FEDERAL ELECTRONIC RECORDS MANAGEMENT: A STATUS REPORT

HEARING

BEFORE THE

SUBCOMMITTEE ON INFORMATION POLICY,
CENSUS, AND NATIONAL ARCHIVES

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JUNE 17, 2010

Serial No. 111–94

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
MARCY KAPTUR, Ohio
ELEANOR HOLMES NORTON, District of
  Columbia
PATRICK J. KENNEDY, Rhode Island
DANNY K. DAVIS, Illinois
CHRIS VAN HOLLEN, Maryland
HENRY CUELLAR, Texas
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
BILL FOSTER, Illinois
JACKIE SPEIER, California
STEVE DRIEHAUS, Ohio
JUDY CHU, California

DARRELL E. ISSA, California
DAN BURTON, Indiana
JOHN L. MICA, Florida
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
BRIAN P. BILBRAY, California
JIM JORDAN, Ohio
JEFF FLAKE, Arizona
JEFF FORTENBERRY, Nebraska
JASON CHAFFETZ, Utah
AARON SCHOCK, Illinois
BLAINE LUETKEMEYER, Missouri
AHN "JOSPEH" CAO, Louisiana
BILL SHUSTER, Pennsylvania

RON STROMAN, *Staff Director*
MICHAEL MCCARTHY, *Deputy Staff Director*
CARLA HULTBERG, *Chief Clerk*
LARRY BRADY, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

WM. LACY CLAY, Missouri, *Chairman*

CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of
  Columbia
DANNY K. DAVIS, Illinois
STEVE DRIEHAUS, Ohio
HENRY CUELLAR, Texas
JUDY CHU, California

PATRICK T. McHENRY, North Carolina
LYNN A. WESTMORELAND, Georgia
JOHN L. MICA, Florida
JASON CHAFFETZ, Utah

DARRYL PIGGEE, *Staff Director*

CONTENTS

FEDERAL ELECTRONIC RECORDS MANAGEMENT: A STATUS REPORT

THURSDAY, JUNE 17, 2010

House of Representatives,
Subcommittee on Information Policy, Census, and
National Archives,
Committee on Oversight and Government Reform,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:20 p.m., in room 2154, Rayburn House Office Building, Hon. Wm. Lacy Clay (chairman of the subcommittee) presiding.

Present: Representatives Clay, Norton, Driehaus, Cuellar, Chu, Issa, and McHenry.

Staff present: Darryl Piggee, staff director/counsel; Anthony Clark, professional staff member; Charisma Williams, staff assistant; Ron Stroman, full committee chief of staff; Leneal Scott, full committee IT specialist; Rob Borden, minority general counsel; Jennifer Safavian, minority chief counsel for oversight and investigations; Adam Fromm, minority chief clerk and Member liaison; Justin LoFranco, minority press assistant and clerk; Christopher Hixon, minority senior counsel; Ashley Callen, Sery Kim, and Jonathan Skladany, minority counsels; and Mark Marin and Molly Boyle, minority professional staff members.

Mr. CLAY. Good afternoon. The Information Policy, Census, and National Archives Subcommittee will now come to order.

Without objection, the chairman and ranking minority member will have 5 minutes to make opening statements, followed by opening statements not to exceed 3 minutes by any other Member who seeks recognition. And, without objection, Members and witnesses may have 5 legislative days to submit a written statement or extraneous materials for the record.

Welcome to today's hearing, a status report on Federal electronic records management. My opening statement, which I would have made now, will be entered into the record. However, I would like to address an issue that the minority raised during a hearing held by this subcommittee last week on reauthorizing the National Historical Publications and Records Commission.

My Republican colleagues repeatedly questioned the accuracy of the information provided by a witness, Dr. Ira Berlin, on his disclosure form. I had thought that we had resolved the issue during the hearing last week when Dr. Berlin answered the increasingly unpleasant questions directly. However, in a letter dated yesterday, June 16th, to Dr. Berlin, signed by Mr. Chaffetz of Utah and Mr. Jordan of Ohio, the minority continued to assert that Dr. Berlin

was not accurate and completely forthcoming in his disclosure form and his testimony.

Further, the minority asked the Archivist of the United States, Mr. Ferriero, during the hearing for his opinion about duplication among grant programs, and the Archivist gave his opinion. I concur with his opinion, as did the many expert witnesses who came before the subcommittee, that the NHPRC is not duplicative of other programs. And yet, in a second letter, also dated yesterday and sent to Archivist Ferriero, Mr. Chaffetz and Mr. Jordan suggest that the Archivist was not accurate during his testimony at the same hearing.

In both letters the minority strongly suggests that the witnesses were not truthful and urged them to reflect on their testimony and correct it as soon as possible.

Let me state unequivocally and for the record that Dr. Berlin completed his disclosure form accurately and thoroughly. He has provided the subcommittee, and the minority has received a copy, with this information that confirms his form and his testimony was accurate and complete.

I also want to state for the record that Archivist Ferriero was asked his opinion and he gave it truthfully. The minority may certainly disagree with that opinion, just as they may fundamentally misunderstand the nature of the NHPRC, its critical value to this Nation, the distinction between teaching at a university and representing that university, and the differences among Federal grant programs. But to suggest that either of these distinguished witnesses were anything but candid and forthright when appearing before this subcommittee is disgraceful.

I think the minority owes both Dr. Berlin and Archivist Ferriero, who is here today, apologies for the way they treated these honorable and widely respected witnesses.

Now I will yield to my colleague, the ranking minority member, Mr. McHenry, of North Carolina, to respond to what I just said or for an opening statement.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

Statement
Of
Chairman Wm. Lacy Clay, Chairman
Information Policy, Census, and National Archives Subcommittee
Oversight and Government Reform Committee
Thursday, June 17, 2010
2154 Rayburn HOB
2:00 p.m.

"Federal Electronic Records Management: A Status Report"

Welcome to today's hearing, a status report on federal electronic records management. In the course of carrying out their responsibilities, federal agencies create records, many of them electronic, that document the rights of American citizens, the actions of federal officials, and the national experience.

It is the responsibility of each agency, with the support of the National Archives, or NARA, to economically and effectively create and manage records necessary to meet business needs and to keep records long enough to protect rights and assure accountability. The National Archives has an additional responsibility to make sure that records of permanent archival value are preserved and made available for future generations. The focus of today's hearing is not on NARA's responsibility to preserve and make those records available, but on federal agencies' management of their electronic records.

This has been a topic of interest to Congress for many years. In 2003, the Government Accountability Office, or GAO, testified at a hearing of this Subcommittee that "most electronic records…remain unscheduled…and as a result, they were at risk of loss." The Subcommittee Chairman at the time stated that "while NARA has been charged with oversight responsibility regarding these matters, they have been provided little, if any authority, to enforce compliance."

As we will hear from our witnesses today, the state of electronic records management has not changed much since 2003. During a recent self-assessment administered by NARA, seventy nine percent of agencies were found to be at moderate or high risk of improper destruction of their electronic records.

However, initiatives adopted by the Administration within the last eighteen months as well as renewed congressional oversight have produced signs of hope. The requirements of the Open Government Initiative and NARA's public ratings of agencies may finally give records management programs the high level of attention they need in order to improve.

Mr. MCHENRY. Well, Mr. Chairman, thank you. And I appreciate your courtesy in working with me on this subcommittee, especially on this important issue. I see that my ranking member is here. This is an issue that I think was dealt with and would be better addressed by the ranking member, so I would be happy to yield to the ranking member.

Mr. ISSA. I thank the gentleman, and I join with the ranking member of the subcommittee reiterating that all we want to do is maintain the importance of this committee, which requires all witnesses be sworn, that they all make signed statements before they testify as to their truthful testimony, and that we be able to check that for consistency.

Last week, I know the chairman is aware of this, we were halfway through and people were still getting the paperwork right. We asked for no more than we would give if the shoe was on the other foot, and we hope to be held to that standard in the future.

Having said that, certainly it is not our interest today to slow up our witnesses from testifying because of failures previously, so I would yield back the time to the gentleman.

Mr. MCHENRY. I thank the ranking member. Thank you for clarifying that.

In the interest of what is happening today, I appreciate the panel being here today. We are talking about a very important issue that Archivist Ferriero and I have discussed personally, and I know is of distinct interest to him in his new position. And much of what we are talking about now has a much longer time period that we are discussing than the current leadership of the Archives.

So, having said that, we want to talk about how we are going to move forward. Certainly, it is important that we have the Archives efficiently and effectively fulfilling their mission to secure our Nation's records. Our history can so easily be lost by a misplaced computer file, records destroyed, theft, and all these discussions that we have had previously in this subcommittee with testimony from the Archives, from the testimony from the GAO, from the IG, and that record is there; it is established. We have millions of records lost and we want to ensure that, going forward, we are able to keep records.

Archivist Ferriero was quoted on May 25th in the Washington Post as saying, "I think the electronic records archive is probably the biggest, most complex visible and important project that we need to get running. Citizens will be able to, from their home, at any time of the day or night, access the records of government. All the agencies now are experimenting with electronic records and our job is to make sure that we have created the capacity to ingest these records, keep them for perpetuity, and make them available in perpetuity. So that, I think, is my biggest chore."

That might be an understatement. It is certainly a large chore, and that is what we want to discuss today.

The GAO has highlighted some of these challenges in recent reports and criticized the Archives for failing to accurately disclose program costs, schedules, and performance. In addition to sharing the GAO's concerns, I think as we all do, I am concerned about the fact that 21 agencies failed to participate in the Archives records management self-assessment. The self-assessment is a critical tool

for the Archives to evaluate the progress of each and every agency as they transition into digital records management systems.

I think this is the larger issue overall of modernizing our Federal Government so that we have a 21st century bureaucracy, not a 1920's bureaucracy. And, unfortunately, we have the worst of both worlds currently with a quasi-digital, yet quasi-paper management technique, or lack of even management, period.

As I mentioned before, boxes of paper documents fill dozens of the Archives' warehouses across the country. These are the records of our Federal Government and certainly important to the history of our country. And a warehouse is susceptible to fire, flood, burglary, and so many of the other challenges based on just storing in that form.

Finally, I would say that even storing digitally, the question is, 50 years from now, how can we access these things. As a layperson and as individuals, 20 years ago we had a DOS prompt. Nobody uses a DOS prompt anymore. Well, except a few Federal agencies still. Google didn't exist 20 years ago. I mean, everything is evolving so quickly, so the importance of getting it right now, so that we can build on this, is certainly very important.

And I think the American people should be concerned about this because it is our history and our records, and we want to be able to look at our records today just as we look today at records from 100 years ago, and the nice written correspondence with the squiggly handwriting, and we can look at handwriting and judge those things. We are in a different day and age.

So I am interested to hear the testimony. I do think this is important. I certainly appreciate the chairman calling this important hearing and, with his work that we have done together on this subcommittee and his willingness to work across party lines, I appreciate that. Thank you.

Mr. CLAY. I thank the ranking member too. I see that the ranking member of the full committee is still here, and the two colleagues that wrote these letters, Mr. Chaffetz and Mr. Jordan, are not here. Perhaps staff can find them somewhere and perhaps they want to offer up an apology to the Archivist, as well as the——

Mr. ISSA. Mr. Chairman.

Mr. CLAY. I yield.

Mr. ISSA. Thank you. We stand by our letter. We recognize that anyone's interpretation of the letter is subject to many things, but as of this moment we still have inconsistency in the Archivist's previous testimony as to duplicate grants and so on. We don't consider that there were false statements, but they do need to be corrected for the record. I will be glad to inform both Members to come down.

Mr. CLAY. I know that Professor Berlin did correct the record or state it for the record, his involvement. Here is the point. The point is that we should not invite witnesses here and then continually berate them even after they leave through communications from the full committee.

Mr. ISSA. Mr. Chairman——

Mr. CLAY. I have the letters here, Mr. Issa, and I think it is inappropriate.

Mr. ISSA. Mr. Chairman, I speak for the full committee; the other two Members do not. It is our intention to hold accountability while

not berate any witness or have anything other than respect for their accurate statements. And if they are inaccurate, give them full opportunity to correct the record.

We know that mistakes happen in live testimony all the time, and we have no intention of doing anything more than making sure that the final record is correct. So on behalf of the full committee, if anything was taken other than that from our letter, I apologize.

Mr. CLAY. Thank you.

Mr. MCHENRY. And, Mr. Chairman, I reserve the right to berate witnesses if they are from BP.

Mr. CLAY. We will continue with the hearing.

Let me introduce our first panel. Our first witness will be the Archivist of the United States, David Ferriero. Mr. Ferriero has led the National Archives since his confirmation last November. He previously served as the Andrew W. Mellon Director of the New York Public Library, the largest public library system in the United States. Mr. Ferriero earned Bachelors and Masters degrees in English Literature from Northeastern University in Boston and a Masters Degree from the Simmons College of Library and Information Science, also in Boston.

Mr. Ferriero is accompanied by Mr. Jason Baron, who has been the Director of Litigation for the National Archives since 2000. He is a frequent public speaker on the subject of the Federal Government's obligations with respect to the preservation of electronic records and he is an adjunct professor at the University of Maryland, which happens to be my alma mater.

After the Archivist, we will hear from Mr. Paul Wester, the Director of Modern Records Program at the National Archives. Mr. Wester joined NARA in 1990 as a graduate student also from the University of Maryland. He has delivered speeches on electronic records issues and NARA's strategic direction for Federal records management.

Our next witness will be Mr. David Wennergren, the Deputy Assistant Secretary of Defense for Information Management, Integration and Technology, and Deputy Chief Information Officer. He is also the vice chairman of the U.S. Government's Federal CIO Council. Mr. Wennergren received his Master of Public Policy from the University of Maryland, a continuing theme.

And our final witness on this panel will be Ms. Valerie Melvin, Director of Information Management and Human Capital Issues within the U.S. Government Accountability Office's Information Technology Team. Ms. Melvin is also a graduate of, you guessed it, the University of Maryland, with a B.S. degree in business administration and a Master's degree——

Mr. MCHENRY. And I must chime in. I got married 2 weeks ago and I married a graduate from the University of Maryland.

Mr. CLAY. We are so happy that you married up.

Mr. MCHENRY. Thank you. [Laughter.]

Mr. CLAY. Archivist Ferriero, it looks like you are the only one who is not a Terp. The University has connections to the National Archives. Maybe they might want to think about granting you an honorary degree.

I thank all of our witnesses for appearing today and look forward to their testimony.

It is the policy of the subcommittee to swear in all witnesses before they testify. Would you all please stand and raise your right hands?

[Witnesses sworn.]

Mr. CLAY. Thank you. You may be seated.

Let the record reflect that the witnesses answered in the affirmative.

Of course, as you all know, you will have 5 minutes to summarize your testimony. Your complete written statement will be included in the hearing record.

Archivist Ferriero, please begin.

STATEMENTS OF DAVID S. FERRIERO, ARCHIVIST OF THE UNITED STATES, U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, ACCOMPANIED BY JASON BARON, DIRECTOR OF LITIGATION, U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION; PAUL WESTER, DIRECTOR, MODERN RECORDS PROGRAMS, U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION; DAVID M. WENNERGREN, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR INFORMATION MANAGEMENT, INTEGRATION AND TECHNOLOGY, DEPUTY CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF DEFENSE; AND VALERIE C. MELVIN, DIRECTOR, INFORMATION MANAGEMENT AND HUMAN CAPITAL ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

STATEMENT OF DAVID S. FERRIERO

Mr. FERRIERO. Chairman Clay, Ranking Member McHenry, congratulations, and Congresswoman Chu, I am David Ferriero. I am the Archivist of the United States, and thank you for providing me the opportunity for the National Archives and Records Administration to testify about governmentwide Federal records management and the central role that records management plays in the accomplishment of the mission of the National Archives.

The backbone of transparent and accountable 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.

NARA believes that across the Federal Government agencies can do more to fulfill their records management responsibilities, particularly with regard to the exponential growth in electronic records.

NARA's records management approach is grounded in three principles: Federal agencies must economically and effectively create and manage records necessary to meet business needs; Federal records must be kept long enough to protect rights and assure accountability; and, third, Federal records of archival value must be preserved and made available by the National Archives for future generations.

Most Federal agencies need to do a more effective job managing their records and other information assets to meet their business needs, to protect or assure accountability for the citizen or the Federal Government, and to ensure records that document the national

experience are preserved and made available for future generations in the National Archives.

Agency heads and senior leaders must work with NARA, the Office of Management and Budget, and General Services Administration, as well as with groups like Chief Information Officers Council, the Federal Records Council, and the Federal Web Managers Community to develop the information technology tools necessary to manage electronic records in a cost-effective way.

The technical changes associated with developing the IT tools for electronic records management are not insignificant. The lack of effective tools today is due in part because heads of agencies and senior leaders across the Federal Government have not been held accountable in meaningful ways for meeting their Federal records and information management obligations. The Federal Government spends $80 billion annually on information technology, most, if not all, of which create or receive Federal records in some form. Developing cost-effective electronic records management tools that work and then integrating them into agency IT systems is essential to managing this national asset.

Over the past 10 years, NARA has developed a substantial body of electronic records management policy and guidance. The policy includes the first full revision of Federal records management regulations in nearly 25 years. The endorsement for civilian agency use of Department of Defense Electronic Records Management Application Design Criteria Standard, the development of the Records Management Profile, and associated tools for use by Federal agency CIOs to help them think about and account for records management and enterprise architecture; and the issuance of Federal records management guidance on topics such as managing Web records, managing records in a multi-agency environment, and using email archiving applications to store and manage Federal records. All of our electronic records management policy and guidance documents can be found on our Web site, Archives.gov.

In the past 18 to 24 months, NARA has been much more assertive in exercising its statutory authority in this area and reporting on its activities. However, work remains to be done by both NARA and the Federal agencies in creating, preserving, and making available the electronic Federal records that are part of the Nation's documentary heritage.

