountable by strengthening the Federal Advisory Committee Act (FACA). These amendments to FACA ensure that committee members appointed to provide the President or an agency with expert advice comply with conflict of interest and other federal ethics laws. Title I also closes loopholes by clarifying that FACA applies to advisory subcommittees and that committees established by contractors are subject to FACA if formed at the request or direction of an agency or the President.
(Passed the House on July 26, 2010, by a vote of 250 to 124.)

Improving Public Access to Presidential Records.
Title II amends the Presidential Records Act to establish a process for handling executive privilege claims to ensure the timely release of presidential records. Under Title II, current and former presidents have up to 90 days to object to the release of records by the Archivist. Title II also makes clear that the right to assert executive privilege is personal to current and former presidents and cannot be bequeathed to assistants, relatives, or descendants.
(Passed the House on January 7, 2009, by a vote of 359 to 58).

Requiring Greater Disclosure of Donations to Presidential Libraries.
Title III requires organizations that raise funds for presidential libraries and their affiliated facilities to disclose information about their donors to Congress and the National Archives and Records Administration. The legislation further requires the Archives to make that information available to the public in a free, searchable, and downloadable database on the internet.
(Passed the House on January 7, 2009, by a vote of 388 to 31).

Modernizing and Strengthening Records Preservation Requirements.
Title IV modernizes the requirements of the Federal Records Act and Presidential Records Act to ensure that e-mails and other electronic messages are preserved. Title IV directs the Archivist to issue regulations requiring agencies to preserve electronic messages in an electronic format. These regulations must cover the capture, management, preservation, and electronic retrieval of electronic records. The Archivist is also directed to establish standards for the capture, management, and preservation of electronic messages that are presidential records.
(Passed the House on March 17, 2010, by voice vote).

Improving the Effectiveness of GAO.
Title V clarifies and strengthens the authority of the Government Accountability Office to access agency records and pursue litigation if access is improperly denied by a government agency. Title V increases GAO's effectiveness by ensuring that it is not unnecessarily restricted in efforts to secure information in the course of performing auditing and investigative functions for Congress.
(Passed the House on January 13, 2010, by voice vote.)

The Honorable Elijah Cummings
United States House of Representatives
2235 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Darrell Issa
United States House of Representatives
2347 Rayburn House Office Building
Washington, D.C. 20515

April 18, 2011

Dear Chairman Issa and Ranking Member Cummings,

Our undersigned groups strongly support HR 1144, which we believe will make the government operate with more transparency and accountability. H.R. 1144, "The Transparency and Openness in Government Act," will enhance the effectiveness of federal advisory panels, provide more access to presidential records, secure electronic messages generated by Administration officials, ensure donations to presidential libraries are part of the public record, and give the Government Accountability Office more teeth.

The reforms in H.R. 1144 are ripe for bipartisan action and support, since they are commonsense, noncontroversial measures, all of which passed the House of Representatives in the 111th Congress with substantial bipartisan support.

Title 1 of this bill, the Federal Advisory Committee Act Amendments Act, was approved by a bipartisan House vote of 250 to 124 in July 2010. It addresses weaknesses in the advisory committee process raised by the Government Accountability Office in 2004. The GAO thoroughly examined the FACA process and raised serious concerns about the ways agencies select and designate members, too frequently wrongly designating experts as representative stakeholders not subject to conflict of interest reviews. The GAO also recommended greater transparency for the member selection process such as "providing information on how the members of the committees are identified and screened, and indicating whether the committee members are providing independent or stakeholder advice."

This title will give the public more information about any conflicts of interest among advisory panel members and how the agency addresses them, make all meetings available on the agency's web site, and achieve a breakthrough for public participation allowing public comments for panel members and other openness.

Title II of this bill, Presidential Records Act Amendments, was sponsored in the 111th Congress by Rep. Edolphus Towns (D-NY), with Republican co-sponsors Reps. Issa (CA) and Dan Burton (IN). It passed the House by a vote of 359 to 58.

Past presidents have blocked the public release of presidential records and expanded the ability to use claims of executive privilege to do so. This title establishes a process for handling executive privilege claims over presidential records to ensure the timely release of these records. This title will ensure that requests by former presidents to redact certain presidential records are part of the public record, and that presidents may withhold a presidential record only if a former president has a constitutionally valid reason for doing so.

Title III, the Presidential Libraries Donation Reform Act, sponsored in the 111th Congress by Rep. Towns, with the bipartisan sponsorship of Reps. Issa and John Duncan (TN), passed the House in January 2009 by a vote of 388 to 31.

This title repairs a gaping hole in our campaign finance disclosure system. Gifts to presidential libraries can often total $1 million or more, and yet they are not required to be disclosed. This title would require quarterly reporting to Congress and the National Archives of donations to presidential libraries of $200 or more. This disclosure requirement would last up to four years after a president leaves office.

Title IV, Electronic Message Preservation, passed the House in March 2010 by voice vote. Emails and other electronic messages throughout the government are currently at risk. With little guidance for better methods, many agencies print them out to file—and some simply discard them. Title IV will ensure that all records that belong to the American people are preserved. The title requires the National Archivist to issue rules that address the capture, management, preservation, and retrieval of electronic records.

Title V, The Government Accountability Office Improvement Act, introduced in the 111th Congress by Rep. Towns, passed the House by a voice vote in January 2010.

The Government Accountability Office (GAO) is sometimes hamstrung in its efforts to audit or investigate agencies on behalf of Congress. Title V clarifies the authority of the Government Accountability Office (GAO) to access agency records, and enforce this authority in court, if necessary.

We hope we can work with you to ensure that this package of reforms receives bipartisan support and prompt action in the House.

Sincerely,

John W. Curtis, Ph.D.
Director of Research and Public Policy
American Association of University Professors

Christopher Finan
President
American Booksellers Foundation for Free Expression (ABFFE)

Anne L. Weismann
Chief Counsel
Citizens for Responsibility and Ethics in Washington

John Richard
Essential information

Mark Cohen
Executive Director
Government Accountability Project

J.H. Snider, Ph.D.
President
iSolon.org

Michael D. Ostrolenk
Co-Founder/National Director
Liberty Coalition

Rick E. Melberth, Ph.D.
Director of Regulatory Policy
OMB Watch

Patrice McDermott
Director
Openthegovernment.org

Danielle Brian
Executive Director
Project on Government Oversight

Progressive Librarians Guild

Jeff Ruch
Executive Director

Public Employees for Environmental Responsibility (PEER)

Lucy A. Dalglish
Executive Director
The Reporters Committee for Freedom of the Press

Helen R. Tibbo
SAA President, 2010 – 2011
Society of American Archivists

Hagit Limor
President
Society of Professional Journalists.

Francesca Grifo, Ph.D.
Senior Scientist and Program Director
Scientific Integrity Program
Union of Concerned Scientists

Toby Nixon
President
Washington Coalition for Open Government

Chairman ISSA. Mr. Ferriero, you said things are so dangerous, and I don't think the Ranking Member got to hear what was so dangerous about 30 years in an electronic age.

Mr. FERRIERO. As you know, because of changes in technology, 30 years to be retained in an agency is a very long time. Different information technology systems being used, different records management systems being used, great risk of loss of records in 30 years.

Chairman ISSA. In other words, we can't read DOS 3.3 so well today. OK, thank you.

The gentleman from Tennessee, Mr. DesJarlais.

Mr. DESJARLAIS. Thank you, Mr. Chairman.

We started in on this discussion just now on the 30-year problem in document preservation, and I think maybe we should explore that further. Mr. Stern, certainly feel free to jump in.

Does the NARA favor elimination of the current 30-year presumption?

Mr. FERRIERO. Yes.

Mr. STERN. And I would just add the 30-year issue is about when they transfer permanent records into the National Archives. For agencies only a tiny fraction of all the records they create are permanent for transfer into the Archives, and our concern is, on permanent records, we want to ensure we get them as early as possible so that we don't have a problem of format obsolescence.

Mr. DESJARLAIS. Often on Presidential recordkeeping is it common that on the second term they are more aggressive getting these archived? Is it your presumption that we should start earlier in a president's term?

Mr. STERN. The advantage of, in any Presidential term, even two terms, that is only 8 years at the longest, so that is relatively recent enough that we are able to get all the records in a reasonable good format. But we work with the new administration on day one and, from our perspective, we are planning a transition the first day the President is in office in terms of working and coordinating to ensure that all records, particularly electronic records, would be in the right shape and format so they can be transferred to us when the President leaves office.

Mr. DESJARLAIS. OK.

Mr. Ferriero, which and how many Federal agencies currently take advantage of pre-accessioning and turn over their documents before they are required to do so?

Mr. FERRIERO. Pre-accessioning?

Mr. DESJARLAIS. The early turnover of documents.

Mr. FERRIERO. Only about half a dozen.

Mr. DESJARLAIS. Half a dozen? And you would like to see that?

Mr. FERRIERO. Actually, as the Archivist, I would be really interested in getting in at the creation so that we have better control.

Mr. DESJARLAIS. What part of the Federal Records Act would have to be updated to eliminate the current 30-year presumption?

Mr. FERRIERO. I believe it is Section 2107, 2108 have language with respect to the agency retention up to 30 years.

Mr. DESJARLAIS. OK. Would the NARA prefer a default preservation rule that requires periodic turnover; quarterly, semiannually, annually, of agency electronic documents?

Mr. FERRIERO. We are exploring various models.

Mr. DESJARLAIS. Mr. Stern, would the NARA be able to handle a shift to periodic submission of agency electronic documents at current funding and personnel levels?

Mr. STERN. Yes, we think we will. In terms of the issues of pre-accessioning, we would just get copies for storage in its original format; the agencies would still have legal custody and be responsible for access, use, all of those issues until there is the formal legal transfer, which still could take place many years down the line. We just want to ensure we get a copy set that we can preserve in that original format.

Mr. DESJARLAIS. Mr. Ferriero, shifting gears a little bit, the Federal Records Act appears to split the responsibility for managing Federal records between the NARA and GSA. Is this by design or a remnant of the old GSA authorizing statute?

Mr. FERRIERO. This is a remnant.

Mr. DESJARLAIS. OK.

Mr. FERRIERO. In 1985 the agency separated from GSA and that still is in the law.

Mr. DESJARLAIS. Are there any practical functional problems as a result of the fact that the Federal Records Act talks of GSA as having a role in the Federal record management?

Mr. FERRIERO. Not really.

Mr. DESJARLAIS. OK.

Mr. FERRIERO. And they have never exercised any, at least in my experience they have never exercised any authority over records.

Mr. DESJARLAIS. And do you have any idea what GSA's perspective is regarding possible clarification of duties?

Mr. FERRIERO. I am sure they would be amenable.

Mr. DESJARLAIS. They would favor it?

Mr. FERRIERO. I would guess.

Mr. DESJARLAIS. All right.

Mr. Stern, what parts of the Federal Records Act would have to be updated to clarify NARA's exclusive custodial role?

Mr. STERN. I believe that is in Chapter 29 is where they talk about the responsibilities of the Archivist and the Administrator of GSA. So that would be a place to look to clarify that issue.

Mr. DESJARLAIS. And Mr. Colangelo, I wasn't meaning to ignore you; I was afraid I might mispronounce your name as well. But I am out of time and I will yield back, Mr. Chairman.

Chairman ISSA. You gave me back 12 seconds.

Mr. DESJARLAIS. Well, I hate to do that.

Chairman ISSA. That is all right. We will let it happen this one time.

The gentlelady from New York, Mrs. Maloney.

I am sorry, I got my paper just as I announced the wrong order. So now I have the right order starting with yourself.

Mrs. MALONEY. I thank the chairman for calling this meeting on this important topic.

A lot of what we are talking about today involves the preserving of Federal records, but preserving Federal records is really, in my opinion, not enough. I would say that it is equally as important to make these records available to the press and available to the general public.

Now, the American people have a right to know what their government is doing, what meetings are taking place, what they are working on, and one of the ways that they are able to figure this out is by having the press really report on the records on what the government is doing. I would like to point out that the Obama administration has taken many very important steps to open up government and to allow the public to see what is taking place. It is probably the most transparent government in the history of our country, and I would like to give one specific example and ask for your comment on this.

In December 2009, the White House began making all visitor access logs available on the White House Web site so the public knows who is wooing whom, who is going to the meetings; what are they working on; who has access. So I would like to ask Mr. Ferriero or Mr. Stern to comment on how important a step was this for the White House to make the visitor logs available to the general public, to the press to write about it. This is the first time in history this has been opened up to the American people. How important a step is this?

Mr. FERRIERO. I will start. I think it is incredibly important, but it also needs to be coupled with other heads of agencies releasing their calendars and their schedules also, and we haven't made as much progress there.

Mrs. MALONEY. Mr. Stern, do you have a comment?

Mr. STERN. Well, with respect to those records, those records are preserved as Presidential records and they are all transferred to the National Archives when the President leaves office, so we have White House entry records going all the way back, even before there was an electronic system, even before to entry records in the Roosevelt White House. So it is certainly our mission as the National Archives to open records as quickly as we can when they come to us, and we always encourage the rest of the government to be as open as they can too.

Mrs. MALONEY. But this is the first time it has been opened to the general public before it went to Archives or put on a Web site.

Mr. STERN. I believe on a systematic basis, that is my understanding, yes.

Mrs. MALONEY. I would also like to point out that this administration has probably been more effective than any other in the history of our country and has made use of the social media, such as Facebook, Twitter, YouTube, blogging, and these applications bring great innovation and allow people to have access to what our government is doing and what the activities are, but they also bring very special challenges for the archiving of this information because of the tremendous volume that is generated every single day.

So I would like to ask you, Mr. Ferriero, the National Archives has a blog, Facebook page, Twitter, and YouTube accounts. How do you preserve the records generated on this social media? How do you preserve it now?

Mr. FERRIERO. It is an exciting time to be the Archivist because of the rapid changes in technology and also because of, as you mention, the volume of content that is now being generated. We have developed guidelines for the agencies to consider their use of social media; it is on our Web site and we have raised a series of ques-

tions with them to analyze the content of their postings on social media to make decisions about whether they are records or not. If they are records, then they need to be captured just as under the guidance of the Federal Records Act, and we have provided guidance on the capture of that content also.

Mrs. MALONEY. Would you say the benefits of using social media and these various tools to communicate with the general public outweigh the challenges posed to archiving it?

Mr. FERRIERO. Yes, definitely. This administration is committed to involving the American public in the workings of government in a way that it has never been involved before, and this is the way it is happening.

Mrs. MALONEY. I would like to close, since both of you have mentioned the importance of having the agencies involved and that the performance of the agencies in managing electronic records are equally as important, and I would just like to point out that we have a bill before Congress, the Message Preservation Act, that calls upon the agencies to electronically save this information and to save their emails electronically, and I urge my colleagues on both sides of the aisle to join me and many others in pushing for the passage of this bill.

Thank you very much. My time has expired.