Our Nation's historical record hinges on the ability of each Federal agency to effectively manage their records. Heads of agencies and senior leaders across the Federal Government need to understand that the records and information they and their organizations are creating are national assets that must be effectively managed and secured so that the public can be assured of the authenticity of the record. Heads of agencies and senior leaders need to be held accountable for managing these assets. Not only is it required by law in the Federal Records Act, effective records management, adequate and proper documentation of the Federal Government's activities and transactions is good government and a necessary condition of an open government.

To more fully explain the concerns in the electronic environment, my colleague, Paul Wester, Director of Modern Records Programs

at NARA, will discuss the results of two recent analyses completed by NARA's National Records Management Program.

Thank you for the opportunity to appear today, and I look forward to answering any questions that you have.

[The prepared statement of Mr. Ferriero follows:]

TESTIMONY OF DAVID S. FERRIERO
ARCHIVIST OF THE UNITED STATES

BEFORE THE SUBCOMMITTEE ON
INFORMATION POLICY, CENSUS AND NATIONAL ARCHIVES

OF THE
HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

ON
"FEDERAL ELECTRONIC RECORDS MANAGEMENT: A STATUS REPORT"

JUNE 17, 2010

Chairman Clay, Ranking Member McHenry, and members of the Subcommittee, I am David S. Ferriero, Archivist of the United States. Thank you for providing the opportunity for the National Archives and Records Administration (NARA) to testify about government-wide Federal records management and the central role that records management plays in the accomplishment of the mission of the National Archives.

The backbone of a transparent and accountable 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.

NARA believes that across the Federal Government agencies can do more to fulfill their records management responsibilities, particularly with regard to the exponential growth in electronic records.

NARA's records management approach is grounded in three principles:

- Federal agencies must economically and effectively create and manage records necessary to meet business needs

- Federal records must be kept long enough to protect rights and assure accountability, and

- Federal records of archival value must be preserved and made available by the National Archives for future generations.

Most Federal agencies need to do a more effective job managing their records and other information assets to meet their business needs; to protect rights or assure accountability for the citizen or the Federal government; and to ensure records that document the national experience are preserved and made available for future generations in the National Archives.

Agency heads and senior leaders must work with NARA, the Office of Management and Budget, and the General Services Administration, as well as with groups like the Chief Information

1

Officers (CIO) Council, the Federal Records Council, and the Federal Web Managers Community to develop the Information Technology (IT) tools necessary to manage electronic records in cost effective ways.

The technical challenges associated with developing the IT tools for electronic records management are not insignificant; the lack of effective tools today is due in part because heads of agencies and senior leaders across the Federal government have not been held accountable in meaningful ways for meeting their Federal records and information management obligations. The Federal Government spends $80 billion annually on information technology, most – if not all – of which create or receive Federal records in some form. Developing cost effective electronic records management tools that work – and then integrating them into agency IT systems – is essential to managing this national asset.

Over the past ten years, NARA has developed a substantial body of electronic records management policy and guidance. The policy includes the first full revision of Federal records management regulations in nearly 25 years; the endorsement for civilian agency use of Department of Defense Electronic Records Management Application (RMA) Design Criteria Standard; the development of the Records Management Profile and associated tools for use by Federal agency CIOs to help them think about and account for records management in enterprise architectures; and the issuance of Federal records management guidance on topics such as managing web records, managing records in a multi-agency environment, and using e-mail archiving applications to store and manage Federal records. All of our electronic records management policy and guidance documents can be found at www.archives.gov/records-mgmt/.

In the past 18 to 24 months, NARA has been much more assertive in exercising its statutory authorities in this area and reporting on its activities. However, work remains to be done by both NARA and the Federal agencies in creating, preserving, and making available the electronic Federal records that are part of the nation's documentary heritage.

Our nation's historical record hinges on the ability of each Federal agency to effectively manage their records. Heads of Agencies and senior leaders across the Federal Government need to understand that the records and information they and their organizations are creating are national assets that must be effectively managed and secured so that the public can be assured of the authenticity of the record. Heads of Agencies and senior leaders need to be held accountable for managing these assets. Not only is it required by law in the Federal Records Act; effective records management – adequate and proper documentation of the Federal government's activities and transactions – is good government and a necessary condition of an open government.

To more fully explain our concerns in the electronic environment, my colleague Paul Wester, Director of Modern Records Programs at NARA, will discuss the results of two recent analyses completed by NARA's National Records Management Program.

Thank you for the opportunity to appear today and I look forward to answering any questions you may have.

Mr. CLAY. Thank you, Archivist Ferriero.

Mr. Wester, we will proceed with your testimony.

STATEMENT OF PAUL WESTER

Mr. WESTER. Good afternoon, Chairman Clay, Ranking Member McHenry, and Congresswoman Chu. My name is Paul Wester, and I am the Director of the Modern Records Programs at the National Archives and Records Administration. I am pleased to appear before you today to provide a status report on Federal electronic records management.

On April 20th, NARA issued a report entitled, "Records Management Self-Assessment 2009: An Assessment of Records Management Programs in the Federal Government." In this report we analyzed the responses to a self-assessment survey NARA sent to 242 Federal cabinet level agencies, their components, and independent agencies. The goal of the self-assessment was to gather data to determine how effective Federal agencies are in meeting the statutory and regulatory requirements for Federal records management.

Based on our analysis and scoring of 220 agency responses, we rated 36 percent of Federal agencies as being at high risk and 43 percent of Federal agencies as being at moderate risk in their records management programs.

Earlier this week NARA completed and issued a report entitled, "NARA's Electronic Records Project, Summary Report: Fiscal Year 2005 through Fiscal Year 2009." In this report we detailed Federal agency compliance with NARA Bulletin 2006–2002, NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002. In this Bulletin, issued in December 2009, NARA formally established a September 30, 2009, deadline for all Federal agencies to submit records schedules to NARA for all of their existing electronic records systems. It also required Federal agencies to schedule new electronic records systems as they are developed.

By the September 30, 2009, deadline, NARA had received electronic records scheduling reports from 160 of 240 Federal agencies for a 67 percent response rate. Of the reporting agencies, 42 percent were considered low risk. However, 25 percent of the reporting agencies were categorized as moderate to high-risk agencies, having submitted schedules to NARA for less than 90 percent of all of their electronic records systems. Thirty-three percent of agencies did not respond to the deadline at all.

We are troubled by the results of this report, as well as the self-assessment of Federal agencies' records management programs. Even though these are baseline reports, we are troubled by the potential levels of risk to Federal records. Overall, the results are unacceptable. We in the agencies need to find ways to do better.

Toward this end, we have undertaken a number of activities. First, we are working to increase awareness of electronic records management requirements and raise accountability for noncompliance. Second, in conjunction with an audit from NARA's Office of the Inspector General, we are undertaking a year-long study of ways to improve NARA's oversight of records management practices. We expect this work to be completed in June 2011.

NARA is also reviewing areas where it maybe useful to clarify the direction in which the Federal Government must move to improve the management of electronic records.

While we will likely identify others in the course of our analysis, there are two broad areas that we know we must examine now. First, we need to identify cost-efficient ways to ensure that agencies manage electronic records electronically and do not rely on paper-based recordkeeping systems to manage electronic records. We need to transition away from traditional print and file record-keeping systems.

Second, given the special long-term preservation and access challenges associated with electronic records, NARA plans to identify ways in which Federal agencies can be encouraged to transfer preservation copies of permanently valuable electronic records to the National Archives as soon as possible for safe keeping.

If NARA is not actively engaged with agencies to fully understand the electronic formats in which records are being created and used, then records may be at risk. As part of its comprehensive review of records management practices, NARA will review options for mitigating this particular risk.

As we state in our strategic plan: Fundamental changes in the Federal Government's business processes, and in the wider information management environment, have critical implications for the records life cycle. Today, the Federal Government creates the bulk of its records and information in electronic form. To deal with these challenges and carry out our mission, NARA must provide leadership and be more agile in adapting to change in information technology and in the Federal recordkeeping environment.

NARA's role as the Nation's record keeper is vital to the future of our Nation. Without a vigorous, forward-thinking records management program, we risk losing the information that documents the daily work of our government and ultimately the history of our Nation.

We look forward to meeting these challenges and carrying out the mission of the National Archives and Records Administration in the years to come.

Thank you for this opportunity to discuss Federal electronic records management with the committee, and I look forward to answering your questions.

[The prepared statement of Mr. Wester follows:]

TESTIMONY OF PAUL M. WESTER, JR.

DIRECTOR, MODERN RECORDS PROGRAMS
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

BEFORE THE SUBCOMMITTEE ON
INFORMATION POLICY, CENSUS AND NATIONAL ARCHIVES

OF THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

ON

"FEDERAL ELECTRONIC RECORDS MANAGEMENT: A STATUS REPORT"

JUNE 17, 2010

Good afternoon Chairman Clay, Ranking Member McHenry, and members of the Subcommittee. My name is Paul Wester and I am the Director of the Modern Records Programs at the National Archives and Records Administration (NARA). I am pleased to appear before you to provide a status report on Federal electronic records management.

The Federal Records Act (FRA) gives NARA responsibility to conduct studies, inspections, or surveys of the records and the records management programs and practices within and between Federal agencies; and to report to the appropriate oversight and appropriations committees of the Congress on these inspections, surveys, and other records management matters.

On April 20, 2010, NARA issued a report entitled "Records Management Self-Assessment, 2009: An Assessment of Records Management Programs in the Federal Government." In this report we analyzed the responses to a mandatory records management self-assessment survey NARA sent to 242 Federal Cabinet Level Agencies, their components, and independent agencies. The goal of the self-assessment was to gather data to determine how effective Federal agencies are in meeting the statutory and regulatory requirements for Federal records management.

Based on our analysis and scoring of 220 agency responses, we rated 36% of Federal agencies as being at High Risk and 43% of Federal agencies as being at Moderate Risk in their records management programs. Only 21% of Federal agencies were found to be at Low Risk in their records management programs.

In the report, we offered the following findings:

- There are varying levels of agency compliance with NARA's required records management regulations and policy, and there are a wide variety of approaches that Federal agencies take in attempting to meet their responsibilities.

- Records management training is not offered consistently or required across the Federal Government, and where it is offered or even required, it is unevenly offered within each Federal agency. If an agency trains only a fraction of its employees – and trains them in an ad hoc manner – it is unlikely that training will significantly improve an agency's ability to manage its records.

- Agencies still struggle to address electronic records, web records, and e-mail management issues. Nearly half of responding records officers do not participate in Capital Planning and Investment Control (CPIC), Systems Development Life Cycle (SDLC), or Business Process Design (BPD) processes in their agencies.

Overall, the findings from the self-assessment are troubling. It is unacceptable that 79% of reporting Federal agencies have moderate to high levels of risk associated with their records management programs, particularly their electronic records management programs.

In June 2010, we issued a second electronic records management report entitled, "NARA's Electronic Records Project, Summary Report: FY 2005 – FY 2009." In this report we detailed Federal agency compliance with NARA Bulletin 2006-02, NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002. In this Bulletin, issued in December 2005, NARA formally established a September 30, 2009, deadline for all Federal agencies to submit records schedules to NARA for all of their existing electronic records and the scheduling of new electronic records systems as they are developed. In subsequent years, we issued additional Bulletins providing agencies with more direction and information on how to meet the September 30, 2009, deadline to assure compliance with the Bulletin.

By the September 30, 2009, deadline, NARA had received electronic records scheduling reports from 160 of 240 Federal agencies for a 67% response rate. Of the reporting agencies, 42% were considered low risk, with records schedules submitted for 90% or more of their existing electronic records.

However, 25% of the reporting agencies were categorized as moderate to high risk, having submitted records schedules to NARA for less than 90 percent of their electronic records, and 33% of agencies did not respond to the deadline at all.

Again, as with the self-assessment, the results of our electronic records project work are troubling. While a great number of Federal electronic records series have been identified and scheduled between FY 2005 and FY 2009-- 2,404 separate series were approved during the period – it is unacceptable that a third of Federal agencies did not respond to the requirement and that 25% of the reporting agencies are at high risk with regard to scheduling their electronic records.

Litigation is focusing more public attention on how agencies manage their electronic records. At least two prominent lawsuits from the past two decades have involved preservation of White House e-mail records. One result of the lawsuit captioned *Armstrong v. Executive Office of the President*, filed in 1989 and originally involving records on National Security Council backup tapes, was that NARA revised its electronic recordkeeping regulations in 1995 to expressly provide for management of e-mail communications as Federal records. In a subsequent lawsuit, *Public Citizen v. Carlin*, the Archivist's authority to promulgate a general records schedule covering e-mail records was upheld. More recently, we understand that in various settings Federal records are increasingly being demanded in their native or "electronic" format, so as to meet the Government's e-discovery litigation obligations. This trend supports our view that agencies need to pay more attention to long-term management of their electronic records in electronic form.

Toward this end, and beyond the two reports cited above and other ongoing work based on our current statutory authority, we have undertaken a number of activities.

First, building on existing work done by the leading information policy agencies like the Office of Management and Budget and the General Services Administration – as well as formal advisory or policymaking groups like the CIO Council, the Federal Records Council, and others – we are working to increase awareness of electronic records management requirements and raise accountability for noncompliance with those requirements.

Second, in conjunction with an audit from NARA's Office of the Inspector General that coincided with the appointment of a new Archivist of the United States in November 2009, we are undertaking a year-long study of ways to improve NARA's oversight of records management practices. A particular area of interest will be an evaluation of the Archivist's statutory authority to conduct oversight responsibilities. We expect this work to be completed in June 2011.

NARA is also reviewing areas where it may be useful to clarify the direction in which the Federal Government must move to improve the management of electronic records, while analyzing the costs and benefits of different approaches.

While we will likely identify others in the course of our analysis, there are two broad areas that we know we must examine.

First, we need to identify cost efficient ways to ensure that agencies manage electronic records electronically and transition away from relying on official recordkeeping systems for electronic records that require the printing and filing of e-mail and other electronic records. Currently, most agencies have "print and file" policies for managing their e-mail. These policies require agency personnel print out and file individual e-mails into official, usually paper-based, recordkeeping systems. 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.

Second, given the special long-term preservation and access challenges associated with electronic records, NARA plans to identify ways in which Federal agencies can be encouraged – to transfer preservation copies of permanently valuable electronic records to the National Archives as soon as possible.

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.

While our staff are often able to negotiate early transfers of electronic and special media records, and while we are increasingly working with Federal agencies to pre-accession permanent electronic records into the National Archives, the current piecemeal approach does not ensure NARA's long-term ability to preserve and eventually provide continuing access to electronic records of enduring value.

For every case where we are able to negotiate the early transfer of preservation copies of permanent electronic records – as we are currently working with the Bureau of the Census to transfer the 2010 enumeration with its 500 terabytes of scanned images which will come to the National Archives in the next 18 to 24 months for preservation until their release in 2082 – there are many, many other series of permanently valuable electronic records that are in jeopardy because we are unaware of them or a preservation copy has not been provided to the National Archives for safekeeping.

As we state in our strategic plan:

> *Fundamental changes in the Federal Government's business processes, and in the wider information management environment, have critical implications for the records lifecycle. Today, the Federal Government creates the bulk of its records and information in electronic form. To deal with these challenges and carry out our mission, NARA must provide leadership and be more agile in adapting to change in information technology and in the Federal recordkeeping environment.*
>
> *NARA's role as the nation's record keeper is vital to the future of our nation. Without a vigorous, forward-thinking records management program, we risk losing the information that documents the daily work of our Government and, ultimately, the history of our nation.*

We look forward to meeting these challenges and carrying out the mission of the National Archives and Records Administration for many years into the future.

Thank you for this opportunity to discuss Federal electronic records management with the Committee, and I look forward to answering your questions.

Mr. CLAY. Thank you so much, Mr. Wester.

Mr. Wennergren, you are up.

STATEMENT OF DAVID M. WENNERGREN

Mr. WENNERGREN. Mr. Chairman, Ranking Member McHenry, and distinguished members of the subcommittee, thank you for the opportunity to appear before you today.

The information age is providing tremendous opportunities for the Department of Defense to improve operational effectiveness through the accelerated and expanded use of information technology. Paper-based business processes are being transitioned to electronic-based solutions.

And thanks to technology advances like service-oriented architecture and the advent of Web 2.0 tools, new information capabilities can be delivered much more rapidly today than we even dreamed possible a few years ago. There is an imperative to have information tools in place both to realize the power of information sharing and to address crucial issues of information security.

Accompanying this pervasive transformation is the ever-increasing importance of electronic records management. And while the challenges that we encounter in implementing electronic records management are significant, we are committed to ensuring compliance with records management rules and regulations, as well as ensuring that records management solutions are transparent to war fighters, relatively simple to use, and aligned with business processes. We have policy and standards in place to address the life cycle of management of records and to ensure compliance with NARA policies.

I would like to take a moment and highlight our electronic records management application standard. This standard identifies the mandatory requirements for records management application software. It leverages our joint interoperability test command to certify applications as compliant and allows DOD components to procure and implement compliant-records management application software. We are pleased that the standard was endorsed by NARA in 2008 and recommended for use by all Federal agencies.

Like all large organizations, we face several challenges in this work: the scope of deploying records management applications across a 3½ million person organization; the need to also simultaneously ensure legacy IT systems are compliant; and the imperative of having a work force that is trained and adept at electronic records management.

While DOD already maintains trained records managers throughout the organization, information technology advances have shifted records management responsibilities from central records management organizations to individual employees. Consequently, our training efforts have expanded to ensure the entire work force understands the importance of making records management an integral part of daily operations.

In closing, we are committed to working with NARA to ensure we effectively address records management, while simultaneously transforming the Department.

Thank you again for allowing me the opportunity to appear, and I am happy to answer any questions that you have.