Mr. DESJARLAIS [presiding]. The gentleman from North Carolina is recognized for 5 minutes.

Mr. MCHENRY. Thank you, Mr. Chairman.

Dr. Ferriero, thank you for being here. I certainly appreciate your leadership and your time, and certainly I appreciated it with Chairman Clay last Congress, having oversight in our subcommittee of NARA, and appreciate the hard work that you do. Also appreciate the fact that you have a North Carolina connection.

I wanted to ask you about the print-to-paper policy. Could you discuss the drawbacks to this idea that rather than keeping a digital record, which seems more efficient, easier to search, easier to maintain, I would guess it would be easier to maintain, compared to this idea that you simply print something off and put in a file?

Mr. FERRIERO. I already have 10 billion pieces of paper; I don't need any more paper. It is embarrassing that in the year 2011 our guidance is print and save. We should be capturing this electronically. I have 44 facilities around the country. The storage costs for paper are enormous.

Mr. MCHENRY. In what ways can we improve this?

Mr. FERRIERO. The guidance in the EMPA is to acknowledge, as we have in the Presidential Records Act, acknowledge electronic communication as record. That will help.

Mr. MCHENRY. What part of the Federal Records Act would have to be updated in order to insist that we have electronic records?

Mr. STERN. You would have to look at the specific provisions, but we are familiar with the legislation, the EMPA, and that would amend I believe it is through Chapter 29, and there may be other provisions that warrant looking at in terms of mandating electronic preservation of at least electronic messages, as that statute does, and our view is that we support the goals of that effort.

Mr. MCHENRY. Now, Dr. Ferriero, we have discussed this before in a larger, broader context. You inherited a lot of difficulties come

in as Archivist, and I have asked you this at every hearing that you have been before the committee, so you probably know where I am going with this, but in terms of how employees rank their happiness with their job and fulfillment with their job, NARA has had some challenges.

You discussed 44 facilities. It is a pretty large institution you are running. But in comparison to other Federal employees' work satisfaction hasn't been the highest at NARA and that has led, in my opinion, to some data losses based off of people not getting full fulfillment out of their job, haven't taken the pride in preserving some of these documents. Now, I know you have a very credible staff, you have great folks that work at NARA, but what have you done to improve this in the year and a half now, 18 months you have been on the job?

Mr. FERRIERO. You are right, we are tied for last place in the Employee Viewpoint Survey, tied with HUD, and it is not where I want us to be. We have, in the past 8 months, gone through a major reorganization, transformation of the agency, created basically a new organization, driving out repetitive kinds of operations and streamlining and making it more efficient, but most importantly putting our user community in the center of what we are doing and engaging the staff in this process. And the engagement of the staff through social media internally has really had an impact on how people feel about being part of one large agency.

I visited now 32 of our 44 facilities, so I have had an opportunity to meet firsthand with the staff to talk to them. First question: What is it like to work here? Tell me the stories. With and without supervisors. So I have gotten a really good picture of what works and what doesn't work, and we are serious about turning that around to make it the best agency in the government.

Mr. MCHENRY. Very good. Very good. Thank you for your testimony today and thank you all for your service to our government.

Mr. DESJARLAIS. The Chair now recognizes the gentleman from Missouri, Mr. Clay, for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman.

Archivist Ferriero, it is very good to see you again. I would like to take a moment to say that you are doing an outstanding job leading the National Archives. Your reorganization, your transformation of the agency will, I believe, result in vastly improved services to all the stakeholders and customers that you serve. This is especially true regarding open government and electronic records management.

I would like to ask you about regulations. As you know, the House, last year, passed the Electronic Message Preservation Act [EMPA]. Under this legislation, you would be required to issue regulations to agencies and the White House on the preservation of electronic messages. This Congress, Ranking Member Cummings has introduced H.R. 1144, the Transparency and Openness in Government Act, which includes the language of EMPA. H.R. 1144 also includes the Presidential Records Act amendments, which overwhelmingly passed the House the last Congress.

Archivist Ferriero, would these improvements, along with the existing statutes, provide you with the tools that you need in order to help agencies comply with Federal recordkeeping statutes and

can you elaborate on how exactly these improvements would be helpful.

Mr. FERRIERO. We are very supportive of the direction of H.R. 1144. As I said, and I don't want to keep repeating myself, my biggest concern is about retention, how long electronic records are retained in the agencies. If we can deal with that, I will be happy.

Mr. CLAY. Thank you. So you agree that we need to get rid of the paper.

Mr. FERRIERO. I agree. I love paper, but——

Mr. CLAY. You have driven that point home this morning about paper; it does become cumbersome and there are ways to transfer that data over to electronic means in this day and age.

Let me ask Mr. Colangelo what is the current state of the White House email archiving system, is it up to task?

Mr. COLANGELO. Congressman, yes, the email archiving is fully operational and is ingesting all email, to the best of my knowledge.

Mr. CLAY. This is more of a comment than a question, but during the previous administration this committee discovered something very disturbing. This was after we learned that the previous White House was unable to properly manage the emails in their system and many were lost. On top of that, dozens of senior White House officials conducted official business using their Republican National Committee email accounts instead of their official government accounts. Countless records, perhaps millions, that should have been preserved under Federal statute were lost.

Mr. Colangelo, do we have to worry about those same problems in this White House?

Mr. COLANGELO. Congressman, what we have done since 2009 is worked with the technology that the Bush administration procured, which is a commercial off-the-shelf product, a proven technology to archive records. So the EOP email systems are being archived. Additionally to that, we have also stabilized our systems and enhanced mobility so that we offer users many choices to access the EOP system when they need to do their EOP work either from a laptop or a secure Web-based system, so that they have the opportunity to do EOP work anytime.

Mr. CLAY. Thank you for your response and all of the witnesses' responses.

Mr. Chairman, I yield back.

Mr. DESJARLAIS. The Chair thanks the gentleman.

The Chair will now recognize the gentlelady from New York, Ms. Buerkle, for 5 minutes.

Ms. BUERKLE. Thank you, Mr. Chairman, and thank you to our panelists for being here this morning.

My question has to do with the split between the responsibility for managing Federal records with regards to NARA and GSA. If you could, what we are looking at right now appears to split the responsibility. Is that by design or is that something that was it just so happened that way?

Mr. STERN. Yes, the National Archives used to be part of GSA, and in 1985 we were split and became an independent agency from GSA, but when they revised the statute at that time, they left some responsibilities for economy and efficiency and such with GSA in coordination with the Archivist of the United States. Our experi-

ence in the last 25-plus years is that GSA has really lost interest and hasn't played any functional role in dealing with management and preservation of records, so I think it is not unreasonable to consider whether they need to have a role in the statute. And as the Archivist testified earlier this morning, we don't think GSA will likely have any resistance either.

Ms. BUERKLE. I apologize, I have been advised that this has already been covered before I got here, so I apologize for that.

Let's go to the whole email question and the preservation of those. Do you have, Mr. Ferriero, any recommendations regarding potential additional rules for ensuring that the transfer of the Presidential administration electronic documents will be finished within a 60-day timeframe? How can we make sure that happens?

Mr. FERRIERO. I am not sure the 60 days, where that comes from. The transfer actually happens at the end of the administration, so everything is retained in the White House until the administration changes. In fact, during the inauguration ceremony Archive staff is in the White House.

Chairman ISSA [presiding]. Would the gentlelady yield?

Ms. BUERKLE. Sure.

Chairman ISSA. To the gentlelady's question, would you prefer that there be transfers during the administration so that, in fact, if there are any questions, you find out about them while they are still using the same software and the same personnel are still there?

Mr. FERRIERO. That is a good question. As I said, we have these regular meetings with our colleagues in the White House about how they are managing their records. I hadn't really thought about capturing them sooner. It is certainly an attitude I have on the other side, on the Federal records scenario.

Ms. BUERKLE. I believe that this issue is raised because, in the instance where, obviously with President Clinton and President Bush, those were two terms, but in the event that there was a single term president, the turnaround within the 60 days, I think that is where that question came from.

Mr. FERRIERO. I see.

Ms. BUERKLE. Thank you. I yield back.

Chairman ISSA. Would the gentlelady further yield?

Ms. BUERKLE. Sure.

Chairman ISSA. Mr. Ferriero, you earlier talked in terms of what could be captured, what couldn't be captured. Obviously, the Ranking Member and I have an agreement that in times of an emergency in which the system is down, you come as you are, bring what you have, and do what you must.

But assuming that there are covered persons, and we would have to define covered persons not to be just anybody, but covered persons that have personal emails and personal Facebooks, do you believe the statute should give an absolute right for those covered persons' documents, if you will, to be reviewed by a third party to ensure that there is compliance with the law?

I am not talking about, you know, if you will, preempting people's personal rights, but if you are a covered person and you have access and you may or may not have used it, is that discretion

something you would like see reviewable at least by the Office of the Presidency itself?

Mr. FERRIERO. Certainly by the Office of the Presidency, yes. And I could, after more thought, extend that. My concern, as I have said, has to do with any time there is the human element involved, when someone has to make a decision and remember to transfer those to their official email system. The beauty of the White House email system now is it automatically captures it.

Chairman ISSA. It is 100 percent even if it is just you emailing your wife to say you will be late, like so many people do at the White House everyday.

Mr. COLANGELO. Correct. It preserves all inbound and outbound communication.

Chairman ISSA. So I guess my followup, Mr. Colangelo, is since you capture 100 percent of all communication on the Exchange system at the White House, and since that includes private conversations that do occur, I mean, people do email home ET, I am phoning home, I won't be home at any reasonable time tonight, they just killed bin Laden, if that happens, you capture it, it is there.

Thirty years from now people will be able to see what somebody said that evening to their family on why they weren't going to be home until after midnight. Shouldn't we, in reverse, also have that ability to collect data from covered persons the other direction in some organized way, in your opinion?

Mr. COLANGELO. From a technology standpoint, Mr. Chairman, I am not necessarily sure how we would collect data from personal accounts.

Chairman ISSA. The time has expired. I yield back.

At this time we recognize the gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman. And, Mr. Chairman, I would ask, without objection, my opening statement be entered into the record.

Chairman ISSA. Without objection, so ordered.

[The prepared statement of Hon. Gerald E. Connolly follows:]

Opening Statement of Congressman Gerald E. Connolly

Presidential Records in the New Millennium

Oversight and Government Reform Committee

May 2, 2011

An examination of Presidential record archiving demonstrates how much more transparent the federal government has become over the last century. Our challenge is to update federal record keeping standards without creating so much red tape that it ties up resources which would otherwise be used serving the public.

Prior to the Franklin Delano Roosevelt Administration, there was no standard procedure to preserve Presidential records. President Roosevelt pioneered the concept of a Presidential library to preserve records from his administration, a tradition that has endured through subsequent administrations. These libraries have created tremendous archival value and served as storehouses of primary sources for popularly accessible historical work such as Robert Caro's magnificent biographies of Lyndon Johnson. In 1974, Congress strengthened Presidential record keeping requirements with passage of the Presidential Recordings and Materials Preservation Act. More recently, in each of the two previous Congressional sessions the House passed legislation to update record keeping requirements to include electronic communication. In this session, Ranking Member Cummings introduced the Transparency and Openness in Government Act, which would improve electronic and other record keeping.

The Transparency and Openness in Government Act, of which I am a cosponsor, would make several important updates to record keeping policy. First, it would maintain records of electronic communication from the executive branch. These records would be managed in a way that would make them accessible for researchers using electronic search functions. Mr. Cummings' legislation also would establish standards for releasing Presidential records to the public expeditiously and would create a transparent process to manage claims of executive privilege. These reforms make sense in the digital age and I would hope this Committee can mark up Mr. Cummings' Transparency and Openness in Government Act.

I hope that we also will consider how to streamline record collection and storage. We must minimize the time agencies and the executive branch spends collecting and maintaining these files because they have other important work to do. Every minute that the Department of Homeland Security would spend collecting electronic records is one less minute it would spend tracking down child predators and other criminals. We must recognize that there is a balance between absolute transparency and agency functionality.

Mr. CONNOLLY. I thank the Chair.

Mr. Ferriero, NARA's 2010 Records Management Self-Assessment Report identifies several difficulties in managing electronic records: technological complications and preservation, proper disposition, the volume, propriety in cutting-edge technologies to create records, and decentralized environment in which they reside. What mechanisms are currently in place to encourage collaboration between records management and IT professionals as needed?

Mr. FERRIERO. That is a terrific question. I have been the Archivist for 18 months and——

Mr. CONNOLLY. Did you hear that, Mr. Chairman? It was a terrific question.

Mr. FERRIERO [continuing]. And one of the first partnerships I created was with the CIO. The CIO sits at the head of the CIO council. We have a records management council also, and I discovered that the records managers and the information officers have never worked together, talked, met together. So the situation is that we have the IT folks off developing systems, all of which have records implications, not talking to their records managers. So we convened the first-ever joint meeting of the two to start this relationship of records managers being at the table with their CIOs as new systems are being developed.

The situation is even more complicated for me because, in the wonderful world of the Federal job family, there is no such thing as a records manager. So we are working now with OPM to create a family of jobs around information management that will address the problem. So the result is in many agencies and subagencies the assignment for records management falls to the most junior person in the agency; not a full-time job, high turnover, not very well trained, and we get what we get from that situation.

Mr. CONNOLLY. A recent report by the American Council for Technology Industry on government best practices for social media recordkeeping identified the need to develop communications between social media team and records management as best practice No. 1. The report also said until best practices and tools emerge to assist in the records management of social media records, agencies were tending toward retaining all social media content so that those portions of the records are protected.

Given the overwhelming volume of data this could encompass, I would be interested in your thoughts about what is the best practice going forward? What are the challenges of the save everything approach to management?

Mr. FERRIERO. The issue that I described about the CIOs and records managers is similar to records managers and Web managers. So we have recently brought together the Federal Web managers and the records managers to talk about this very issue of what needs to be captured and how it needs to be captured. I referred earlier to some guidance that NARA has provided for helping those folks responsible for the social media to ask a series of questions about the content to determine whether it is record or not record.

Mr. CONNOLLY. You make reference to NARA and I think there was some indication that these best practices would be put on the Web site. Any idea of time line for that?

Mr. FERRIERO. The guidance is up, the report is up. In terms of best practices, that is coming. When?

Mr. CONNOLLY. What is that?

Mr. FERRIERO. Within a year.

Mr. CONNOLLY. Without a year. Hopefully sooner.

Mr. FERRIERO. Yes, I agree.

Mr. CONNOLLY. My time is almost running out but, Mr. Colangelo, is it really reasonable to expect employees in the White House not to, from time to time, have to use Gmail or to use their iPads to communicate with spouses, friends, family, whatever? I mean, that is not something that is normally enforced in the normal workplace.

Mr. COLANGELO. That is correct. That communication also takes the stress off of our system, so it reduces the work system as only for work systems, and it keeps the clear separation between personal and government issue equipment.

Mr. CONNOLLY. So people are allowed to use their work computers for Gmail?