[The prepared statement of Mr. Wennergren follows:]

20

STATEMENT BY

MR. DAVID M. WENNERGREN

DEPUTY ASSISTANT SECRETARY OF DEFENSE

FOR INFORMATION MANAGEMENT, INTEGRATION, AND TECHNOLOGY

AND DoD DEPUTY CHIEF INFORMATION OFFICER

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SUBCOMMITTEE ON

INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

2154 RAYBURN HOUSE OFFICE BUILDING
JUNE 17, 2010
2:00 P.M.

Good afternoon, Chairman Clay, Congressman McHenry and Members of the

Information Policy, Census, and National Archives Subcommittee. My name is David

Wennergren, and I am the Deputy Assistant Secretary of Defense for Information

Management, Integration and Technology and Deputy Chief Information Officer (CIO).

I want to thank you for the opportunity to appear before the Subcommittee to discuss

issues related to electronic records management and the Department's efforts in

complying with existing statutory and regulatory requirements from the National

Archives and Records Administration (NARA).

TRANSITIONING THE DEPARTMENT INTO THE INFORMATION AGE

The Information Age provides tremendous opportunities to improve operational

effectiveness through the accelerated use of information technology. The Department of

Defense is increasingly reliant on information technology in all aspects of its operations,

and our success will be measured by how we effectively manage information in a

contested environment. Across the Department, paper-based business processes are

being transitioned to electronic-based solutions. And thanks to technology advances like

service-oriented architecture and the advent of Web 2.0 tools, new information

capabilities are able to be delivered much more rapidly today than was even dreamed

possible a few years ago. To this end, the Department has been making significant

strides in implementing a Service-Oriented Information Enterprise where data assets,

services, and information sharing solutions are visible, accessible, understandable, and

trusted by all authorized users. This service-oriented environment strategy for DoD

establishes web services as the preferred means by which data producers and capability

providers can make their data assets and capabilities available across the DoD and

beyond. It also establishes services as the preferred means by which consumers can

access and use these data assets and capabilities.

Accompanying this transformation is the ever increasing importance of electronic records

management, to include records storage, records scheduling of electronic information

systems, proper disposition of records, and preservation of media devices. The

Department is committed to ensuring compliance with records management regulations,

integrating records management into any newly developed information system and

bringing legacy systems into compliance.

The challenges that we encounter as we develop Information Technology (IT)

tools for records management are not inconsequential and our goal is to develop records

management application software that is transparent to the worker, relatively simple to

use, consistent and compatible with existing business processes, and scalable to grow as

electronic demands evolve.

DoD RECORDS MANAGEMENT INTRODUCTION

Policy and standards to implement the DoD Records Management Program are in

place, and this guidance addresses both the life cycle management of information as

records in all types of media, as well as ensuring compliance with policies and

procedures issued by NARA. Effective records management involves close

collaboration across all DoD Components as they implement records management solutions within their respective subordinate organizations. Together, we ensure that all DoD Component Records Managers adhere to the core tenets outlined by the Archivist of NARA to:

- create and manage the records needed to meet our DoD business needs,

- keep records long enough to protect rights and assure accountability, and

- preserve those DoD records of archival value for future generations.

DoD maintains trained records managers at all levels to help achieve these principles. In addition, as information technology advances have resulted in the shifting of responsibility for records management from central records management organizations to individual employees, we are all working to ensure that we have a trained and educated workforce that understands the importance of making records management an integral part of the daily operational cycle for all organizations.

Two key DoD policies drive this records management work. The first is DoD Directive 5015.02, "DoD Records Management Program," which provides overarching guidance to the entire Department. The second is DoD 5015.02-Standard, "Electronic Records Management Software Applications Design Criteria Standard," April 2007. This latter document, known as the Standard, is used primarily to test and verify software proposed for use within DoD as a records management application or "RMA."

DoD 5015.02 STANDARD

The DoD Standard identifies mandatory baseline requirements for Records Management Application (RMA) software used by DoD Components in implementing their records management programs. Use of the Standard allows Components to procure, test and implement compliant records management application software. In addition, the Standard defines required system interfaces and search criteria that RMAs shall support, outlines requirements for classified marking and access control, and identifies non-mandatory features deemed desirable for RMA software. It includes requirements for managing Freedom of Information Act and Privacy Act records. The Standard also includes requirements for RMA-to-RMA interoperability, archival transfer to the NARA, and the use of metadata. Information sharing is a key focus for the Department and the use of metadata is an important element in DoD's information sharing strategy. Metadata can also be an important tool used for records management, which is why it was included in the latest revision of the standard.

We are pleased that the DoD Standard was endorsed by NARA in 2008 for use by all Federal agencies. NARA's endorsement states that the Standard complies with NARA's instruction for transferring permanent electronic records to NARA and the official endorsement is included in its entirety in NARA Bulletin 2008-07. Through this endorsement, NARA has recommended that agencies use the DoD Standard and the DoD-certified products as a baseline when selecting an RMA to manage an agency's electronic records.

Currently, the Joint Interoperability Test Command (JITC), under the Defense

Information Systems Agency, manages the compliance testing process for the DOD

Standard and certifies records management applications as compliant to our Standard.

An example of how this standards process has influenced our enterprise-wide

environment can be seen in the deployment of a tested RMA solution on the Navy

Marine Corps Intranet, which serves well over 350,000 users. DoD Components use this

Standard in the implementation of their records management programs to include

certification testing by Joint Interoperability Test Command (JITC). The DoD Standard

has also been used by some states, other Federal agencies and even some in the

international community. It is open enough to encompass different functions and

infrastructures, but serves to assure consistently useful electronic records products.

PLANNED UPDATE TO DOD DIRECTIVE FOR RECORDS MANAGEMENT

Just as the information management environment is continually changing, so must

our policies for records management need to adapt to stay relevant. Consequently, we are

in the process of revising the DoD Directive for Records Management. Our revised

directive will incorporate the NARA Federal Enterprise Architecture Records

Management Profile. We are also building records management requirements into our

DoD Information Technology (IT) governance processes for capital planning, enterprise

architecture, business process design, and system development life cycle. To avoid

having to retrofit IT systems with RM software, we plan to ensure that records

management is built into newly created electronic information systems and that legacy

systems, in their next stages of delivery, include an electronic records management solution. The revised Directive will ensure interoperability of electronic information at the DoD Component and interagency levels where electronic records are shared or transferred to another federal agency. And finally, to focus on comprehensive training, DoD will ensure its employees and contractors receive records management training to include understanding user responsibilities in managing DoD information as records, knowing the proper records disposition procedures, and learning to use records management software tools, if applicable.

SUMMARY

In conclusion, the Department is focused, in concert with NARA, on creating responsive policies for ensuring all information systems are developed with records management in the forefront and not as an afterthought. We are committed to successfully managing a diverse records management portfolio to comply with NARA guidance while leading the Department toward service-oriented enterprise operations and aggressively working to move away from paper-based, labor intensive processes.

Mr. CLAY. Thank you so much for your testimony.

Ms. Melvin, you have 5 minutes.

STATEMENT OF VALERIE C. MELVIN

Ms. MELVIN. Thank you, Mr. Chairman, Ranking Member McHenry, and members of the subcommittee. I am pleased to participate in today's hearing on the electronic records management in the Federal Government. As you have requested, I will provide some background on the roles of agencies and NARA, and briefly discuss some of the challenges of managing electronic records.

As you know, the Federal Records Act requires agencies to have programs and appropriate systems to manage information documenting government functions, decisions, and other important transactions. If such records are poorly managed, individuals might lose access to legitimate benefits, the Government could be exposed to legal liabilities, and records of historical interest could be lost forever. Poorly managed records also increase the costs of responding to FOIA requests or litigation-related discovery actions and impede accountability and efficiency.

Nonetheless, as we have long reported, records management has historically been subject to neglect, in part because it is not a core agency mission. A major challenge for agency records managers is to make the case for investing in records management in an environment of limited resources.

Although agency heads are ultimately responsible for their agencies' records, NARA has a role in improving Federal records management through providing guidance, assistance, and oversight. In its oversight role, NARA is responsible for conducting inspections or surveys, conducting records management studies, and reporting the results.

However, in 2008, we reported that NARA had not fully used its oversight authority, as it had not conducted any inspections of agency programs since 2000, nor consistently reported the results of its oversight activities. Accordingly, we recommended that NARA implement a new approach to oversight that more fully used its existing authority.

In response, as has been mentioned already, NARA developed an oversight strategy that included the agency records management self-assessment survey, which it recently reported on. NARA had said that it plans to use annual surveys to provide an overall picture of Federal records management and to inform its oversight activities, including inspections.

As weaknesses reported in NARA's survey indicate, giving priority to records management remains a major challenge. Effective records management, electronic or otherwise, requires investing time and resources to analyze the information an agency receives, produces, and uses to fulfill its mission. This allows an agency to determine what categories of documents and informational records, and it can then associate its records with information that will help it find and use those records, and finally dispose of those no longer needed.

Electronic records are particularly challenging because of their complexity, ever-increasing volume, and decentralized environment in which they are created. In the desktop computer age, individual

users create and store large numbers of documents, particularly email, and it is difficult to get users to distinguish record from non-record material and treat it appropriately.

Even when electronic record keeping features are integrated into email systems, users may resist having to categorize every email they send or receive. In an ideal situation, records would be automatically identified and captured, with little or no user intervention. Technology that aims to automatically categorize records is beginning to appear, but its effectiveness will depend on devoting resources to proper implementation and the context of established records management programs.

As our work has demonstrated, technology is a tool to help solve problems, not a solution in itself, however. Like any technology, electronic records management systems require careful planning and analysis of agency requirements, business processes and information, along with the necessary management attention and resources to ensure effective implementation.

The long history of records management neglect suggests that raising its priority will not happen easily. However, several factors could encourage progress: first, NARA's public scoring of agency records management programs could raise their profile within agencies; second, greater recognition of the increasing risk posed by weak management of electronic records and information could focus management attention; third, the recent Open Government Directive includes specific requirements for records management as part of its push to make more information public. This could help make records and information management a more central agency mission. Finally, congressional oversight, such as this hearing, could also help raise the priority given to this important issue.

Mr. Chairman, this completes my prepared statement, and I would be pleased to respond to any questions.

[The prepared statement of Ms. Melvin follows:]

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Information
Policy, Census and National Archives,
Committee on Oversight and Government
Reform, House of Representatives

INFORMATION MANAGEMENT

The Challenges of Managing Electronic Records

Statement of Valerie C. Melvin,
Director, Information Management and Human Capital
Issues

GAO
Accountability * Integrity * Reliability

June 17, 2010

INFORMATION MANAGEMENT

The Challenges of Managing Electronic Records

Why GAO Did This Study

Federal agencies are increasingly using electronic means to create, exchange, and store information, and in doing so, they frequently create federal records: that is, information, in whatever form, that documents government functions, activities, decisions, and other important transactions. As the volume of electronic information grows, so does the challenge of managing electronic records. Both federal agency heads and the National Archives and Records Administration (NARA) have responsibilities for managing federal records.

As requested, after providing some context about records management in the federal government and the roles of federal agencies and NARA, this testimony describes the challenges of electronic records management and potential means of addressing these challenges.

In preparing this testimony, GAO relied primarily on its previous work, supplemented by analysis of publicly available documents.

What GAO Found

Under the Federal Records Act, agencies are to manage the creation, maintenance, use, and disposition of records in order to achieve adequate and proper documentation of the policies and transactions of the federal government and effective and economical management of agency operations. If records are poorly managed, individuals might lose access to benefits for which they are entitled, the government could be exposed to legal liabilities, and records of historical interest could be lost forever. NARA is responsible, among other things, for providing records management guidance, assistance, and oversight.

However, as GAO has previously reported, records management has received low priority within the federal government. Prior reports have identified persistent weaknesses in federal records management, including a lack of policies and training. GAO's most recent report, in 2008, found weaknesses in e-mail management at the four agencies reviewed due in part to insufficient oversight and training. This year, NARA published the results of its first annual agency records management self-assessment survey, indicating that almost 80 percent of agencies were at moderate to high risk of improper disposition of records.

Electronic records are challenging to manage, especially as electronic information is being created in volumes that pose a significant technical challenge to the ability to organize and make it accessible. Further, electronic records range in complexity from simple text files to highly complex formats with embedded computational formulas and dynamic content, and new formats continue to be created. Finally, in a decentralized environment, it is difficult to ensure that records are properly identified and managed by end users on individual desktops (the "user challenge"). E-mail is particularly problematic, because it combines all these challenges and is ubiquitous.

Technology alone cannot solve the problem without commitment from agencies. Electronic recordkeeping systems can be challenging to implement and can require considerable resources for planning and implementation, including establishing a sound records management program as a basis. In addition, the "user problem" is not yet solved, particularly for e-mail messages. Further, automation will not solve the problem of lack of priority, which is of long standing. However, several developments may lead to increased senior-level attention to records management: NARA's use of public ratings as a spur to agency management, growing recognition of risks entailed in poor information and records management, the requirements and emphasis of the recent Open Government Directive, and the influence of congressional oversight. Senior management commitment, if followed through with effective implementation, could improve the governmentwide management of electronic and other records.

_____United States Government Accountability Office

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to discuss critical issues surrounding electronic records management in the federal government. As you are aware, federal agencies are increasingly using electronic means to create, exchange, and store information, and in doing so, they frequently create federal records. According to the Federal Records Act,[1] federal records are information in whatever form that documents government functions, activities, decisions, and other important transactions, and such records must be managed and preserved in accordance with the act.[2] As the volume of electronically stored information grows, so does the challenge of managing electronic records.

As requested, after providing some context about records management in the federal government and the roles of federal agencies and the National Archives and Records Administration (NARA), my statement will focus on describing the challenges of electronic records management and potential means of addressing these challenges.

My comments today are based primarily on our previous work, all of which was conducted in accordance with generally accepted government auditing standards, supplemented by analysis of information contained in publicly available documents, following appropriate GAO quality assurance processes.

Background

The federal government collects, generates, and uses large amounts of information in electronic form, from enormous geographic databases to individual e-mails. Much of that information can constitute official federal records, and agencies must have ways to manage such records.

---

[1] 44 U.S.C. chapters 21, 29, 31, and 33.

[2] The definition of a record is given at 44 U.S.C. 3301.

Federal Agencies and NARA Have Responsibilities for Federal Records Management

Under the Federal Records Act,[3] each federal agency is required to make and preserve records that (1) document the organization, functions, policies, decisions, procedures, and essential transactions of the agency and (2) provide the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities.[4] If these records are not effectively managed, individuals might lose access to benefits for which they are entitled, the government could be exposed to legal liabilities, and historical records of vital interest could be lost forever. In addition, agencies with poorly managed records risk increased costs when attempting to search their records in response to Freedom of Information Act requests or litigation-related discovery actions. Finally, without effective management of the documentation of government actions, the ability of the people to hold the government accountable is jeopardized.

Effective records management is also an important tool for efficient government operation. Without adequate and readily accessible documentation, agencies may not have access to important operational information to make decisions and carry out their missions.[5]

Accordingly, to ensure that they have appropriate recordkeeping systems with which to manage and preserve their records, agencies are required to develop records management programs.[6] These programs are intended, among other things, to provide for accurate and complete documentation of the policies and transactions of each federal agency, to control the quality and quantity of records they produce, and to provide for judicious preservation and disposal of federal records.

---

[3] 44 U.S.C. chapters 21, 29, 31, and 33.

[4] 44 U.S.C. § 3101.

[5] See, generally, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[6] 44 U.S.C. § 3102.

Among the activities of a records management program are identifying records and sources of records and providing records management guidance, including agency-specific recordkeeping practices that establish what records need to be created in order to conduct agency business.

Under the Federal Records Act and the regulations issued by NARA, records must be effectively managed throughout their life cycle, which includes records creation or receipt, maintenance and use, and disposition. Agencies *create* records to meet the business needs and legal responsibilities of federal programs and (to the extent known) the needs of internal and external stakeholders who may make secondary use of the records. To *maintain and use* the records created, agencies are to establish internal recordkeeping requirements for maintaining records, consistently apply these requirements, and establish systems that allow them to find records that they need. *Disposition* involves transferring records of permanent, historical value to NARA for archiving and destroying all other records that are no longer needed for agency operations.

One key records management process is *scheduling,* the means by which NARA and agencies identify federal records and determine time frames for disposition. Creating records schedules involves identifying and inventorying records, appraising their value, determining whether they are temporary or permanent, and determining how long records should be kept before they are destroyed or turned over to NARA for archiving. For example, one general records schedule permits civilian agencies to destroy case files for merit promotions[7] (2 years after the personnel action is completed, or after an audit by the Office of Personnel Management, whichever is sooner). No record may be destroyed or permanently transferred to NARA unless it has been scheduled, so the schedule is of critical importance. Without schedules, agencies would have no clear criteria for when to dispose of records and, to avoid disposing of them unlawfully, would have to maintain them indefinitely.

---

[7] That is, records relating to the promotion of an individual that document qualification standards, evaluation methods, selection procedures, and evaluations of candidates. Such records are covered under the General Records Schedule 1, Civilian Personnel Records.

Scheduling records, electronic or otherwise, requires agencies to invest time and resources to analyze the information that an agency receives, produces, and uses to fulfill its mission. Such an analysis allows an agency to set up processes and structures to associate records with schedules and other information (metadata) to help it find and use records during their useful lives and dispose of those no longer needed.

Records schedules are based on content and are media-neutral; that is, electronic records are classified on the same basis—by content— as physical records. In addition, agencies are to compile inventories of their information systems, after which the agency is required to develop a schedule for the electronic records maintained in those systems.

NARA also has responsibilities related to scheduling records. NARA works with agencies to help schedule records, and it must approve all agency records schedules. It also develops and maintains general records schedules covering records common to several or all agencies. According to NARA, records covered by general records schedules make up about a third of all federal records. For the other two thirds, NARA and the agencies must agree upon agency-specific records schedules.