Mr. COLANGELO. No. I am sorry. On their government equipment they are not allowed to access social media or Web-based email sites, it is blocked from a technical standpoint on our network.

Mr. CONNOLLY. So it is a much stricter standard than exists in most workplaces.

Mr. COLANGELO. That is correct.

Mr. CONNOLLY. I thank you.

My time is up, Mr. Chairman.

Chairman ISSA. Thank you.

The gentleman from Oklahoma is recognized, Mr. Lankford.

Mr. LANKFORD. I would like to yield back my time to the chairman at this point.

Chairman ISSA. Oh, OK. Well, I will take the time for a few minutes. I thank the gentleman.

Mr. Ferriero, you oversee, from a FOIA standpoint, a tremendous amount of information, even though you work with the libraries where many of the assets reside. Ultimately, a Freedom of Information Act request on any president covered under your records, your many archives, belongs to you, isn't that correct?

Mr. FERRIERO. That is right.

Chairman ISSA. How many people do you have, roughly, doing FOIA within your jurisdiction? Directly and indirectly, because obviously librarians at the various libraries assist.

Mr. STERN. We do submit a report to the Department of Justice that has that number. I am afraid I don't remember specifically.

Chairman ISSA. It is in the many hundreds, though.

Mr. STERN. Yes. At the Presidential libraries where FOIA applies, which is Reagan forward, there is probably about roughly 50 archivists doing FOIA review and processing, and then there is at least that number dealing with Federal archival records here in Washington and in our regional archives.

Chairman ISSA. But if I can followup, the desire to FOIA 30-year-old material generally from the government is pretty minimal, right? In other words, agencies control for 30 years their documents; you control them when they are too old for anyone to ask.

Mr. STERN. Well, the original model of the archives was you wanted the records to get to an age where they are no longer needed by the agency and where the restrictions pretty much are lifted. So in the old model, after 30 years, when they transferred records to us, we could presume that the records were virtually open in their entirety, unless there was classified information or personal privacy information. So the ideal is, when they come to us, we can just make them open; you wouldn't need to make a FOIA request because you could just come to the research room and we could provide them.

Chairman ISSA. Following up on that, because this really is a major reform committee on both pieces of legislation question. Today, if President Obama were to decide not to run for a second term, which I understand he has already made that decision, you are only 2 years away from receiving 4 years of information.

So you have this variable that goes from 4 years to 8 years; presumably it will be 8 years for this administration like it was for the previous two. But when I look at the Department of Homeland Security, you have decades before, under completely different cabinet officers, those records are going to be available.

In a sense, in your opinion, and, Mr. Ferriero, I think I will bring this one to you, in a sense, doesn't an administration's sunset and an even hand of a nonpartisan entity become the more logical custodian at the end of an administration of, for example, Department of Homeland Security from the Bush administration? Right now Secretary Napolitano hires 400 people to decide whether or not Bush era records are publicly available or not.

Does that seem like an area of modernization that we should hold hearings on and decide whether or not to take the entire presidency as a period of time in order to refresh broadly? And that is why I asked about your own history, because you are making FOIA decisions on President W. Bush today, while in fact you are not making decisions on any of his people and his administration. Instead, the succeeding administration of the opposite party is making those decisions. Complex question. What would you say?

Mr. FERRIERO. But it is an interesting thought.

Mr. STERN. Well, I would just add, under the Presidential Records Act, when we receive the records from an administration, there is a 5-year period where there is no public access. So, in fact, right now there is still no access under FOIA——

Chairman ISSA. Without joint consent.

Mr. STERN. Well——

Chairman ISSA. An administration can choose to release. There have been releases after an administration has gone sunset, but they have been in concert.

Mr. STERN. Before the 5-years, a very tiny amount. So generally it is not until 5 years after the administration leaves office that we start opening records to FOIA requests on a systematic basis.

Chairman ISSA. But that is still 15-plus years sooner than you will the cabinet officers' records.

Mr. STERN. So the notion that if we were to get more records earlier and have to process them, I think it would have to be accompanied by rather massive addition of staff and resources to deal with the processing element of it, and part of the old model is they

are the agencies' records, the agencies can decide on the restrictions and on access, and they have greater resources than we would have if we take in massive amounts of agency records in addition to Presidential records.

Chairman ISSA. Well, even my borrowed time is now expiring, but I would let you know what I am thinking, and the Ranking Member. It has become my at least straw person belief that in fact FOIA should broadly not belong to the administration; that it should be handed off in its greatest portion to individuals who report to someone who wants public information public, private information private, and who is apolitical.

That general belief doesn't change the fact that the Department of Defense, what is going on today, must be determined by the Department of Defense and its current cabinet officer. But the sooner that transfer were to occur, the more likely the public would have a fair right to know not in any way determine either by the vindictiveness of the next administration or the graciousness of covering up by the next administration, both of which, quite frankly, the record shows there has been a certain amount of that has gone on under both parties.

I recognize the Ranking Member for his second round.

Mr. CUMMINGS. I was just listening to the chairman's proposal. One of you said that everything seems to boil down to discretion, even a proposal like that, determining which records are supposed to be released under FOIA.

But let me go back to you, Mr. Ferriero. You, in answering one of the chairman's questions, he was talking about those personal emails where somebody says I have to stay late because something has gone on in the White House, just a little note to their wife or husband, whatever. You are not trying to preserve those kind of records, are you?

Mr. FERRIERO. They are. They are captured.

Mr. CUMMINGS. But that is not the kind of stuff that you really are that interested in.

Mr. FERRIERO. Well, it is interesting because I learned a lot when we were working on the Elena Kagan confirmation hearing and we had to deliver a lot of content from the Clinton White House, 65,000 email messages that Elena Kagan had some role in, and very often those messages were a combination of personal and business, and it is hard to separate out, unless you are going message by message and determining what is personal and what is not personal. So the procedure, policy in the White House now of capturing everything works for me.

Mr. CUMMINGS. Mr. Colangelo, in the beginning of your testimony you talked about how you had to come in and equipment apparently was outdated and there were some problems. We needed to just bring, I guess, our software up so that it could do the job we needed it to do. And I am wondering where are we now with that and how do you make sure—I was just telling the chairman a few minutes ago that he and I came along a while back, and we can still remember when people were using carbon paper and typewriters, and now all technology changes, seems like, every 5 or 6 days, if not every day.

So how do you keep up with that? How do you make sure you stay on the cutting edge and at the same time make sure that it is a balanced approach so you are not just getting equipment that is going to be outdated tomorrow? And I ask that so I am just trying to figure out the efficiency and effectiveness of maintaining these records. Do you follow me? Believe it or not, I have some 8-tracks in my basement and nothing to play them on. So I am just wondering.

Mr. COLANGELO. Thank you, Mr. Cummings. Congressman, what we did in the beginning of the administration was really invest in stabilizing our core. We averaged somewhere in the 70 percent uptime in the first 40 days of the administration; now we are over 99 percent operational uptime. We had to replace a lot of key systems because they were in need of upgrade.

How we do this now, going forward, is we have a continual investment in our infrastructure so that it is not an uphill battle, it is a constant level flow, that we are constantly upgrading new systems, as I mentioned in my testimony, where we are looking at upgrading our archiving system before it becomes out of date. So let's beat that before it gets to that end-of-life state.

And now we constantly look at new technology before integrating it into the EOP enterprise to ensure that it does follow the compliance and records management and helps meet the business need. So it is constantly meeting that business need and also making sure that we are compliant with that.