Under the Federal Records Act, NARA is given general oversight responsibilities for records management as well as general responsibilities for archiving—the preservation in the National Archives of the United States of permanent records documenting the activities of the government.[8] Of the total number of federal records, less than 3 percent are permanent. (However, under the act and other statutes, some of the responsibilities for oversight over federal records management are divided across several agencies. Under the Federal Records Act, NARA shares a number of records management responsibilities and authorities with the General

---

[8] 44 U.S.C. § 2904. Relevant NARA regulations implementing the Federal Records Act are found at 36 C.F.R. §§ 1220–1238.

Services Administration (GSA).[9] The Office of Management and Budget (OMB) also has records management oversight responsibilities under the Paperwork Reduction Act[10] and the E-Government Act.[11])

For records management, NARA is responsible for issuing guidance; working with agencies to implement effective controls over the creation, maintenance, and use of records in the conduct of agency business; providing oversight of agencies' records management programs; approving the disposition (destruction or preservation) of records; and providing storage facilities for agency records. The act also gives NARA the responsibility for conducting inspections or surveys of agency records and records management programs.

Federal Records Management Has Been Given Low Priority and Has Had Persistent Weaknesses

Historically, despite the requirements of the Federal Records Act, records management has received low priority within the federal government. As early as 1981, in a report entitled *Federal Records Management: A History of Neglect*,[12] we stated that "persistent records management shortcomings" had been attributed to causes that included "lack of commitment by top management, emphasis on agency missions, and the low priority of records management." Almost 30 years later, the priority problem has remained remarkably persistent.

For instance, a 2001 study prepared for NARA by SRA International, Inc., on perceptions in the federal government with respect to records management, concluded that recordkeeping and records

[9] These shared responsibilities are due in part to the origins of NARA. The 1984 National Archives and Records Administration Act, Pub. L. No. 98-497, 98 Stat. 2280 (Oct. 19, 1984), transferred the functions of GSA's National Archives and Records Service to the newly created NARA.

[10] *See* 44 U.S.C. § 3504.

[11] *See* 44 U.S.C. § 3602.

[12] GAO, *Federal Records Management: A History of Neglect*, PLRD-81-2 (Washington, D.C.: Feb. 24, 1981).

management in general receive low priority, as evidenced by lack of staff or budget resources, absence of up-to-date policies and procedures, lack of training, and lack of accountability.[13] This assessment also concluded that although agencies were creating and maintaining records appropriately, most electronic records remained unscheduled, and records of historical value were not being identified and provided to NARA for archiving.

In 2002, drawing on the 2001 study, we reported that the low priority given to records management programs was a factor in program weaknesses.[14] We noted that records management is generally considered a "support" activity. Because support functions are typically the most dispensable in agencies, resources for and focus on these functions are often limited.

In 2008, we reported on weaknesses in federal e-mail management at four agencies.[15] The four agencies reviewed generally managed e-mail records through paper-based processes, rather than using electronic recordkeeping. (A transition to electronic recordkeeping was under way at one of the four agencies, and two had long-term plans to use electronic recordkeeping.) We attributed weaknesses in agency e-mail management (such as senior officials not conforming to regulations) to factors including insufficient training and oversight regarding recordkeeping practices (as well as the onerousness of handling large volumes of e-mail)—similar to the effects of low priority described by SRA. Accordingly, we recommended that agencies with weaknesses in oversight, policies, and practices develop and apply oversight practices, such as reviews and monitoring of records management training and practices, that would be adequate to ensure that policies were

[13] SRA International, Inc., *Report on Current Recordkeeping Practices within the Federal Government* (Dec. 10, 2001) (www.archives.gov/records-mgmt/faqs/pdf/report-on-recordkeeping-practices.pdf). This document reports on both a recordkeeping study performed by SRA International and a series of records system analyses performed by NARA staff.

[14] GAO, *Information Management: Challenges in Managing and Preserving Electronic Records*, GAO-02-586 (Washington, D.C.: June 17, 2002).

[15] GAO, *Federal Records: National Archives and Selected Agencies Need to Strengthen E-Mail Management*, GAO-08-742 (Washington, D.C.: June 13, 2008).

effective and that staff were adequately trained and were implementing policies appropriately.

Further evidence of the persistence of the priority issue was provided in 2008, when NARA surveyed federal senior managers about their perception of records management. According to the survey, only 64 percent of managers saw records management as a useful tool for mitigating risk.

In April 2010, NARA released a report on its first annual records management self-assessment, which analyzed responses to a survey sent in September 2009 to 245 federal cabinet-level agencies, agency components, and independent agencies.[16] According to NARA, the survey results showed that almost 80 percent of agencies were at moderate to high risk of improper disposition of records.[17] For example, the survey found that not all agencies had appropriate policies in place for handling e-mail, and that only a little over half of the responding agencies had training in place for high-level executives and political appointees on how to manage e-mail; this is consistent with the finding in our 2008 report on e-mail practices regarding insufficient training and oversight regarding recordkeeping practices. NARA rated almost half of the responding agencies (105 of 221) as high risk in the area of e-mail.

NARA's survey also indicated, among other things, that a large proportion of agencies have not scheduled existing systems that contain electronic records. In December 2005, NARA issued a bulletin requiring agencies to have NARA-approved records schedules for all records in existing electronic information systems by September 30, 2009. 27 percent of agencies responding to NARA's

---

[16] NARA, *Records Management Self-Assessment 2009: An Assessment of Records Management Programs in the Federal Government* (April 2010); 220 agencies responded, for a response rate of 91 percent.

[17] NARA assessed risk by calculating a weighted score based on agencies' responses to the 34 survey questions. Scores above 90 of 100 possible points are considered low risk, 60 to 89 are moderate risk, and below 60 are high risk. NARA also identified issues that impact the reliability of the data including not covering the full universe of agencies, issues relating to the roles of department vs. component-level records officers, and problems involving some questions being unclear. NARA did not validate agencies' self-reported results.

September 2009 agency self-assessment survey indicated that fewer than half of their electronic systems were scheduled. Such large numbers of unscheduled systems are a problem for agencies because their records cannot legally be disposed of, with the consequences for increased cost and risk mentioned earlier.

NARA concluded that the varying levels of agency compliance with its records management regulations and policies have implications for the government's effectiveness and efficiency in conducting its business, protecting citizens' rights, assuring government accountability, and preserving our national history.

Our Previous Reports Have Recommended Strengthening NARA's Oversight Approach

The Federal Records Act gave NARA responsibility for oversight of agency records management programs by, among other functions, making it responsible for conducting inspections or surveys of agencies' records and records management programs and practices; conducting records management studies; and reporting the results of these activities to the Congress and OMB.[18]

We have made recommendations to NARA in previous reports that were aimed at improving NARA's insight into the state of federal records management as a basis for determining where its attention is most needed. In 1999, in reporting on the substantial challenge of managing and preserving electronic records in an era of rapidly changing technology,[19] we noted that NARA did not have governmentwide data on the electronic records management capabilities and programs of all federal agencies. Accordingly, we recommended that NARA conduct a governmentwide survey of these programs and use the information as input to its efforts to reengineer its business processes. However, instead of doing a governmentwide baseline assessment survey as we recommended,

---

[18] In particular, the reports are to include evaluations of responses by agencies to any recommendations resulting from inspections or studies that NARA conducts and, to the extent practicable, estimates of costs to the government if agencies do not implement such recommendations.

[19] GAO, *National Archives: Preserving Electronic Records in an Era of Rapidly Changing Technology*, GGD-99-94 (Washington, D.C.: July 19, 1999).

NARA planned to obtain information from a limited sample of agencies, stating that it would evaluate the need for such a survey later.[20]

In 2002, we reported that because NARA did not perform systematic inspections of agency records management, it did not have comprehensive information on implementation issues and areas where guidance needed strengthening.[21] We noted that in 2000, NARA had suspended agency evaluations (inspections) because it considered that these reached only a few agencies, were often perceived negatively, and resulted in a list of records management problems that agencies then had to resolve on their own. However, we concluded that the new approach that NARA initiated (targeted assistance) did not provide systematic and comprehensive information for assessing progress over time. (Only agencies requesting assistance were evaluated, and the scope and focus of the assistance were determined not by NARA but by the requesting agency.) Accordingly, we recommended that it develop a strategy for conducting systematic inspections of agency records management programs to (1) periodically assess agency progress in improving records management programs and (2) evaluate the efficacy of NARA's governmentwide guidance.

In response to our recommendations, NARA devised a strategy for a comprehensive approach to improving agency records management that included inspections and identification of risks and priorities. Subsequently, it also developed an implementation plan that included undertaking agency inspections based on a risk-based model, government studies, or media reports.[22]

---

[20] In 2001, as mentioned earlier, the NARA-sponsored SRA study was released (www.archives.gov/records-mgmt/faqs/pdf/report-on-recordkeeping-practices.pdf). This document reports on both a recordkeeping study performed by SRA and a series of records system analyses performed by NARA staff.

[21] GAO, *Information Management: Challenges in Managing and Preserving Electronic Records,* GAO-02-586 (Washington, D.C.: June 17, 2002).

[22] GAO, *Electronic Records Archives: The National Archives and Records Administration's Fiscal Year 2006 Expenditure Plan,* GAO-06-906 (Washington, D.C.: Aug. 18, 2006).

In 2008, we reported that under its oversight strategy, NARA had performed or sponsored six records management studies in the previous 5 years, but it had not conducted any inspections since 2000, because it used inspections only to address cases of the highest risk, and no recent cases met its criteria.[23] In addition, NARA's reporting to the Congress and OMB did not consistently provide evaluations of responses by federal agencies to its recommendations, as required, or details on records management problems or recommended practices that were discovered as a result of inspections, studies, or targeted assistance projects.

Accordingly, we recommended that NARA develop and implement an oversight approach that provides adequate assurance that agencies are following NARA guidance, including both regular assessments of agency records and records management programs and reporting on these assessments. NARA agreed with our recommendations and devised a strategy that included annual self-assessment surveys, inspections, and reporting. It has now begun implementing that strategy, having released the results of its first governmentwide self-assessment survey, as mentioned earlier.

Managing Records in Electronic Form Presents Major Challenges

As we have previously reported,[24] electronic records pose major management challenges: their volume, their complexity, and the increasingly decentralized environment in which they are created. E-mail epitomizes the challenge, as it is not only voluminous and complex, but also ubiquitous.

- *Huge volumes of electronic information are being created.*

Electronic information is increasingly being created in volumes that pose a significant technical challenge to our ability to organize it and

---

[23] GAO, *Federal Records: National Archives and Selected Agencies Need to Strengthen E-Mail Management*, GAO-08-742 (Washington, D.C.: June 13, 2008).

[24] GAO, *Information Management: Challenges in Managing and Preserving Electronic Records*, GAO-02-586 (Washington, D.C.: June 17, 2002).

make it accessible. An example of this growth is provided by the difference between the digital records of the George W. Bush administration and that of the Clinton administration: NARA has reported that the Bush administration transferred 77 terabytes[25] of data to the Archives on leaving office, which was about 35 times the amount of data transferred by the Clinton administration. Another example is the Department of Energy's National Energy Research Scientific Computing Center, which said that, as of January 2009, it had over 3.9 petabytes of data (that is, about 4,000,000,000,000,000 bytes) in over 66 million files and that the volume of data in storage doubles almost every year.[26]

- *Electronic records are complex.*

  Electronic records have evolved from simple text-based files to complex digital objects that may contain embedded images (still and moving), sounds, hyperlinks, or spreadsheets with computational formulas. Some portions of electronic records, such as the content of dynamic Web pages, are created on the fly from databases and exist only during the viewing session. Others, such as e-mail, may contain multiple attachments, and they may be threaded (that is, related e-mail messages are linked into send–reply chains). They may depend heavily on context. For example, to understand the significance of an e-mail, we may need to know not only the identity but the position in the agency of the sender and recipients. (Was it sent by an executive or a low-level employee?) In addition, new technologies, such as blogs, wikis, tweets, and social media, continue to emerge, posing new challenges to records managers.

- *Identification and classification of electronic records are difficult in a decentralized computing environment.*

  The challenge of managing electronic records significantly increases with the decentralization of the computing environment. In the centralized environment of a mainframe computer, it is

---

[25] A terabyte is about 1 trillion bytes, or 1000 gigabytes.

[26] We did not verify the specific numbers, which are provided for illustrative purposes only.

comparatively simple to identify, assess, and manage electronic records. However, in the decentralized environment of agencies' office automation systems, every user can create electronic files of generally unstructured data that may be formal records and thus should be managed. Documents can be created on individuals' desktop computers and stored on local hard drives. E-mail can come from outside the agency. In cases like these, the agency generally depends on the individual to identify the document or the e-mail as a record, and, through placing it in a recordkeeping system, associate it with its appropriate schedule, make it searchable and retrievable, and preserve it until it is due for disposal.

As we reported in 2008,[27] e-mail is especially problematic. E-mail embodies several major challenges to records management:

- It is unstructured data, and it can be about anything, or about several subjects in the same message, making it difficult to classify by content.

- There is a very large volume of it: one study estimates that a typical corporate user sends or receives around 110 messages a day.[28] Further, there may be many copies of the same e-mail, which can increase storage requirements or require a means of determining which copy to keep. Keeping large numbers of messages potentially increases the time, effort, and expense needed to search for information in response to a business need or an outside inquiry, such as a Freedom of Information Act request.

- It is complex: e-mail records may have multiple attachments in a variety of formats, they may include formatting that is important for meaning, and they include information about senders, recipients, and time of sending. Recordkeeping systems must be able to capture all this information and must maintain the association between the e-mail and its attachment(s).

---

[27] GAO, *Federal Records: National Archives and Selected Agencies Need to Strengthen E-Mail Management*, GAO-08-742 (Washington, D.C.: June 13, 2008).

[28] The Radicati Group, Inc., *Email Statistics Report, 2010* (Palo Alto, Calif.: April 2010).

- Its relevance depends on context. It may be part of a message thread that is necessary to understand its content, or it may discuss other documents or issues that are not well identified. An e-mail that says "I agree. Let's do it" may be about a major decision or about going to lunch next week.

- It may not be obvious who is responsible for identifying an e-mail as a record and at what point. NARA regulations require that both senders and recipients may be responsible for identifying records. However, an e-mail may have multiple recipients and be forwarded to still other recipients.

Agency Commitment Is a Prerequisite for Addressing the Electronic Records Challenge

As NARA has pointed out, the decision to move to electronic recordkeeping is inevitable, but as we and NARA have previously reported, implementing such systems requires that agencies commit the necessary resources for planning and implementation, including establishing a sound records management program as a basis. Further, automation will not, at least at the current state of the technology, solve the "end user problem"—relying on individual users to make sound record decisions. Nor will automation solve the problem of lack of priority, which, as our previous work has shown, is of long standing. However, several developments could lead to increased senior-level attention to records management: NARA's use of public ratings as a spur to agency management, growing recognition of risks entailed in poor information and records management, the requirements and emphasis of the recent Open Government Directive, and the influence of congressional oversight. Senior management commitment, if followed through with effective implementation, could improve the governmentwide management of electronic and other records.

Electronic Recordkeeping Systems Are Challenging to Implement and Will Not Yet Solve the End User Problem

Moving to electronic recordkeeping is not a simple or easy process. Agencies must balance the potential benefits against the costs of

44

redesigning business processes and investing in technology. Our previous work has shown that such investments, like any information technology investment, require careful planning in the context of the specific agency's circumstances, in addition to well-managed implementation.

In 2007, a NARA study team examined the experiences of five federal agencies (including itself) with electronic records management applications, with a particular emphasis on how these organizations used these applications to manage e-mail.[29] Among the major conclusions was that although the functionality of the software product itself is important, other factors are also crucial, such as agency culture and the quality of the records management program in place. With regard to e-mail in particular, the survey concluded that for some agencies, the volume of e-mail messages created and received may be too overwhelming to be managed at the desktop by thousands of employees across many sites using a records management application alone. A follow-up study in 2008 added that although a records management application offers compliant electronic recordkeeping, "it can be expensive to acquire, time consuming to prepare for and implement, requires user intervention to file records, and can be costly over the long haul for data migration and system upgrades."[30] NARA found that in most instances agencies had to work to overcome user resistance to using the system.

This user challenge has led records management experts to believe that end users cannot be relied on to manage e-mail records, or indeed any other types of records. A recent Gartner study concluded that user-driven classification of records, especially e-mail, has failed and will continue to fail;[31] a study by the Association for

---

[29] NARA, *A Survey of Federal Agency Records Management Applications 2007* (Jan. 22, 2008).

[30] NARA, *Continuing Study of Federal Agency Recordkeeping Technologies 2008* (Washington, D.C.: 2008).

[31] Gartner Research, *How to Address the Federal Government's Records Management Challenges*, G00165869 (Mar. 14, 2009).

Information and Image Management (AIIM)[32] stated "it is simply not plausible to expect all creators of records to perform accurate, manual declaration and classification."[33] According to Gartner, "What enterprises really need (and want) is a mechanism that automatically classifies messages by records management type … without user intervention."[34] At the time of writing (August 2007), Gartner described such technology as "in its infancy," but expected it to mature rapidly because of high demand.

This technology, automated records classification (sometimes called "autocategorization"), might help address the user problem. (The Air Force is currently working with autocategorization projects.[35]) However, like other information technology, it requires resources for setup and maintenance to be effective, and it is not simple to implement.[36] Further, according to AIIM, autocategorization might not work for an agency's particular documents or file plan, and might not be sufficiently accurate or cost effective.

Some proposals have been made to simplify the e-mail problem. Gartner recommends treating e-mail as a separate issue from general records management, perhaps by putting all e-mail in a single category of temporary records with a uniform retention period. Similarly, the Director of Litigation in NARA's Office of General Counsel has suggested keeping all e-mail created by key

---

[32] AIIM is a nonprofit organization focused on the management of documents, content, records, and business processes, as well as enterprise content management (ECM).

[33] Richard Medina, David Gaffaney, and Linda Andrews, "Autocategorization: One Key Component for Enterprise Records Management," *AIIM E-Doc Magazine*, Vol. 20, Iss. 4 (July/August 2006).

[34] Gartner Research, *Best Practices in Records Management: FAQs*, G00149526 (Aug. 17, 2007).

[35] Michael Corrigan and J. Timothy Sprehe, "Intelligent Categorization: Air Force Information Asset Management," presentation delivered at FIRM Council March Program, (Mar. 4, 2010). http://www.digitalgovernment.com/Downloads/E-Discovery-Records--Information-Management-Conference.shtml

[36] Automated classification systems may for example depend on sets of rules, such as the appearance of specific key words, to determine whether a document is a record and what series of records it belongs to. (For example, the words "litigation" and "plaintiff" appearing in a document might identify it as a legal record.)

senior officials (with some additional designations by agency components) as permanent and treating all the rest as temporary. Both proposals would make managing e-mail simpler, but could increase the risk that significant information will not be preserved.

Recent Developments Could Help Spur More Action on Information and Records Management

Raising the priority of records management has been and continues to be an uphill battle. As we have reported, government needs to prioritize the use of resources, and records management has not been a high priority. Further, records management can also be time- and resource-consuming and technically difficult to implement.

NARA can influence this situation by providing effective guidance and assistance to agencies, as well as through its oversight and reporting activities. With its recently initiated annual self-assessment survey, NARA is responding to our earlier recommendations on oversight by beginning an effort to develop a comprehensive view of the state of federal records management as a basis for determining where its attention is most needed. Reporting the results of the survey, with scores for individual agencies and components, to the Congress, OMB, and the public is one way to help bring the records management issue to the attention of senior agency management.

Another factor that could help raise awareness of the value of records management is the growing recognition of the risks of weak electronic records and information management, as a result of fear of potentially large costs to organizations that have to produce electronically stored information to respond to litigation, as well as well-publicized incidents of lost records, including e-mail. This recognition of risk is coupled with increased awareness of the value of organizations' information assets; according to AIIM, the field of enterprise content management (which includes records management) has been accepted, driven by the need to control the content chaos that pervades local drives, file shares, email systems, and legacy document stores. As a result, according to an AIIM survey, the highest current priorities for ECM activity are electronic records management and managing e-mails as records.

Further, recent Open Government initiatives, which emphasize the importance of making information available to the public for transparency and accountability, could be an additional impetus to addressing electronic records management. OMB's Open Government Directive makes a direct link between open government and records management by requiring that each agency's Open Government Plan include a link to a publicly available Web site that shows how the agency is meeting its existing records management requirements.[37] More generally, the directive urges agencies to use modern technology to disseminate useful information. According to an Administration official, records management plays a crucial role in open government by ensuring accountability through proper documentation of government actions.[38] Increased attention to information and records management could provide another spur encouraging agencies to devote resources to managing their electronic records more effectively.

Finally, the priority that agencies give to addressing weaknesses may be increased by hearings such as this, which show that the Congress recognizes the importance of good records management for the efficient, effective, and accountable operations of government.

In summary, federal records management has been given low priority for many years. However, the explosion of electronic information and records is an increasing risk to agencies, and could even become a drag on agencies' ability to perform their missions if not brought under control.

Raising visibility, as NARA is doing by publishing the results of its self-assessment survey, can raise the perception among senior

---

[37] OMB, *Open Government Directive*, M-10-06 (December 8, 2009).

[38] Cass R. Sunstein, Administrator of the Office of Information and Regulatory Affairs, OMB, "Open Government and Records Management," Keynote, NARA 2010 Records Administration Conference (May 12, 2010). http://archives.gov/records-mgmt/pdf/sunstein-raco2010.pdf

agency officials of the importance of records management. Also significant is the push for Open Government, which, by heightening the importance of agencies' providing information to the public, makes information a more central part of their missions and could help highlight the actual importance to agencies of actively managing their information. Strong indications from the Congress that records management needs more attention could also raise the priority among agency management.

Mr. Chairman, this completes my prepared statement. I would be pleased to respond to any questions you or other Members of the Subcommittee may have at this time.

Contact and Acknowledgments

If you should have questions about this testimony, please contact me at (202) 512-6304 or melvinv@gao.gov. Other major contributors include Barbara Collier, Lee McCracken, J. Michael Resser, and Glenn Spiegel.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Mr. CLAY. Thank you so much, Ms. Melvin.

We will now proceed to questioning of the witnesses on the 5-minute rule, and we will begin with the gentlewoman from California leading off the questions.

Ms. CHU. Thank you, Mr. Chair.

Well, I was alarmed to hear about the results of the NARA study that 79 percent of all agencies are at a high or moderate risk of improper destruction of records, and the numbers are disturbingly high. Let me ask do you have the proper authority to carry out your statutory and regulatory responsibilities, Mr. Wester? And, if not, are there specific legislative changes that need to be made in order to ensure that NARA can properly carry out its mission?

Mr. WESTER. Thank you very much for the question. What we need to do in the coming years, conduct our analysis of our current statutory authorities and the policies that we have in place right now to see what kinds of limitations we have with the authorities and policies we have right now to improve records management.

My sense of it is there are things that we can do in the policy arena, in the guidance arena, and with making agencies more aware and publicizing the different aspects of either lack of attention or poor management of records within agencies that I think will be able to help us improve records management within agencies. In the meantime, we need to conduct the analysis of our statutory authorities and the guidance and regulation that we already have to see if it meets the needs that we see as the National Archives, as well as the needs that Federal agencies have to better manage their records.

Ms. CHU. So you think there might be some extra authority that you may need, but you have to do the study first?

Mr. WESTER. I believe that is true.

Ms. CHU. Because I noted that out of the 240 Federal agencies that were supposed to submit to you by September 2009, only 160 even responded. What can you do to make them respond? And are we to assume that the rest that did not respond have even worse records?

Mr. WESTER. I don't think we should assume that they have worse records. Some of the issues that we have with the agencies who were non-responsive have issues of resources within their organizations that have kept them from getting the submissions in on time. We have had our staff following up on agencies who did not respond and we have subsequently gotten materials back from them. But what our reporting has helped do is raise the issue within those agencies, because a lot of the agencies have found out from the publication of our report and the distribution of our report in the press and in other arenas, they have found out that their records management programs are not up to snuff and senior leadership within those agencies has taken a greater interest in this issue and has helped to highlight it and make changes or increase the emphasis on these issues within those agencies to make the awareness higher and that agencies will be able to devote resources to answer the questions in the future and help us be able to follow-up on issues that arose from that survey.

Ms. CHU. So again going back to the authority, what can you do to make them respond? And also if you inspect an agency's elec-

tronic records program and you have a suggestion for change, what can you do to make them respond to whatever you suggest?

Mr. WESTER. Within our current statutory authority, we have the authority to go into an agency and conduct an inspection, go in and inspect records, inspect how agencies are managing those records. We also have the authority to make reports to Congress and to OMB, both to Oversight Committees as well as the Appropriations Committees to make those issues aware to the funding sources and the oversight sources, both executive and in the legislative branch.

We also have the authority to continue to followup on those reports and make reports to the public on how well agencies are managing or not managing their records, following up on those inspections, and that is what we intend to do with the inspections.

Ms. CHU. And what if they don't respond?

Mr. WESTER. We would bring these issues to the attention of more senior folks in the agency and to the Oversight Committees and the Appropriations Committees. That is the authority that we have currently.

Ms. CHU. Ms. Melvin, you suggested that perhaps the authority that NARA has has not been utilized to its maximum. Could you explain that?

Ms. MELVIN. Yes. Following up, actually, on a 2008 report that we issued and which we discussed on NARA's oversight and the extent to which it had been undertaken, our concern was that we believe that NARA has authority that it had not used fully; and we based this on the fact that in recent years NARA had not conducted inspections.

At the time that we looked at it in 2008, they were primarily performing studies; however, we found that they had not conducted any inspections since 2000. At that time we made recommendations to NARA as far as increasing its inspections to look for opportunities, to have a more comprehensive evaluation and provide a more governmentwide picture.

We recognize that they now have done the survey, and we would look at that as a first step toward moving in that direction, but clearly, from our perspective, we think that there are opportunities. We have seen that they have been really good at putting plans in place, but from the standpoint of actually following through to actually conduct oversight through inspections, in particular, and looking at more thoroughly, I should say, at what agencies are undertaking in the way of records management is something that we would like to see more of.

Ms. CHU. And how many of the 245 agencies have formal record retention policies? And of those that don't, what can you do to make them get a policy, Mr. Wester?

Mr. WESTER. Most of the agencies, virtually all the agencies have records retention policies. The issue is the validity of those policies given how old some of them are, how current they are, and how well they cover different aspects of changing records management environment. Where we have moved from a paper environment to an electronic environment, some of those policies have not kept pace with the issues that those agencies need to confront as they manage their records.

Ms. CHU. OK, thank you. I see my time is up. I yield back.

Mr. CLAY. Thank you.

The gentleman from North Carolina is recognized.

Mr. McHENRY. Thank you, Mr. Chairman.

And thank you all for your testimony.

To Ms. Melvin's point, Mr. Wester, the followup, the inspections, can you respond to that?

Mr. WESTER. Yes. We are going to be launching an inspection starting next week with the Office of the Secretary of Defense and the Under Secretary for Intelligence to take a look at how email is managed within those two organizations.

Mr. McHENRY. So you are beginning that process?

Mr. WESTER. We are beginning that process right now.

Mr. McHENRY. OK.

So, Ms. Melvin, to your point, how well has NARA, in your view, implemented the recommendations of the GAO in order to move forward on electronic records management?

Ms. MELVIN. On electronic records management specifically? They have been working to implement our recommendations. We have seen some implemented, but from the standpoint of our overall recommendations, I believe the recommendations for the 2008 report are still in process, so we have not fully seen that they have been fully implemented at this time.

Mr. McHENRY. OK.

Dr. Ferriero, thank you for your testimony. We have had this discussion before, that you are taking an agency that has some personnel challenges. We have some good folks at NARA and you have explained that, but there is a lack of motivation among a large group, and you have to change the culture. With electronic records archive, you inherited, I will say that clearly, you inherited a problem here. It is over budget, behind schedule. What progress is being made?

Mr. CLAY. Excuse me. Mr. McHenry, let me just state that NARA is building the electronic records archive, ERA, to maintain that small percentage of records that they receive, but this is not the subject of the hearing. The hearing is on the Federal Records Act, not ERA.

Mr. McHENRY. OK. Well——

Mr. CLAY. Hopefully, we can confine our questioning to the Federal Records Act.

Mr. McHENRY. OK, I didn't think that was a problem. I have asked a variety of questions of Dr. Ferriero, and this is one that I keep bringing up. I just want to see that there is progress being made because——

Mr. CLAY. There will be a hearing in the future on ERA.

Mr. McHENRY. OK. Well, then, Mr. Chairman, do you want to ask questions, then? I will yield my time to you, because this is of interest to me in terms of progress being made, and I didn't realize I was limited by the scope of the questions.

Mr. CLAY. Well, I mean, look, the witnesses are here to talk about the Federal Records Act.

Mr. McHENRY. OK. Well, all right.

Well, self-assessment. You mentioned the self-assessment. The SEC didn't respond. Even the Congressional Budget Office didn't

respond. How in the hell do we get these agencies to respond, Dr. Ferriero?

Mr. FERRIERO. For me, the self-assessment was the baseline that we need to move forward. As you heard, NARA has not exercised its inspection authority since 2000, and this was the beginning of a reestablishment of our authority. I will be communicating directly with the agencies who haven't responded with some reasons for noncompliance with our direction, and we will continue to followup with them.

For me, the self-assessment is kind of the beginning of identifying those agencies that are in most need of help, and we need to focus on those particular agencies especially to ensure that they get the support and guidance that is available from NARA.

Mr. MCHENRY. OK. You used the word accountability a number of times in your testimony. Do you have the ability to hold these agencies accountable?

Mr. FERRIERO. I believe we do. Put yourself in the situation of an agency that hasn't had any authority exercised over them for 8 years, and all of a sudden they get a demand for a self-assessment. There is an attitude that develops that they don't take it seriously, and I would guess that we experienced some of that in this process.

Mr. MCHENRY. Mr. Wester, do you want to comment on that?

Mr. WESTER. What I would like to say is that we have launched a new assessment for 2010 that we launched in the middle of May, and as part of launching the self-assessment for 2010, the Archivist sent personal letters to each of the agency heads, and I have to say that the response that we have gotten from the senior levels of agencies has been much more robust than it was when we had done it in the previous manner before Mr. Ferriero came on board in November.

So I think we are making great strides with the agencies in raising the awareness at the senior levels about this issue, but, as the Archivist said, we need to followup with the agencies to make sure that they continue to complete the self-assessments and, more importantly, continue to improve their records management programs.

Mr. MCHENRY. All right.

I yield back, Mr. Chairman.

Mr. CLAY. Mr. Cuellar of Texas, you are recognized.

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

My questions are more procedures dealing with relationships with agencies, NARA and GAO. GAO has done a series of reports, and I think they have been mentioned. The one in 1999, where they recommended several things, including conducting a governmentwide survey of the programs and the information used. Instead of using a governmentwide baseline assessment survey, I think it was more limited in scope, is that correct, Ms. Melvin?

Ms. MELVIN. That is correct, yes.

Mr. CUELLAR. OK. Then in 2002 there was another report and NARA came up with a strategy for a comprehensive report on that, but again there were some issues there, is that correct?

Ms. MELVIN. That is correct, yes.

Mr. CUELLAR. All right. Then, of course, we are looking at your current report here also. But I guess my question to the panel is

GAO comes up with recommendations and then what happens? I mean, the purpose is to improve the process. What happens? What happens in the process when a report comes up from GAO?

I mean, if I was part of NARA, I would say, "OK, I agree with the recommendations" or "I don't agree with the recommendations." But if I do agree with the recommendations, let's see how fast we can implement it.

Who wants to be first?

Mr. WESTER. I will go first. To talk about what we have done at the National Archives over the time period that you have described in relationship to the engagements that we have had with GAO, what we have done is we have gotten the recommendations, we have taken a look at how we can respond to them, and we have made plans and attempted to address each of the recommendations that have been brought before us and have tried to make strides in dealing with the recommendations and improving records management, electronic records management within the government.

One of the things that has been a challenge for the National Archives during this time period has been the change of the records environment within agencies across the Federal Government. When our work began, more or less in 2000, which is probably a good marker to use for this discussion, we were in a transitional period across the Federal Government, where we had a lot of agencies who were still primarily paper-based organizations that were increasingly using electronic records.

From 2000 on, what the National Archives had to do was figure out how to address the increasing electronic records challenge within the government and develop guidance and policies, and promulgate those guidances and policies and update our regulations to help agencies know what to do to better manage their electronic records.

So there was a long period of time when we spent a good deal of resources on that issue, and it has only been in the last probably 18 to 24 months, perhaps a little longer than that, that we have gotten a body of guidance and regulation in place that we are able to now hold agencies more accountable specifically to electronic records issues across the government.

So it has been, as you observe, a long journey for us, and it has probably taken us too long, but that is the path that we have gone on in trying to be responsive to the issues that have been brought before us by GAO, as well as the environment that we find ourselves in with the Federal agencies.

Mr. FERRIERO. Could I respond to that also?

Mr. CUELLAR. Yes, sir.

Mr. FERRIERO. As the head of the agency, I treat these reports, as well as the reports from my Inspector General, very seriously. These are, in lots of cases, early warning signs for me in terms of where we need to correct action and, as I said, these reports have my full attention.

Mr. CUELLAR. Anybody else?

[No response.]

Mr. CUELLAR. And I will close up with this, Mr. Chairman. I guess, in trying to improve the process and get better results, if a recommendation comes in and you truly disagree with it, because

there will be times that we are going to disagree. GAO is not 100 percent correct, just like we are never 100 percent. Then I understand you can go ahead and have a dialog on that. But once you all accept the recommendation, we are hoping that at that time that you all, as fast as possible, within certain contours, implement that as soon as possible.

Mr. Chairman, I will just ask GAO. Any thoughts on that?

Ms. MELVIN. Whenever we make the recommendations, we are hopeful that an agency will consider them in the fullest. Again, our concerns had not been so much with the fact that they were not planning toward efforts, but that we did not see the level of investment in those efforts, if you will, to make sure that there were——

Mr. CUELLAR. Excuse me. The commitment, right? I think that is the term that you used in here, the commitment?

Ms. MELVIN. We wanted to see definitely a greater commitment to trying to get a governmentwide look at what was happening in Federal records management. We did see the agency take steps, but steps that, from our position, fell short of what we thought were necessary for them to have or to provide the necessary oversight and to be in a position to influence agencies, if you will, to have better records management programs in place.

Mr. CUELLAR. OK, thank you. And I know it is difficult, complex, ever-changing, but I appreciate all the efforts that you all do. Thank you.

Mr. CLAY. Thank you, Mr. Cuellar.

Mr. CUELLAR. Thank you, Mr. Chairman.

Mr. CLAY. Mr. McHenry, you are recognized for 5 minutes.

Mr. MCHENRY. Dr. Ferriero, just to followup with what we have discussed before, in terms of improving morale. What has your approach been? What progress have you made?

Mr. FERRIERO. I am putting a lot of faith in the governmentwide employee viewpoint survey, and I am pleased to report that 83 percent of NARA employees participated this year, compared to 52 percent last year. They got personal email messages from me; they got voicemail messages from me; I did video to encourage people to participate; and here again we are expecting the results within a couple of weeks.

This will be another baseline for me in terms of just how bad things are in terms of morale. We have established a task force to help me work through these issues as we start getting the results to improve the environment, the culture of the agency.

It has my full attention. As I said before, this is the most important thing that I have to worry about. We have to get this right in order to do everything else that the agency has before it.

Mr. MCHENRY. You have served at large institutions with significant technology, both New York universities, more of a quasi-governmental agency. You have had a variety of information protection background. How far behind or ahead would you rank the Archives and what you are walking into in comparison to those other sectors you have worked in?