Mr. CUMMINGS. Finally, Mr. Chairman, I would just again ask that we schedule a date as soon as possible for the marking up of 1144. Mr. Ferriero, I think, has agreed that this is a giant step in the right direction. It is really noncontroversial and I think it is something that we all could be proud of and could in a bipartisan way. Again I ask that and, with that, I yield back.

Chairman ISSA. I thank the gentleman.

I will just do a very short second round myself.

Mr. Ferriero, the challenge you face would appear to be that each administration delivers you records in a certain way. The Clinton administration, as I understand it, delivered you Lotus Notes as a system.

Famously, from this committee's standpoint, the next president tried to take Lotus Notes and transfer it to Microsoft Office Suite, including Exchange, and then discovered, among other things, that they are image backups and were not capturing. So we have seen these transitions.

What is it we can do for you broadly, as the Archivist, either through mandating that the systems that are delivered to you be in an open format or an interoperable format or in some format that at least allows you to port them in the future that would help you? As we look at updating these things, there is sort of the question of paper was understood. You could specify 8½ by 14 bond paper with 10 courier. But those days are gone. And if I had DOS 3.3 WordPerfect followed by we won't even go through SuperCalc and all the other programs that are long forgotten, they would deliver me an amazing nightmare. You have that, don't you?

Mr. FERRIERO. I do have that nightmare, and it makes paper look very good today. The electronic records archive that we are

creating, in fact, is designed to accommodate those changes in technology as well as changes in attachment. It has neutralized formats basically to make it possible for us to migrate the digits through time so that they are available in perpetuity.

On the other hand, being much more involved at the creation point, as I talked about earlier, is important to us so that we can establish standards around email creation and electronic record creation and capture.

Chairman ISSA. So, in closing, if, in our modernization legislation, we mandated that all agencies give you sufficient comfort with their preservation on an annual basis so that either the material could be transferred or changes could be made so that the next year you are not getting 2 years of information that is going to be very expensive to change, that would be helpful. Second, if in fact we design for transfer at the front-end, then you could save and the American people could save a huge amount of money, isn't that correct?

Mr. FERRIERO. I agree.

Chairman ISSA. Well, that will be among other things in our legislation.

I will close. Mr. Colangelo, you talked about the good and the bad of the Bush administration. Is there a way that we could ensure that the funding and the capability of each administration were more best practices as a matter of course, or is it simply that President Bush did a great job of capturing email archives and creating the Naz and the Volt and so on, while toward the end refreshing servers was not a priority and you inherited them over 3 years old? Those kinds of good and bad, should we have a role or are you satisfied that each administration does the best they can and hands off?

Mr. COLANGELO. From a technology standpoint, I think it is important to invest in infrastructure so that there is a continual flat line there versus the up and down.

Chairman ISSA. OK.

I might note, by the way, that the White House has almost always been at least one generation of the Exchange system ahead of the House.

With that, I thank all of you.

Oh, I apologize. Now I would recognize Mr. Lankford for a second round.

Mr. LANKFORD. Thank you very much, Mr. Chairman.

Mr. Colangelo, I just had a couple questions for you. Reading through your notes, and I apologize for slipping in a little bit late here. Tell me a little bit about the Facebook tracking and Twitter. I know certain sites or certain locations have that, have access; others are blocked from that. How is that being tracked? I see some conflict in how we are able to handle that with the technology.

Mr. COLANGELO. Thank you, Congressman. So, from a technology standpoint, we have an enterprise-wide gateway that blocks all staff from accessing these, and then when a component staff member makes a request for this, it is reviewed by their counsel and then if it is appropriate for the business use, they are allowed access through a certain policy and they have access to an approved number of sites.

We have looked for an enterprise-wide preservation system. Technology hasn't matured enough currently, but we are continuing to look and hoping that it will come around. What happens now is records are preserved by a component-by-component basis. And I know today actually the White House released a blog post on WhiteHouse.gov describing their process for capturing records on some of these sites.

So, for example, on Twitter they use an RSS, Real Simple Syndication, that emails back into the email archive system, and Facebook uses screen captures. And then for different sites there are APIs that capture this and then sometimes it is just electronic capturing of a screen.

Mr. LANKFORD. But the email system that you use specifically with Facebook or the message-to-message with Twitter, how are those captured?

Mr. COLANGELO. For every individual that is provided access into the social networking sites, they are provided additional guidance and training from legal counsel on their Presidential Record Act obligations.

Mr. LANKFORD. Right. But you are saying currently they are not capturing, so the other Gmail and those things are blocked for that, but the actual email out of Facebook, they are just given guidance saying don't do it on that one, but they are not actually tracked, they are not recorded, they are not anything. So a personal message, for instance, on another email, don't forget to grab milk on the way home, would be captured through the traditional email system, but a message that is going through Facebook, through the email system on that, for those computers, would not be captured in any way.

Mr. COLANGELO. Personal email is blocked, again, from all——

Mr. LANKFORD. Right. I mean, if they did it through the traditional system.

Mr. COLANGELO. On the individual users, it is managed on a component-by-component basis for those who have access to those suites. As I mentioned, we don't have an enterprise preservation system currently available.

Mr. LANKFORD. OK. Is that an issue for us, that there is basically email that is going through our system that basically they are just told not to do anything on that should be related to official business, that would just be personal on that, or what are the parameters that are given to them to say you have access to Facebook, but please don't in these areas?

Mr. COLANGELO. I know that the guidance is pretty detailed. I don't have that access, so I haven't gone through the training, so I can't actually speak to that.

Mr. LANKFORD. OK. Do you consider that to be an issue for us at this point, that we do have a series of email communications that are hanging out there that we are not archiving, or do you think that—how can we know on that one way or the other?

Mr. COLANGELO. From a numbers perspective, it is roughly 2 percent, as I noted in my written testimony, so 2 percent of the EOP population that have this access on the government systems. And these users are special users in and of themselves.

Mr. LANKFORD. That is part of the issue. It is not just that there is 2 percent, it is who are the 2 percent I guess would make a significant difference.

Mr. COLANGELO. Sure. And the users are largely the White House new media team, the folks that manage the President Obama's Facebook and the other Facebook accounts out there. And then I know it is also for some lawyers for assessing of candidates, as it is a common corporate practice as well to look at social networking.

Mr. LANKFORD. Is that something that we would consider valuable in a preservation status?

Mr. Ferriero, is that something that you would think, somewhere down the road, people would want to be able to look at?

Mr. COLANGELO. It is the business of the White House. Those are Presidential records.

Mr. LANKFORD. I think we need to find a solution to that. That is one of those things that is hanging out. I understand the technology change and how things are shifting. There is nothing off-the-shelf on that, but it may be something that we need to address in the coming days.

Obviously, this President, as is par for our culture as a whole, is very interested in being able to use social media sites, and I think it is very appropriate. The inappropriate side is we have a large volume of a lot of interaction with constituents and with people and with the White House that is not being tracked and is not being monitored.

Mr. COLANGELO. We continue to look into this technology. We are hoping that the industry evolves.

Mr. LANKFORD. I would just suggest that is something we need to address in the coming days, to be able to establish whether it is a relationship with the social sites or some way to be able to establish that technology-wise.

And with that I yield back.

Chairman ISSA. Thank you. And I thank the gentleman for his interest, and with your history of tracking, what, 21,000 young people every year going through your camps, I suspect that you know more about how to keep track of the hardest things to keep track of in the world.

With that, I want to thank all of our witnesses. You have been very generous with your time. I appreciate your input; it will help us as we go forward. Clearly, some of you will be back again as we try to implement good policy after so many years of a law sustaining that.

With that, we stand adjourned.

[Whereupon, at 11:02 a.m., the committee was adjourned.]