Mr. FERRIERO. Is your question around technology or is it around protection of collections?

Mr. MCHENRY. Both.

Mr. FERRIERO. OK. In terms of technology, it feels very similar to probably the environment 15 years ago in terms of what I would describe as everyone doing their own thing. This figure that I cited, $80 billion a year on information technology, is a huge figure, and it reminds me very much of the university environment years ago where every department was able to do their own thing, buy their own systems, and then enterprise systems came in and kind of reduced the costs associated with that.

So there is some of that I see at work now. I think some of the ideas around cloud computing that I am hearing will address some of those issues. And there are some examples of enterprise systems that are underway, but it is in the early stages, I would say, reflective of the amount of money that is being spent.

On the collection side, we have established a holdings protection task force. As you know, we have had some problems in terms of materials that are lost, and we are serious about correcting those problems and creating a sense of urgency around that within the agency, all 44 facilities across the country.

Mr. MCHENRY. Is it a greater challenge, in your view, the protection of electronic data, rather than some of the traditional paper forms of data collection? I mean, do you have sort of a greater concern with one——

Mr. FERRIERO. It is more complicated. It is more complicated because of threats to access to destroy electronic information, to change it. So ensuring the authenticity of that original record is certainly more complicated than the paper environment.

Mr. MCHENRY. OK. Because Archives certainly has a long history of being able to protect that traditional data.

Mr. FERRIERO. And to ensure that 100 years from now you are looking at what was originally created. Exactly.

Mr. MCHENRY. And is that part of the struggle, being able to create a system by which future generations will be able to retrieve this electronically?

Mr. FERRIERO. And that those digits get migrated as technology changes. Exactly.

Mr. MCHENRY. Well, thank you. Thank you for your candor.

Mr. CLAY. Thank you, Mr. McHenry.

Mr. Wennergren, the DOD has established a standard for records management applications that has been endorsed by NARA. Is this something that the Department simply created once or is it continually revised and improved?

Mr. WENNERGREN. Yes, sir, it is a continuing process. We have actually dozens of tools from many different companies, different operating systems. We have a whole market basket of tools that have gone through this compliance process, so we look at them, we make sure that they are going to meet the needs, and then we publish those lists of preferred products, if you will. And then our agencies can go buy those products and be assured that they are going to get a product that works for them. With NARA's endorsement, it has sort of opened the door to others to take advantage of that too.

We also have examples inside of the Department of Defense. The Navy, for example, has a records management compliant product. It is on hundreds of thousands of desktops; it has millions of

records. So we have great successes within the Department of people using those tools, but now we have a lot of interest from others. So we have other Federal agencies, States, local governments, even some other nations that have come to find out what these preferred products are and how they can take advantage of using them too.

Mr. CLAY. So you are pretty much spreading the gospel, so to speak, to other agencies and to other countries about records management.

Mr. WENNERGREN. Yes, sir. If we get a line to secure products that work well and are interoperable, that is always the best approach. So we are happy to have any agency come ask us for the information about how we do the compliance process. The products that are certified are available on the Web site, so anybody can go look at them and go buy the one that they choose.

Mr. CLAY. Exactly how many agencies would you estimate have adopted some of your practices?

Mr. WENNERGREN. See, I don't have a good answer on that, sir, because what I know is that lots of people come and ask for information, but at DOD I don't keep track of then what they go and buy. So I have a list of like literally 80 or 90 organizations that have come and asked us about how do you do the certification testing and all that sort of stuff, but then we don't keep track if the city of Illinois came and was interested, we don't actually know whether they go and buy them or not, because they would go buy them directly from the vendor.

Mr. CLAY. OK. Thank you for that.

Ms. Melvin, examining the challenges of electronic records is not something new for GAO. However, this administration has been more proactive about transparency than previous Presidents. How will the Open Government Initiative help with electronic records management?

Ms. MELVIN. Well, the Open Government Directive that was put in place does have within it a requirement that agencies include in their plans a link to a Web site that would provide information on their records management programs.

Mr. CLAY. Let me ask you about Members of Congress. A lot of us have BlackBerries. We have official business on there; we also may get an email from our children, from our parents, from our wives, saying, "on your way home would you stop at the store and get some milk." I mean, is it up to the Members to decide what is official and what is not? If we wanted to save our records for our offices, we pretty much make that determination?

Ms. MELVIN. That is one of the critical issues that we point to in the statement that I provided to you today. From the stand of email in particular, there are numerous challenges relative to the complexity, relative to the content, the context of the email messages.

And this is in light or around the context that historically getting users to really be responsible for records management is a difficult task, so you are compounding that by asking them to identify specific emails that may be a record or non-record. It is still a challenge; it is one of those that we point out is very critical for agencies to have to make a determination as a part of their records management programs how in fact they are going to define what

a record is, what an email record is, and how they will categorize that information versus personal or non-record information. It is a very difficult task.

Mr. CLAY. Anyone else on the panel have any suggestions? Mr. Wennergren.

Mr. WENNERGREN. Well, sir, I don't know if I have a suggestion, but you have hit upon one of the crucial challenges as you move to this electronic records management world, that, in the old days you wrote a letter and you had somebody who was the correspondence clerk, and they knew to archive that letter.

But, indeed, now everyone from our junior enlisted personnel to our senior admirals and generals, you have to decide you are creating a record and then make sure that the email from your wife is deleted and the email that is a record is saved.

So, again, one of the things that we all need to work on together is making sure that the electronic tools that are available take advantage of metadata and things like that to try to help make those decisions for you so the user isn't stuck trying to make those decisions on their own.

Mr. CLAY. I see. I see. Thank you very much.

Let me thank the panel of witnesses for their testimony today. This panel is dismissed. Thank you.

I would now like to introduce our second panel. Even though none of the witnesses are Maryland Terps, we welcome them to this hearing. [Laughter.]

Our first witness will be Dr. Gregory Hunter, a professor at the Palmer School of Library and Information Science at Long Island University, C.W. Post Campus. He is director of the Certificate Program in Archives and Records Management at LIU. He received his Ph.D. in American History from New York University and is a Certified Records Manager and Certified Archivist. Welcome to the committee.

Our next witness is Ms. Carol Brock, here today representing ARMA International. Ms. Brock is a certified records manager with 23 years experience. In 2007, with Ms. Brock's leadership, GAO earned the Archivist Achievement Award. She is currently pursuing her Ph.D. in digital preservation and information policy at the University of Texas at Austin.

After Ms. Brock we will hear from Ms. Anne Weismann, chief counsel for Citizens for Ethics and Responsibility in Washington. Ms. Weismann works extensively on access to Federal electronic records, as well as transparency in government. She previously served as Deputy Chief of the Enforcement Bureau at the Federal Communications Commission and as an Assistant Branch Director at the Department of Justice.

I thank all of our witnesses for appearing today and look forward to their testimony.

Of course, it is the policy of the subcommittee to swear you in. Would you please rise and raise your right hands?

[Witnesses sworn.]

Mr. CLAY. Thank you. You may be seated.

Let the record reflect that the witnesses answered in the affirmative.

I ask that each witness now give a brief summary of their testimony. Please limit your summary to 5 minutes. Your complete written statement will be included in the hearing record.

Dr. Hunter, please begin with your opening statement.

STATEMENTS OF GREGORY S. HUNTER, ASSOCIATE PROFESSOR OF LIBRARY AND INFORMATION SCIENCE, LONG ISLAND UNIVERSITY, C.W. POST CAMPUS; CAROL BROCK, CERTIFIED RECORDS MANAGER, REPRESENTING ARMA INTERNATIONAL; AND ANNE WEISMANN, CHIEF COUNSEL, CITIZENS FOR ETHICS AND RESPONSIBILITY IN WASHINGTON

STATEMENT OF GREGORY S. HUNTER

Dr. HUNTER. Chairman Clay, Ranking Member McHenry, and members of the subcommittee, I do want to thank you for giving me the opportunity to testify today. The only thing that I would add to my background that you did mention is that, in addition to my university work, I did have a career as a working records manager; I was manager of corporate records for ITT World Headquarters, and before that I was archivist for the United Negro College Fund. So I come by my teaching this honestly, having done it for many years, and I continue to consult for government and organizations in this area as well.

We did hear, with the previous panel, about the status of electronic records management. I didn't think I would be able to add anything to what we had just heard. I thought I could perhaps add to the committee's deliberations by talking a bit about some best practices from the private sector, from my experience in my 30-year career that may be applicable to some of the issues that the subcommittee is wrestling with.

In my written testimony there were several areas that I discussed at length. Today I am just going to highlight briefly a couple of those areas for you.

The first area deals with the definition of a record. The GAO reports that were mentioned previously have one theme in common: that the agencies are spending a great deal of time sorting out what is a record from a non-record. And your example with the BlackBerry is relevant as well to this. This consumes a great deal of agency time and there is a reason for this, certainly: the records have to be managed according to Federal requirements; whereas the non-records don't maintain that burden.

What I want to suggest is that, in the private sector, what I believe people are moving toward is less of a focus on record or non-record. In the world of electronic discovery, electronically stored information is what is discoverable, not record or non-record; and the definition of a Federal record certainly is in law now. But the subcommittee may want to begin at the very beginning, perhaps, in its deliberations and decide whether or not the existing definition of record and non-record, legacies from the 1950's, really are fruitful for our current discussion.

In the private sector, organizations will define much more as record. Many of those records have short-term value, but by defining them in that way we spend less time sorting out record from

non-record and we spend much more time trying to manage those resources efficiently.

So the first area in the written testimony talks about record versus non-record.

The second area is the status of records management. And if people don't understand what a record is, certainly there will be difficulty having them understand what records management is and why they should care about that. In the written testimony, I spend some length talking about pushing responsibility for records management down within the hierarchy. Records management has to be seen as something helping someone's business processes. It has to be seen as something that is worth doing because it assists the agencies, not just because there is a requirement for that.

So making records management emphasizing the customer service aspect of it, pushing responsibility down the organizational chain. I know we are dealing with big problems, $80 billion worth of budget and electronic tools to help solve this. But this still ultimately is a people profession and a people problem, and pushing that responsibility down the chain, making managers, not just the agency heads, but front-line managers, responsible for the implementation of records management policies and procedures.

In the private sector that is done through the human resources structure, making certain that records management responsibilities are detailed in your job description, that you are accountable for it, that you are reviewed on that. So I do recommend both for managerial responsibility and records liaisons that NARA and agency staff look at ways to push that responsibility down.

One last thing that I would like to talk about just a bit, because I know compliance is a concern and has been a concern in the previous panel. I would like to talk a little bit about compliance and, again, talk about a private sector model. The private sector model is that the most successful records management programs within corporations are working with the people in the organizations responsible for compliance. They are partnering in the corporate world the compliance departments that were established after Sarbanes-Oxley, in particular.

In the university settings, this is working with internal audit. And I do want to point out to the committee that one of the best models of this is a project done by Indiana University. Under funding from the National Historical Publications and Records Commission, they did establish guidelines for working with internal audit to the success of both parties.

So let me conclude with just a couple of remarks.

Technology has a way of bringing issues to the fore, and as I was preparing this testimony I was rereading a report from 1906 about new technologies and agency responses to that. Agency managers were concerned about efficiency; legal counsel was concerned about evidence. What was interesting to me, though, was that the report was from 1906; from 1906, not 2006. The report was by a group called the Keep Commission, and they were very concerned about Federal agencies implementing the change from the older technology of letter press books to the brand new technology of carbon paper. So the issue sounded strangely familiar to me and maybe

in 2106 your successor will be here with a slightly different twist on this.

But you will see in the written testimony I talk much more about private solutions, and I believe that this kind of dialog, public-private discussions will lead to some of the best practices, and we hope that, as citizens, that it will help Federal agencies as well as private sector organizations.

Thank you, Mr. Chairman.

[The prepared statement of Dr. Hunter follows:]

TESTIMONY OF

GREGORY S. HUNTER, PH.D., CA, CRM

PALMER SCHOOL OF LIBRARY AND INFORMATION SCIENCE

LONG ISLAND UNIVERSITY

BEFORE THE

INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES SUBCOMMITTEE

OF THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

ON

"FEDERAL ELECTRONIC RECORDS MANAGEMENT: A STATUS REPORT"

JUNE 17, 2010

Chairman Clay, Ranking Member McHenry, and Members of the Subcommittee, I am Gregory Hunter, a Professor in the Palmer School of Library and Information Science, Long Island University. Thank you for giving me the opportunity to appear before you to discuss the status of federal electronic records management.

I have over 30 years experience in the profession and am both a Certified Records Manager and a Certified Archivist. At Long Island University, I am a full-time faculty member, Director of the Certificate Program in Archives and Records Management, and Director of the Ph.D. Program in Information Studies. Before joining Long Island University in 1990, I was Manager of Corporate Records at ITT Corporation World Headquarters and Director of Archival Programs for the United Negro College Fund, Inc. In addition to my teaching and other university responsibilities, I have served as a consultant to governments at all levels, multinational corporations, and major not-for-profit institutions.

There have been several reports in recent years about the state of federal electronic records management, including testimony by and reports from the Government Accountability Office to this Subcommittee.[1] These reports have outlined the challenges federal agencies face, especially with the management of e-mail. The reports also detailed the challenges faced by the National Archives and Records Administration in ensuring the consistent implementation of records

---

[1] "Federal Records: National Archives and Selected Agencies Need to Strengthen E-Mail Management," June 2008. "Federal Records: Agencies Face Challenges in Managing E-Mail," April 23, 2008. "Electronic Records: Management and Preservation Pose Challenges," July 8, 2003. "Information Management: Challenges in Managing and Preserving Electronic Records," June 2002.

management policies and procedures across the federal government. Rather than repeat these challenges today, I believe I can best assist the Subcommittee in its deliberations by discussing a number of best practices from the private sector which I believe can be applied with success to the federal environment.

Therefore, I will discuss the following seven areas:

1. Definition of a record
2. Status of records management
3. Managerial accountability
4. Role of records liaisons
5. Simplification of processes
6. Strategic partnerships
7. Assuring compliance

1. Definition of a Record

The GAO reports I mentioned previously have one theme in common. Agencies are spending a great deal of time, effort, and money trying to separate "records" from "non-records" in the digital environment. This especially is the case with e-mail systems and Web sites.

The reason for this agency effort is simple: "records" must be managed in a way that complies with federal law, while "non-records" bear no such burden. Non-records (such as multiple copies of publications and drafts and working papers) are outside the purview of NARA.

It was relatively easy to separate records from non-records in a paper environment. This is not the case with digital records. In fact, discovery rules call for the production of "electronically stored information" – status as a record is not a factor in discovery.

When I work with private sector organizations, I discourage creating a category of "non-record." Rather, I recommend defining *all* evidence of activity, even the drafts and working papers, as "records." Some of these records, of course, will have very short retention periods – but none of the records are outside the purview of the records management program.

Carol Choksky discusses this in greater depth in her book, *Domesticating Information*[2]. She takes particular exception to the common practice with document management systems of "declaring" something to be a record and only managing it from that point forward. Much business activity is documented by items not yet officially declared as records.

Therefore I ask the committee to "start at the very beginning," as they say in the *Sound of Music*, by not assuming that the federal definitions of "record" and "non-record," legacies from the 1950s, still are adequate or desirable. This is a case where I believe that private sector definitions are worthy of examination.

---

[2] Carol E.B. Choksy, *Domesticating Information: Managing Documents Inside the Organization* (Lanham, MD: Scarecrow Press, 2006)

2. Status of Records Management

If people have difficulty understanding what we mean by a "record," it should come as no surprise that they do not value "records management."

An anonymous records manager is quoted as saying: "Records management is like elevator maintenance. It's not noticed until it's gone or something goes wrong."[3] This view is probably more common than we would like to admit.

So how do we raise the status of records management in the federal government? How do we increase familiarity with and commitment to records management policies and procedures?

The private sector faces the same issue. One approach involves "leadership alignment," cultivating senior executives to serve as advocates for records management. There is no substitute for a visible and committed executive champion.

Executive champions, however, only go so far. Records management increases in status when it helps people do their jobs better. This is far from a quick fix. Records managers must focus on external "customer" needs – with a customer being anyone that we serve – rather than internal records management processes.

In effect, records management must become a customer service profession. We must begin by understanding our customer's business processes and the ways that records management principles can help them do their jobs better.

Though I may not want records management equated with elevator *maintenance*, the elevator itself may be an appropriate metaphor. Records management is a means to an end. It gets us from one place to another. We must never let it become a bureaucratic end in itself.

3. Managerial Accountability

Ultimately, records management increases in status when it meets the needs of front-line managers in an organization.

In the private sector, I always stress that records management is a "line" rather than a "staff" responsibility. No government or other organization can afford to hire enough staff people to "do" records management for everyone else.

Front-line managers are responsible for records in the same way that they are responsible for other organization assets. Records management policies and procedures are designed to help front-line managers discharge their primary responsibilities – as noted above, this is the business case for the "value" of records management. Records management policies and procedures

---

[3] For example, see: www.doa.state.wi.us/docview.asp?docid=6549&locid=0

should not be seen as a burden; rather, they should be seen as a tool to save money and increase efficiency.

Best practices in this area involve tying records management into the structures of managerial accountability. This can be done in a number of ways:

- Include records management activities in position descriptions
- Require records management goals in annual plans
- Assess performance against goals during annual personnel reviews

The point is that departmental managers, not lower level employees, need to be evaluated for their commitment to and implementation of records management policies and procedures. Making the evaluation part of the annual performance review is the best way to institutionalize this practice.

4. Role of Records Liaisons

One of the most visible examples of front-line management support – or its lack – is the choice of a department or unit "records liaison." It is common in the private and public sectors to decentralize records management through a network of records liaisons. The choice of and support for these individuals is crucial to the success of a records management program.

I have known many excellent records liaisons, dedicated staff members who have the full support of their department heads. I have known others, however, who were the wrong person, in the wrong job, at the wrong time. How do we encourage the former and discourage the latter?

Everything I have discussed to this point certainly will help: visible evidence of executive support; clear definitions, policies and procedures; and the commitment of the liaison's immediate supervisor.

The key, however, is to formalize the role of records liaison in the human resources structure. The records liaison is essential for the success of front-line records management. The liaison's responsibilities should be included in the employee's position description, and the annual performance review should include an assessment of the employee's achievement of records management as well as other goals. In this way records liaisons who take their responsibilities seriously are acknowledged for their contribution to the success of the program.

5. Simplification of Processes

As noted above, successful records management programs need to focus more on customer business needs and less on bureaucratic processes. To use Peter Drucker's terms, we need to be "effective" rather than just "efficient."[4] This is even more important with digital records.

---

[4] Peter F. Drucker, *The Effective Executive* (New York: Harper, 1967)

The previously-mentioned GAO reports comment on the volume and complexity of digital records. One might think that records management processes need to be more complex to manage these complex records.

I would like to argue just the opposite. If we keep the same-old processes, we will never be able to manage the volume and complexity of digital records. Organizations, including the federal government, must use the challenge of digital records to simplify radically existing records management processes.

There have been some promising steps, such as the use of "big bucket" or "flexible" schedules and the implementation of "media-neutral" schedules. Nevertheless, government processes remain much more complex than their private-sector counterparts.

Mark Greene and Dennis Meissner have written that archivists need "more product" and "less process."[5] I believe this also is the case with records management, especially in the government context.

In particular, I think we need to take a hard look at our approach to information "systems." We must simplify the way we inventory and schedule the records in these systems. We do not have the resources to analyze all information systems in the same time-consuming way. NARA staff and federal agencies must work together to develop effective strategies that consume fewer staff resources.

6. Strategic Partnerships

One way to be effective is to work with the right people. The most successful private-sector records management programs are based upon strong partnerships. Records Management seldom has the clout to succeed alone.

The General Counsel or Legal Department is one of the key strategic partners. From developing records retention schedules to complying with discovery requests, Legal and Records Management must have a close relationship.

Since September 11, 2001, Business Continuity Planning is another logical partner. This especially is the case with digital records. A records inventory, conducted to develop records retention schedules, also can identify "vital records" – those necessary to continue operations after a disaster. The Council of State Archivists is involved in a model partnership with the Federal Emergency Management Agency.[6] This and other partnerships should be encouraged.

---

[5] See "More Product, Less Process: Pragmatically Revamping Traditional Processing Approaches to Deal with Late 20th-Century Collections," available at http://ahc.uwyo.edu/documents/faculty/greene/papers/Greene-Meissner.pdf

[6] The project is called "Intergovernmental Preparedness for Essential Records (IPER). See http://statearchivists.org/iper/index.htm

Information Technology (IT) is a third strategic partner. It is virtually impossible to manage digital records without the cooperation of IT. What I have found, however, is that the partnership works both ways. A records management program enables IT to destroy records in the regular course of business with minimal second-guessing after the fact.

I know that at the highest levels, NARA is actively pursuing these and other partnerships. In keeping with records management as a line responsibility, however, the partnerships must be pushed downward within federal agencies. I recommend the preparation of business cases and other document from the perspective of the strategic partner, not the records management professional.

7. Assuring Compliance

Last but certainly not least, how will we assure compliance with records management policies and procedures? This is an area where NARA has been criticized in the past by GAO and others inside and outside of government.

In September 2009, NARA issued a mandatory records management self-assessment to 242 Federal Cabinet Level Agencies and their components, and independent agencies.[7] I am encouraged by NARA's attempt to establish a baseline for assessment of records management in federal agencies. However, the data must be used with caution.

In particular, the agency staff conducting the self-assessment reflect the concerns I've raised previously in this testimony:

- Some agency staff understand and value records management, while others are less knowledgeable
- Executive support and managerial commitment vary greatly
- Strategic partnerships may or may not be in place

The inconsistent responses by agencies highlight these differences and limit the usefulness of the self-assessment results.

But NARA should not abandon agency self-assessment. Rather, the assessments will become even more useful as agency records management programs develop and mature.

Self-assessment, however, will never be enough. NARA must institute a regular and thorough program of monitoring compliance. While NARA can do this on its own, I would like to suggest a best practice from the private sector.

Successful records management programs are establishing strategic partnerships with internal auditors. This reinforces the point that records management is a line responsibility similar to other line responsibilities. Internal auditors monitor compliance with personnel, fiscal, and other organization policies. They do this by conducting scheduled and unscheduled reviews and

---

[7] National Archives and Records Administration, "Records Management Self-Assessment 2009: An Assessment of Records Management Programs in the Federal Government."

reporting their findings to senior executives. Records management compliance should be monitored in the same way.

One model for cooperation with internal audit is offered by the Indiana University Archives, which explored administration of electronic records with funding from the National Historical Publications and Records Commission.[8] The Indiana University Archives assisted Internal Audit with the review of high-risk departments and activities. As with the best partnerships, both Internal Audit and Records Management realized benefits from the cooperation.

Extending this to the Federal level, I prefer that NARA not be the entity conducting compliance reviews. I recommend that NARA partner with entities that conduct regular reviews of compliance with personnel, fiscal, information technology, and other policies. I believe this is the best way to reinforce the line responsibility for records management as well as being the most efficient use of NARA's resources.

Conclusion

New technologies have a way of bringing issues to the surface. I started this testimony by referring to previous reports. I recently was re-reading an '06 report on the effect of new information technologies on federal agency recordkeeping practices. As one would expect, agency managers and executives were concerned about efficiency and changes to their business processes. Legal counsel was concerned about authenticity of documents and admissibility in evidence.

These concerns are not surprising. What is surprising is that the report was from 1906 rather than 2006. One hundred years ago, the Keep Commission was investigating the shift to a new technology – carbon paper – from the older technology of letterpress books.[9] While technology is different today, the issues for federal agencies sound all too familiar.

I would like to thank the Subcommittee for giving me the opportunity to testify on this important issue. I believe that an ongoing public-private dialog and exchange of best practices is one of the best ways to improve the management of records in institutions of all types. I would be happy to answer any questions you may have.

---

[8] See Philip Bantin, "Strategies for Developing Partnerships in Electronic Records," at http://www.libraries.iub.edu/index.php?pageId=3313

[9] This is discussed in JoAnne Yates, *Control Through Communication: The Rise of System in American Management* (Baltimore: Johns Hopkins University Press, 1989), 48-49.

Mr. CLAY. Thank you, Dr. Hunter. Appreciate that analogy from the other century.

Ms. Brock, you may proceed.

STATEMENT OF CAROL BROCK

Ms. BROCK. Thank you, Chairman Clay and members of the subcommittee, for inviting ARMA International to this hearing on Federal electronic records management. I have been a Federal records management professional for 23 years and have served several Federal agencies and worked closely with the National Archives in my role as a Federal records officer. I am an active member of ARMA International, the Association for Information and Image Management, and the Federal Information and Records Managers Council.

We have been producing electronic records since the 1980's, yet we are not adept at managing them. In an effort to better address electronic records management issues, I returned to school a year ago to work on a Ph.D. in digital preservation and information policy. You can understand that this is near and dear to my heart.

The question of the day is: Why are electronic records so difficult to manage? I will address three reasons why. First, managing electronic records inherits all of the traditional records management challenges. Second, managing electronic records is fraught with technology challenges and requires consistent records management competencies. And, third, managing email poses additional challenges.

I also provide some recommendations, including, first, empowering and funding NARA; second, establishing a role for an agency chief records officer; and, third, establishing a principle-based approach to records management.

So what are the traditional records management challenges? There may be no management involvement or expectations. Senior officials do not see records management as a vital agency function. Also, there are no meaningful or sustaining resources. There are limited staff resources to do mission critical work. Agencies no longer have support staff to perform administrative tasks and workloads continue to increase as staff numbers decrease. No staff training or imperatives exist.

Records management awareness requires continuous enterprise-wide training. Still, many Federal agency staff do not see their work product as records and simply do not have time for training. Also, no enterprise-wide guidance or expectations exist. Record status is generally determined at the end-users desktop. Staff mingle personal materials with their business records.

What are the technology challenges associated with managing electronic records? Technology is not a constant; principles are constant. Electronic media obsolescence is a well known issue. If technology is not reliable, let's employ generally accepted recordkeeping principles. More records does not equal better recordkeeping. Popular wisdom is to save everything because storage is cheap. This perception overlooks the cost of staff searching for information to do their jobs, as well as the cost of fulfilling FOIA, privacy, and discovery requests.

Also, records management must be consistent across the enterprise. Agency staff are as wired as everyone else. Staff are storing records on hard drive, thumb drives, home computer systems, and in the cloud, all of which are outside of an agency's centralized span of control.

Finally, what are some additional challenges associated with managing email? Staff use email for personal productivity, to manage their projects, store their drafts and reference materials, find their records and track their work. Used in these ways, email may never make it into the agency's official recordkeeping systems. Identifying records is not as easy as creating email; an email capture can be complicated.

So what we can do, we can confirm our benchmarks: the National Archives guidance, the ISO standards on information and documentation, and the generally accepted recordkeeping principles. Also, we can create expectations and public policy outcomes. What is needed is a commitment to create, manage, and grow a compliant records management program. If Congress declares agency records management a priority and links agency budgets to compliance, we will see results.

Consider establishing chief records officers in each and every agency. And I can say more on that later. We can give NARA greater visibility and authority, insisting on proven agency compliance with scheduling, dispositions, and effective management of electronic information assets. My perception is that NARA does not have the authority to fulfill their recordkeeping mission.

And, finally, we can integrate enduring records management principles into the operations of every Federal agency. An agency should establish a recordkeeping program that is overseen by senior executives; informed by clear policies and procedures to train and guide personnel; and is transparent through documentation available to all personnel, interested parties, and regulatory and enforcement bodies. And I have a copy of the principles and detailed maturity model, if anyone would care to see it.

Thank you again for this opportunity to comment. I look forward to answering your questions.

[The prepared statement of Ms. Brock follows:]

Testimony of Carol Brock[i], Certified Records Manager
On Behalf of ARMA International
Before the
Subcommittee on Information Policy, Census, and National Archives of the
House Committee on Oversight and Government Reform
On "Federal Electronic Records Management: A Status Report"
June 17, 2010

Thank you, Chairman Clay and members of the Subcommittee, for inviting me to participate in this hearing on Federal Electronic Records Management.

INTRODUCTION

ARMA International (www.arma.org) is the professional association for records and information managers and has served as the source of principles, standards, and best practices for records management. Formed in 1955, ARMA International is the oldest and largest association for the records and information management profession and is known worldwide for setting records and information management (RIM) standards and best practices, and for providing comprehensive education, publications, and information on the efficient maintenance, retrieval, and preservation of information created in public and private organizations in all sectors of the economy.

ARMA has recently developed a principles-based approach to records management – emphasizing with generally accepted recordkeeping principles[ii] the commitment required enterprise-wide and the essential outcomes of any records management program.

With this testimony, I employ my 23 years of professional experience as a records manager and my knowledge of principles, standards and best practices that can guide organizations to develop and deploy effective records management programs.

WHY ARE ELECTRONIC RECORDS DIFFICULT TO MANAGE?

1. Managing electronic records inherits all of the traditional records management challenges.

- NO MANAGEMENT INVOLVEMENT OR EXPECTATIONS. Senior officials do not see records management as a vital agency function. Agency management may understand that the National Archives may report them to Congress for lack of compliance but it is generally understood that Congress will empathize with the agency's mission priorities which do not assign records a priority status.

- NO MEANINGFUL OR SUSTAINING RESOURCES. There are limited staff resources to do mission-critical work. Agencies no longer have support staff to perform administrative tasks and workloads continue to increase as staff numbers decrease. This produces a non-compliant culture of "it is not my job"; "it is a burden"; "let the technology do it". Even staff who understand their records responsibilities have little time to devote to the task. ARMA sees technology as a tool – an increasingly necessary tool; however, we believe that the devolution of

records management to information technology is a strategic error and misses the necessary human component.

- NO STAFF TIME OR IMPERATIVES. Record management awareness requires continuous enterprise-wide training. Still, many federal agency staff – 1) do not see their work product as records, 2) have higher training priorities relative to their business or mission functions, and/or 3) simply do not have time for training.

- NO ENTERPRISE-WIDE GUIDANCE OR EXPECTATIONS. Record status is generally determined at the end-user's desktop; therefore, accurate record classifications are essential to the integrity of an agency's records management program. And despite many high profile cases featuring public embarrassment, staff continues to mingle personal materials with their business records.

- PLAIN ENGLISH FOR RECORDS MANAGEMENT. The Federal definition of a record makes sense only to archivists, records managers, and a few attorneys. What is a draft versus a version? Which is a record? What to do with each and when? – All are issues which continue to plague agency staff. The definition of a Federal record needs to be updated to reflect how business is conducted electronically, i.e. a record (information asset) is evidence documenting decisions, activities, and the business of the organization. A simplified and easily understood definition would streamline training and enhance the staff's ability to understand what is required of them. We need a plain English initiative for records management.

- MANAGING RECORDS EQUALS TRANSPARENCY AND ACCOUNTABILITY FOR A DEMOCRATIC SOCIETY. An agency must manage all of its information assets, regardless of record status, in order to support the agency's mission and business processes, and in order to respond effectively to Freedom of Information Act (FOIA), privacy, and discovery requests. Requests for information under FOIA, Privacy, or discovery are not subject to the "official record" limitations in document production so an agency must manage all of its evidence in order to be responsive. For those agencies using National Security Classified materials, separate classified and unclassified systems are required which simply multiplies the records management challenges. The current expectations of transparency and accountability call out for a principles-based approach to records management – and presents an opportunity for managing our electronic records in a manner that gives the general public a higher level of confidence in the integrity, availability, and safety of our vital records.

- WHY NOT A CHIEF RECORDS OFFICER? Records managers traditionally do not have the authority to accompany the responsibility nor the tools or staff to perform the mission assigned. What about creating Chief Records Officers? This is a role that should be isolated from the role of IT but that should be responsible for assisting the Chief Information Officers understand their responsibility for the records as well as the technology and include records management with general counsel and the inspector generals at the systems development table so all information management requirements are addressed. Is it time to consider a Chief Records Officer in each federal agency? When will we empower the function and enable the competencies of records and information management?

2. Managing electronic records is fraught with technology challenges and requires consistent records management competencies.

- TECHNOLOGY IS NOT A CONSTANT; PRINCIPLES CAN BE. Electronic media obsolescence is a well-known issue. Technology upgrades affect the ability to access evidence produced in earlier generations of applications. Proposed solutions involve emulation, migration, or preservation of the original systems (which would make every agency a computer hardware and software museum). If technology is not a reliable constant, there is a role for processes and procedures based on generally accepted principles for recordkeeping.

- MORE RECORDS DOES NOT EQUAL BETTER RECORDKEEPING. Popular wisdom is to save everything because storage is cheap. This perception overlooks the costs of staff searching for information to do their jobs as well as the costs of fulfilling FOIA, Privacy, and discovery requests.

- THERE IS NO MAGIC WAND OF TECHNOLOGY. Vendors tout recordkeeping applications as "plug and play" but in actually they must be designed to capture the evidence of an agency's business processes. Most recent policy initiatives focus on investments in technology. Introducing electronic records management generally involves introducing electronic workflow processes to an agency, with the associated changes and streamlining of processes. New technology and process changes may produce angst in staff, particularly if an application is not intuitive or easy to use. New and emerging technologies are all the more reason to create recordkeeping programs based on constant and measurable principles.

- PROPERLY DOCUMENTING RECORDS IS NOT EASY. Electronic records management requires metadata to be associated with every record in order to establish the context for the content of that record. It may be user assigned or system generated metadata, but it must include business purpose classification in order for the systems to produce authentic records.

- RECORDS MANAGEMENT MUST BE CONSISTENT ACROSS THE ENTERPRISE. Agency staff are as wired as everyone else. They are using personal computing systems, personal e-mail accounts, instant messaging, and twitter to accomplish their work. Staff are storing records on hard drives, thumb drives, home computer systems, and in the cloud: all of which are outside of an agency's centralized span of control. Most agencies do not yet have policies or processes to deal with these issues. Our failure to capture these records into an agency's recordkeeping system poses an on-going risk.

- ARCHIVING RECORDS CREATES ADDITIONAL ISSUES. NARA accessions only limited formats of electronic records. Agencies use the tools that best fit their business requirements; which are not necessarily those that produce archival quality records. The agencies responsibility is to provide NARA with permanent records which are produced in the normal course of business – migrating to a different format for the purposes of archiving records is an additional cost.

3. Managing e-mail poses additional challenges.

- POLICIES AND PROCEDURES SHOULD DRIVE RECORDS MANAGEMENT – NOT TECHNOLOGIES OR CONVENIENCE. Staff use e-mail to manage their projects, store their drafts and reference materials, find their records, and track their work. Used in these ways, e-mail may not make it into the agencies official recordkeeping systems. To compound the problem, information technology staff often insist on automatic deletion policies in order to control the size of staff mail boxes and the subsequent costs of storage. To avoid losing e-mail, staff often archive their e-mail files to their hard-drives or portable storage devices, which circumvents centralized agency recordkeeping systems.

- IDENTIFYING RECORDS IS NOT AS EASY AS CREATING EMAIL. E-mail capture can be complicated because the recordkeeping system must capture the transmission data, distribution lists, messages, and any and all attachments. Unless the e-mail system is fully integrated with the recordkeeping system, this process will involve multiple steps. If the user is managing threaded e-mail (discussion carried on through successive e-mail messages which are then brought together to record the message in its entirety); the process becomes more complicated.

WHAT CAN WE DO?