[The prepared statement of Hon. Paul A. Gosar and additional information submitted for the hearing record follow:]

Opening Statement
Congressman Paul Gosar
Committee on Oversight and Government Reform
"Presidential Records in the New Millennium: Updating the Presidential Records Act and Other Federal Recordkeeping Statutes to Improve Electronic Records Preservation"
May 3rd, 2011

Chairman Issa and Ranking Member Cummings, thank you for holding this important hearing, about the future of presidential recordkeeping. The United States has an obligation to keep its governance and sunlight laws updated and current with modern norms.

An incident that ran counter to our national values of transparency and accountability was the Watergate scandal of 1974, during which many members of the Nixon Administration were convicted of using official government resources not only to commit crimes, but to hide the knowledge of these crimes after the fact. It was an incident that shook the nation's confidence in its government, to the degree that President Nixon was forced to resign his post.

This scandal precipitated the passage of the Presidential Records Act, which at the time was meant to tackle the issue of presidential records maintenance. While the PRA was seen as an aggressive approach at the time of passage in 1978, it is no exaggeration to say that electronic communications, media, and technology have completely changed the face of how Americans – and their government – do business. But the PRA has not changed with the times, having received no legislative update since its initial passage. More importantly, this Administration and others have not acted consistently with the spirit of openness. In order to trust our government, the people must be able to monitor its activities.

The PRA creates a presumption in favor of openness and broad disclosure. Exceptions and privileges should be narrowly construed. It is now well established that broad public access serves as an important check, and balance, that allows citizens to maintain control over the government by knowing what the government is doing. Indeed, some consider public access to government records a fundamental right.

It is apparent to me, and many others, that broad public access to government records is a vitally important part of our contemporary system of government. One court explained, in reviewing a public records act matter, the following:

> The cornerstone of a democracy is the ability of its people to question, investigate and monitor the government. Free access to public records is a central building block of our constitutional framework enabling citizen participation in monitoring the machinations of the republic. Conversely, the hallmark of totalitarianism is secrecy and the foundation of tyranny is ignorance. It has been written that "[i]f a nation expects to be ignorant and free, in a state of civilization, it expects what never was and never will be."[i]

That statement applies to the federal government as much or more so than any state government. Meanwhile, some federal employees are using communication methods in the course of official business that do not fall under the PRA, leaving ample room for these employees to bypass the laws meant to capture their communication for official storage and possible disclosure to the public. If this is a deliberate attempt to circumvent the PRA, it should be remedied. A staffer at the White House, for example, may use text messages, personal email accounts, social media sites, and the like for official communications – but without the storage and transparency requirements set forth in the PRA and without the ability of an agency to retrieve and produce such communications, simply because these technologies didn't exist when the PRA was made law.

I support the federal government using new media and 21st century communications in order to keep up with the times. However, it is nearly impossible to comply with the spirit of PRA using these technologies. The law is clearly in need of a major overhaul; I look forward to hearing the witness testimonies today on how these changes can be achieved.

---

[i] Jones v. Jennings, 788 P.2d 732, 735-36 (Alaska 1990).

Questions for Mr. Colangelo
Chief Information Officer
Office of Administration, Executive Office of the President

Rep. Darrell Issa, Chairman
Committee on Oversight and Government Reform

Hearing: "Presidential Records in the New Millennium:
Updating the Presidential Records Act and Other Federal
Recordkeeping Statutes to Improve Electronic Records Preservation"

---

1. **Please provide the Committee with the total number of EMC EmailXtender system-based searches and/or the dates and times of such searches since the EOP began using EmailXtender.**

   The EMC EmailXtender system offers search capability through a search utility that employs a user-friendly interface. The search utility can perform keyword searches, along with searches by the sender or recipient of the email. The search utility can also utilize Boolean logic. A limited number of users are authorized to use the search utility. The EOP has used the search utility periodically since it has been operational.

2. **Have any of EmailXtender's weekly audit reports ever revealed any unauthorized attempts by White House or EOP staff to remove e-mail from the EOP network?**

   No, the weekly audit reports have not revealed any unauthorized attempts by White House or EOP staff to remove e-mail from the EOP network.

3. **How many EOP employees have access to EmailXtender's e-mail search capabilities? Of these, how many are political appointees?**

   Five EOP employees have access to the EMC EmailXtender search utility. Three of these employees were appointed under Title 3 of the United States Code and two were appointed under Title 5. All were employed by the EOP prior to the beginning of the current Administration.

4. **You indicated in your written testimony that the EOP's Office of Administration (OA) has only been capturing PIN-to-PIN messaging among EOP employees since November 2010 – in other words, for only about the last six months (*see p. 11*). What was the precise date in November 2010 when this PIN-to-PIN archiving policy went into effect within the EOP, and what accounted for the delay in archiving PIN-to-PIN messages?**

At the beginning of the Administration there was no system in place for archiving PIN-to-PIN messages and the attention and resources of the Office of the Chief Information Officer were focused on keeping core EOP systems up and operational. Over 82 percent of our IT assets were considered "end-of-life" and this outdated and unstable technology caused multiple outages in the beginning of the Administration. It took significant time to reach the operational state that would enable us to pursue capturing PIN-to-PIN messages—both in terms of stabilizing the architecture of the EOP network to the point that it could handle the configuration and having personnel available to work the issue (rather than concentrating mainly on the emergency work needed to stabilize and modernize EOP systems).

Configuring the EOP system to capture PIN-to-PIN messages was a significant project that required researching potential technical solutions, consulting with the National Archives and Records Administration, developing configuration changes, modifying Blackberry device settings on every EOP Blackberry, restarting the system, and creating storage space. To ensure that our system would not crash when PIN-to-PIN logging was initiated, we first conducted a test pilot program (from October 7, 2010 to October 21, 2010) for eleven users. Once we verified the results of the pilot (that our system was not negatively affected by the capturing of the messages and that the messages were being captured properly), we were able to extend the program EOP-wide on October 28, 2010.

5. **Did the EOP have the technical capability to capture PIN-to-PIN messages before November 2010?**

See answer to Question #4.

6. **Was there any plan for capturing the PIN-to-PIN messages that were transmitted among Blackberry-equipped EOP employees before this archiving policy went into effect in November 2010?**

As described in the answer to Question #4, EOP systems could not capture PIN-to-PIN messages. However, PIN-to-PIN messaging is intended for emergency communications—absent an emergency, EOP policy requires EOP staff to conduct work-related electronic communications on their EOP email account.

7. **Have any of these pre-November 2010 PIN-to-PIN messages been stored or kept in any way that permits review by the National Archives and Records Administration (NARA) or the public, now or in the future?**

Any PIN-to-PIN messages that were stored on EOP BlackBerry devices on October 28, 2010 were captured when the EOP BlackBerry Enterprise Server was reconfigured to log PIN-to-PIN messages, even if they were generated prior to October 28, 2010. Those messages associated with EOP components subject to the Presidential Records Act will be transferred to NARA at the end of the current Administration in accordance with that statute.

8. **You indicated in your written testimony that OA has only been tracking SMS (Short Message Service) texts, or "text messages," among EOP employees since "early March" of this year – in other words, for only about the last two months (*see p. 11*). What was the precise date in March 2011 when this SMS archiving policy went into effect within the EOP, and what accounted for the delay in archiving SMS messages?**

EOP employees do not have the ability to send SMS messages on EOP BlackBerry devices. EOP employees do have the ability to receive SMS messages on EOP BlackBerry devices, for the purpose of receiving emergency communications, especially emergency notifications to all EOP employees from the EOP's Joint Secure Operations Center. These emergency notifications are also sent through the EOP email system. Consequently, emergency notifications sent as SMS messages are duplicate copies of messages sent and archived through the EOP email system.

At the beginning of the Administration there was no system in place for archiving SMS messages and the attention and resources of the Office of the Chief Information Officer were focused on keeping core EOP systems up and operational. Over 82 percent of our IT assets were considered "end-of-life" and this outdated and unstable technology caused multiple outages in the first two months of the Administration. It took significant time to reach the operational state that would enable us to pursue capturing SMS messages—both in terms of stabilizing the architecture of the EOP network and having personnel available to work the issue (rather than concentrating mainly on the emergency work needed to stabilize and modernize EOP systems).

Enterprise-wide logging of SMS messages was implemented on March 3, 2011. The reconfiguration work conducted for PIN-to-PIN capturing laid the groundwork for SMS capturing, but additional work, such as researching potential technical solutions, activating capture functionality, and rebooting all EOP Blackberry devices, was still required.

9. **Did the EOP have the technical capability to capture SMS messages before March 2011?**

See answer to Question #8. Prior to March 3, 2011, it was technically possible for the EOP to request from our mobile carrier a manual capture of SMS messages sent or received on EOP BlackBerry devices within a limited window of time. This process was resource intensive for the carrier and not a service normally provided, however, so it could not be used on a regular basis to archive SMS messages. The EOP did utilize this option for one brief period. After the catastrophic earthquake in Haiti in January 2010, a group of EOP staff were among the federal government personnel who traveled to Haiti to assist in relief efforts. On the island, email access was severely limited and SMS was the most reliable means of communication. OCIO temporarily configured the BlackBerry devices of staff traveling to the island and those with whom they were communicating to be able to both send and receive SMS messages. SMS messages from this period were collected manually by our carrier and archived.

10. Was there any plan for capturing the SMS messages that were transmitted among EOP employees before this archiving policy went into effect in March 2011?

As described in the answer to Question #8, EOP employees do not have the ability to send SMS messages on EOP BlackBerry devices. EOP employees do have the ability to receive SMS messages on EOP BlackBerry devices, for the purpose of receiving emergency communications, especially emergency notifications to all EOP employees from the EOP's Joint Secure Operations Center. These emergency notifications are also sent through the EOP email system. Consequently, the emergency notifications sent as SMS messages were duplicate copies of messages sent and archived through the EOP email system.

As described in the answer to Question #9, the EOP did have a plan for capturing SMS messages sent or received on EOP Blackberry devices when that communication was enabled for the purpose of responding to the earthquake in Haiti.

11. Have any of these pre-March 2011 SMS messages been stored or kept in any way that permits review by NARA or the public, now or in the future?

Email copies of SMS security alerts transmitted by the Joint Secure Operations Center were archived in the EOP email system. The messages that were captured during Haiti relief efforts have been preserved and will be transferred to NARA at the end of the current Administration in accordance with the Presidential Records Act. Any SMS messages that were stored on EOP BlackBerry devices on March 3, 2011 were captured when the EOP BlackBerry Enterprise Server was reconfigured to log SMS messages, even if they were generated prior to March 3, 2011. Those messages associated with EOP components subject to the Presidential Records Act will be transferred to NARA at the end of the current Administration in accordance with

that statute.

12. **Does the EOP currently have any directives or policies prohibiting, or the technical ability to block, EOP employees from utilizing their Blackberries' PIN-to-PIN or SMS messaging except under emergency circumstances?**

The EOP does not have the ability to disable SMS and PIN-to-PIN messaging and activate it in an emergency without creating a substantial risk that either the emergency communication functions would not be successfully activated or that activation could be delayed in the crucial immediate period following a sudden emergency. For that reason, and because the White House Complex and the personnel that work within it could face a wide variety of serious security threats without warning, these emergency communications capabilities are always activated on EOP BlackBerry devices.

EOP policy requires EOP staff to conduct work-related electronic communications on their EOP email account, except in emergency circumstances when staff cannot access the EOP email system and must accomplish time-sensitive work.

13. **Do EOP employees who work on the White House grounds (which include the White House itself and the Eisenhower Executive Office Building) have access, via the use of either EOP computer equipment or their own personal electronic devices, to any Wi-Fi (wireless Internet) networks from the White House grounds, and, if so, what procedures or protocols are in place to ensure EOP network security?**

OCIO does not provide Wi-Fi services for EOP employees on White House grounds at this time. EOP secure mobile workstations, the standard computer used by EOP staff, cannot be configured to connect to a Wi-Fi network. OCIO is exploring ways to enable Wi-Fi capability on these workstations in a secure, records-managed environment. Some EOP users are issued Apple computers for official business, which allow users to connect to Wi-Fi networks but are configured to require them to connect to the EOP Virtual Private Network, which incorporates EOP network filters, before going out to the internet. Users could access external wireless networks from their personal devices or personal cell phones, but these devices cannot connect to the EOP network. EOP users have been instructed to use EOP computers and resources for all official work.

14. **Does the President use a secure Blackberry (or similar personal electronic device) that is not connected to EOP's servers, but rather is connected to its own server(s), and, if so, is there some arrangement, in keeping with the Presidential Records Act, that**

archives these communications?

Emails sent and received from the President's mobile device are secured and archived in accordance with the Presidential Records Act.

15. **In the wake of former White House Deputy CTO Andrew McLaughlin's use of personal e-mail to conduct official business and his subsequent reprimand by White House officials, has the White House or the EOP developed any new directives, policies, procedures, or information campaigns for dealing with employees who violate the rules in the way Mr. McLaughlin did?**

Mr. McLaughlin was employed by the Office of Science and Technology Policy (OSTP) within the Executive Office of the President, rather than the White House Office. My understanding is that OSTP leadership sent a memorandum to all OSTP employees that discussed Mr. McLaughlin's use of personal email, reiterated relevant recordkeeping policies, and stressed the importance of properly archiving government records, and that OSTP also held an office-wide training on records management and updated their records training practices. Additionally, each EOP component has practices and policies for training and reminding employees of their record-keeping obligations.

16. **Besides mere requests to EOP employees, what additional methods does the Administration use to ensure compliance with the Presidential Records Act?**

Like every prior administration subject to the Presidential Records Act (PRA) (Reagan, Bush 41, Clinton, and Bush 43) and every agency subject to the Federal Records Act, this Administration's compliance with the PRA rests in part on educated individual EOP employees responsibly managing their own records in accordance with the PRA. From a technological perspective, OCIO has devoted significant time and resources to modernizing EOP IT systems in order to enhance stability, ensure security and provide for robust electronic records management. While operating within financial and staffing constraints, we have been able to take major steps to modernize an EOP IT infrastructure that was struggling to maintain stable and secure operations. These modernization efforts enhanced electronic records management. Additionally, OCIO has worked proactively to improve electronic records management. In this Administration, we have:

- Maintained the EmailXtender archiving system procured by the Bush Administration;
- Taken steps to upgrade or replace that system before it becomes outdated;

- Upgraded our Miscrosoft Exchange and BlackBerry Enterprise servers to improve their reliability;
- Implemented a system for capturing PIN-to-PIN messages for the first time;
- Implemented a system for capturing SMS messages for the first time;
- Installed a new content management system for the White House website that archives every change to the site;
- Made it easier for staff to work on records-managed EOP systems by deploying secure mobile workstations and creating a secure, web-based portal for remote access to EOP desktop and applications; and
- Restricted EOP network access to websites that could pose records management risks, such as nongovernmental email, social networks, and instant messaging services using web gateway filtering that is regularly updated.