1. Confirm our benchmarks. We have the Federal Records Act, National Archives guidance, ARMA International's Generally Accepted Recordkeeping Principles, and ISO Standards 15489-1 and 2 (Information and documentation – Records Management – Part 1 General and Part 2 Guidelines) to inform us of what must be done.

2. Create expectations and public policy outcomes. What is needed is a commitment from each Federal agency to create, manage, and grow a compliant records management program. This commitment of resources, in this time of fiscal austerity, will only happen if Congressional pressure is applied. This top-tier pressure must be accompanied by demands for accountability: measurable results monitored by the National Archives and the Office of Management and Budget against the standards. If Congress declares agency recordkeeping and information management a priority, and links agency budgets to compliance as is done with information technology project spending, we will see results. Require that all agency systems either contain full records management functionality within their application or feed directly into an agency-wide electronic recordkeeping system.

3. Promote more NARA visibility. NARA might be more visible in proactive leadership on agency recordkeeping initiatives: insisting on proven agency compliance with scheduling, dispositions, and effective management of electronic information assets. The Records Management community looks to the National Archives for leadership and advocacy in this realm. Providing assistance with creating information management strategies, electronic tools, and integrating systems would demonstrate NARA's commitment to other Federal agencies. NARA could challenge the Chief Information Officer's Council (CIO) or individual CIOs to build demonstration systems: have a contest to judge the most elegant, fully integrated, transparent, and user-friendly (defined as applying as many automated tools as possible to reduce the burden on agency staff) recordkeeping system possible. Appoint a group of FOIA and Privacy Officers accompanied by attorneys, records managers, inspector generals, and contract auditors to be the judges of the functionality of these demonstration projects. I would love to see my tax dollars applied to a CIO's bonus for that kind of effort.

4. Integrate enduring records management principles into the operations of every Federal agency.
Generally accepted recordkeeping principles speak to *accountability, transparency,* and *compliance* by the enterprise and *integrity, protection, availability, retention* and *disposition* of records and information. These principles create a foundation for an appropriate and effective recordkeeping program that speaks to enterprise-wide commitments and life cycle management of records and information. With these principles –

a. The enterprise would establish a recordkeeping program that (1) is overseen by a senior executive, (2) is informed by clear policies and procedures to train and guide personnel, (3) is auditable, and (4) is transparent through documentation in an understandable manner and available to all personnel and appropriate interested parties, including the appropriate regulatory and enforcement bodies.

b. The recordkeeping program would be constructed to ensure that (1) the records and information have a reasonable guarantee of authenticity and reliability, (2) there is an appropriate level of protection for records and information that are private, confidential, privileged, or in the case of this inquiry, personal information, (3) records and information are maintained to ensure timely, efficient, and accurate retrieval, (4) records and information are maintained for the appropriate or required period of time, and (5) disposition of records and information will be accomplished in an appropriate manner and in the appropriate or required time, and such disposition is documented.

5. Provide NARA with sufficient statutory authority. My perception is that NARA does <u>not</u> have the authority to fulfill their recordkeeping mission. Many staff in the Federal government perceive the Archives as having an unfunded mandate with no enforcement teeth. To records management practitioners, the Archives also appear to be understaffed in key components: they need more technical leadership, expert records management staff dedicated to solving information management issues with agency Record Managers, and system architects who can assist agencies in capturing their records within their business processes.

Thank you again for this opportunity and I look forward to answering your questions.

---

[i] Carol Brock is a Certified Records Manager with 23 years experience working on records and information management challenges for the Federal government. She has worked with ARMA International (Association of Records Managers and Administrators) and the Association for Information and Image Management on a variety of issues and standards. She is a founding member of the Federal Information and Records Managers (FIRM) Council. In 2007, with Carol's leadership, GAO earned the Archivist's Achievement Award for their successful work on simplified retention schedules (the big bucket theory) and the implementation of an enterprise-wide electronic records management system. She is the coauthor of <u>Guideline for Managing E-Mail,</u> ARMA, Prairie Village, KS, 2000 and <u>Framework for the Integration of Electronic Document Management Systems and Electronic Records Management Systems</u>, AIIM's C-30 Committee: ANSI/AIIM Technical Report 48-2004. Revised and updated in 2007. She has served as a stakeholder in numerous GAO reports, including GAO-08-742: Federal Records -

National Archvies and Selected Agencies Need to Strengthen E-Mail Management at
http://www.gao.gov/new.items/d08742.pdf.

ii GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES

Principle of Accountability

An organization shall assign a senior executive who will oversee a recordkeeping program and delegate
program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and
ensure program auditability.

Principle of Integrity

A recordkeeping program shall be constructed so the records and information generated or managed by
or for the organization have a reasonable and suitable guarantee of authenticity and reliability.

Principle of Protection

A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and
information that are private, confidential, privileged, secret, or essential to business continuity.

Principle of Compliance

The recordkeeping program shall be constructed to comply with applicable laws and other binding
authorities, as well as the organization's policies.

Principle of Availability

An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval
of needed information.

Principle of Retention

An organization shall maintain its records and information for an appropriate time, taking into account
legal, regulatory, fiscal, operational, and historical requirements.

Principle of Disposition

An organization shall provide secure and appropriate disposition for records that are no longer required
to be maintained by applicable laws and the organization's policies.

Principle of Transparency

The processes and activities of an organization's recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.

WHAT ARE THEY?

o   A common language describing the tenets of valid recordkeeping

o   A measurable, predictive, and empirically-based basis for recordkeeping

WHY?

o   Builds confidence in the market place and among the general public

o   Creates assurances and transparency for regulators, enforcement agencies, and policymakers

o   Establishes an auditable process, and thereby accountability

WHO?

o   Policymakers – to protect the public by assuring access to information about the operations, policies, and procedures of regulated activities and entities

o   Governmental Agencies – to preserve the integrity of records and information, to document and oversee the use of public funds and resources

o   Business – to document and make available information for regulators, business partners, and general public, as appropriate or required

RESULTS

o   Document the use and investment of public funds

o   Provide appropriate oversight of regulated activities and entities

o   Support informed enforcement actions, as well as legislative and regulatory actions

o   Protect sensitive, proprietary and personally identifiable information

Mr. CLAY. Thank you so much, Ms. Brock, for your testimony. Ms. Weismann, you may proceed for 5 minutes.

STATEMENT OF ANNE WEISMANN

Ms. WEISMANN. Mr. Chairman and Ranking Member McHenry, thank you for the opportunity to testify before you today about the status of Federal electronic records management. I last testified before this committee in December 2009 on the priorities and roles NARA and new Archivist David Ferriero should adopt. My testimony highlighted the dismal state of electronic recordkeeping at that time across nearly all agencies in the Federal Government. Unfortunately, the situation has not improved in the intervening 6 months.

Two years ago, after conducting an online survey submitted to more than 400 agency records managers, my organization, CREW, reported that the vast majority of agencies failed to take advantage of existing technology to preserve their electronic records, and that even knowledgeable agency employees lacked the basic understanding of their recordkeeping response obligations.

NARA's more recent self-assessments confirm these results and reveal, as we have heard today, the extremely troubling statistic that 79 percent of agencies face a moderate or high risk of improperly destroying their records.

Examples abound of the widespread problems within the Federal Government in managing and preserving its electronic records. Our litigation against the Executive Office of the President and NARA brought to light a wealth of evidence of the continuing and systemic failure of the Bush White House to preserve and manage its emails.

In a recently released report, EOP documented the fact the Bush White House archiving system failed to capture 89.4 percent of the universe of known emails for 21 non-consecutive days. That a President failed to preserve nearly 90 percent of some of the most valuable historical documents is both shocking and completely unacceptable.

As a frequent requester under the FOIA, CREW often confronts an agency's inability to locate responsive email records. The Veterans Affairs, for example, recently explained to us its failure to locate a key email was due to the practice of the agency to store its emails on backup tapes that periodically were recycled, even in the face of a pending FOIA request or FOIA lawsuit.

While these persistent problems present great challenges, we believe Congress can provide a solution through legislative amendments to the Federal Records Act and the Presidential Records Act, and my written testimony outlines some of our proposals in that regard.

But I would note that the Federal Records Act carves out an enforcement role for the Attorney General, but gives the Archivist no sway over whether and how the Attorney General exercises that authority. And I think the Department of Justice's handling of the apparently missing emails of former OLC Official John Yoo illustrates the problem with the existing statutory scheme. In July 2009, the Office of Professional Responsibility issued a report of its investigation into the role Mr. Yoo played in the development of

the so-called torture memos. That report, made public in February of this year, notes explicitly the investigation was hampered by the disappearance of all of Mr. Yoo's emails.

Almost immediately NARA asked DOJ to investigate and report back to it, and CREW sent a letter to Attorney General Holder also requesting an investigation. Four months later, DOJ has yet to respond to either request, and the public and Congress are no closer to learning the truth about how and why emails central to an investigation of critical public importance are missing.

Clearly, there is something wrong with a law that says the public must sit by idly while agency heads, including the Attorney General, refuse to act.

Nearly 20 years ago, while an attorney at the Department of Justice, I engaged in a vigorous internal debate over whether email was even a record that had to be preserved with all of its metadata. Today this issue is long settled as a matter of law. But as a matter of practice, agencies continue to treat emails as readily discardable, even while their value has grown exponentially.

Just look at the currency Elena Kagan's Federal and Presidential electronic records have as Congress evaluates her nomination for the Supreme Court. Simply stated, emails are the gold we mine for an answer to questions that perplex and worry us, or the truth behind an administration's or agency's controversial decisions and actions. Yet, we fail to handle these treasures with care. Congress must act to ensure our past will be available for future generations to study and learn from.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Weismann follows:]

Statement of
Anne L. Weismann
Citizens for Responsibility and Ethics in Washington

Before the
Information, Policy, Census, and National Archives Subcommittee
of the Committee on Oversight and Government Reform

"Federal Electronic Records Management: A Status Report"

June 17, 2010

Mr. Chairman, Ranking Member McHenry, and Members of the Subcommittee, thank you for the opportunity to testify today about the status of federal electronic records management. I last testified before this Committee in December 2009 on the priorities and roles the National Archives and Records Administration (NARA) and Archivist David S. Ferriero should adopt. My testimony highlighted the dismal state of electronic record keeping at that time across nearly all agencies in the federal government. Unfortunately, the situation has not improved in the intervening six months.

By way of background, I am Chief Counsel for Citizens for Responsibility and Ethics in Washington (CREW), a non-profit, non-partisan organization dedicated to bringing transparency and accountability to our government and government officials. CREW has worked tirelessly over the years to highlight the importance of proper records preservation and management, functions that lie at the heart of achieving these principles. I am pleased to participate in this tremendously important hearing and to speak about a topic that has animated so much of my work over the past few years: how to improve electronic records management in the federal government.

Two years ago, through an on-line survey submitted to more than 400 agency records managers, CREW investigated how agencies of the federal government preserve their electronic records. Our April 2008 report, *Record Chaos: The Deplorable State of Electronic Record Keeping in the Federal Government*, discloses some very disturbing findings. The vast majority of agencies fail to take advantage of existing technology to preserve their electronic records, and instead treat electronic records like paper records by following a print-and-save policy. Responses to the survey confirmed that even knowledgeable agency employees lack a basic understanding of their record keeping obligations and how they can be satisfied. This lack of understanding correlated directly to a lack of compliance with record keeping obligations.

More recently, NARA required all federal agencies to complete self-assessments of their records management programs. According to those assessments, released publicly in April 2010, 79 percent of agencies, including the White House's own Office of Administration, face a high or moderate risk of improperly destroying their records. Archivist David Ferriero decried this risk as "unacceptable."[1] Further, 39 percent of agencies fail to conduct periodic internal evaluations of their records management practices, and nearly a quarter of agencies lack a policy for managing email records. Problems persist even among those agencies claiming to have email policies; 22 percent omit any explanation of how to manage email in an electronic mail system. As the archivist explained, these failures prevent the government from meeting its business needs, impede accountability, and place in peril the availability of permanently valuable records to future generations. *Id.*

Unfortunately, examples abound of the widespread problems within the federal government in managing and preserving its electronic records. Litigation by CREW and the National Security Archive against the Executive Office of the President and NARA brought to light a wealth of evidence of the continuing and systemic failure of the Bush White House to

---

[1] His remarks are found at http://blogs.archives.gov/aotus/?p=186.

preserve and manage its electronic records. Although the Bush administration possessed much of this evidence for years, it failed to restore the huge number of emails that mysteriously had gone missing from servers in the Bush White House over a critical two and one-half year period, and continually refused to implement an appropriate and effective electronic records management system. Evidence recently provided us by the White House shows that for at least a sampling of 21 non-consecutive days in the Bush administration, the Bush White House archiving system failed to capture 89.4% of the universe of known emails. Those emails would not be available today but for the demand of CREW and the National Security Archive, in settlement of their litigation, that at least some portion of the missing emails be restored.[2] That a president failed to preserve nearly 90 percent of some of his most valuable historic documents is both shocking and completely unacceptable.

Beyond the White House email problem, as a frequent requester under the Freedom of Information Act (FOIA), CREW often confronts an agency's inability to locate responsive email records because the agency lacks an effective method for archiving and searching electronic records. Agencies like the Department of Education have told us they simply have no way of finding emails responsive to our FOIA requests. The U.S. Department of Veterans Affairs attempted to excuse its failure to locate a key email known to exist and clearly responsive to our FOIA request with the explanation the agency stored its emails on backup tapes and had a practice of periodically recycling those tapes. Apparently the email we were seeking, along with any other related and likely relevant emails, was recycled.

These examples coupled with CREW's report, the results of NARA's agency self-assessments, and various GAO reports conducted over the years confirm a fundamental truth: when it comes to managing federal electronic records, we have a huge and growing problem on our hands. Agencies routinely and systematically ignore their clear obligations to preserve electronic records, particularly email. Agency personnel do not even understand what those obligations encompass, and their agencies have done little to educate them. Most agencies have no effective way to manage their email records beyond asking individual employees to print them to paper and save them in paper files.

Left unaddressed, these problems will only worsen, particularly with widespread blackberry use and a growing reliance on new social media, from Facebook to Twitter. Even those agencies with electronic record keeping systems and good record keeping policies are not immune from problems. The current White House, after years of litigation, now employs an electronic record keeping system that works and appears to meet all legal requirements. Nevertheless, a high-ranking and technologically savvy official at the White House's Office of Science and Technology Policy recently was found to have used his private Google account to conduct official business.

---

[2] For the Committee's convenience, the report describing this comparison process and its results is attached as Exhibit A.

These persistent problems present great technological challenges, but are not without solutions. Congress, in particular, has a key role to play through legislative amendments to existing statutes, most particularly the Federal Records Act.

Until quite recently, NARA interpreted its statutory responsibilities under the Federal Records Act very narrowly, refusing to actively oversee and manage agency compliance with that statute. The recently completed agency self-assessments show just how ineffective that approach proved to be: the records at 79 percent of federal agencies are at risk of improper destruction. While the new archivist has attempted to revitalize NARA's role in ensuring agency compliance with record keeping laws and regulations, he remains stymied by a dearth of specific enforcement tools and the statutory authority to compel agencies to do anything, including responding to mandatory self-assessments.

The Federal Records Act carves out an enforcement role for the attorney general, but gives the archivist no sway over whether and how the attorney general exercises that enforcement authority. The current situation involving the apparently missing emails of former Office of Legal Counsel (OLC) Assistant Attorney General John Yoo illustrates what happens when the attorney general refuses to act, even in the face of a request from the archivist. In July 2009, the Department of Justice's Office of Professional Responsibility issued a report detailing the results of its investigation into the roles Mr. Yoo and other top OLC officials played in the development of the so-called "torture memos." That report, which was made public on February 19, 2010, notes explicitly the investigation was hampered by the disappearance of all of Mr. Yoo's emails. Almost immediately, NARA asked the Department of Justice to investigate and report back to it, and CREW sent a letter to Attorney General Holder requesting that he launch an investigation into what appear to be violations of the Federal Records Act by Mr. Yoo and possibly others. Four months later, the Department of Justice has yet to respond to either request, and the public and Congress are no closer to learning the truth about how and why emails central to an investigation of critical public importance are missing.

Clearly there is something wrong with a law that says the public must sit by idly while agency heads -- including the attorney general -- refuse to act when informed important agency records have been destroyed or mysteriously have gone missing. Although the agency head suffers no adverse consequences from his or her inaction, the public suffers the irreparable loss of important records.

Congress should therefore amend the Federal Records Act to give the archivist explicit and expanded oversight and enforcement responsibilities. When presented with evidence suggesting a possible violation of record keeping laws, the archivist should be required to initiate an independent investigation, and should be afforded the power to compel agency cooperation. Upon completion of this investigation, the archivist should report his or her findings to the inspector general of the agency in question and issue public notice of this report. The inspector general, in turn, should be required to conduct a follow-up investigation in all cases where the archivist has identified possible evidence of record keeping violations. At that point the archivist, the attorney general, and the public should be afforded access to the conclusions of the

agency inspector general.

Further, in the event the attorney general decides not to act on any of these findings, Congress should allow greater oversight by expanding private rights of action under the Federal Records Act. Currently, as interpreted by the courts, outside groups like CREW can sue only to trigger the enforcement provisions in the Federal Records Act, which include notice to the archivist and a referral to the attorney general. Where NARA cannot act – such as in the case of an agency that fails to respond to NARA's request for more information – and the attorney general refuses to act – as did Attorney General Michael Mukasey when informed by CREW that millions of federal email records were missing from White House servers – there must be a role for outside groups to compel compliance with the law.

We also urge Congress to carry through with legislation that would require all agencies in the federal government to have in place effective electronic record keeping systems within two years, with fiscal consequences for those agencies that fail to meet this requirement. The Electronic Communications Preservation Act would give agencies four years in which to implement effective electronic records management. But the urgency of the situation has now been confirmed in multiple ways, through multiple studies, assessments, and everyday experiences. Given the current crisis, we cannot afford to wait four years for a solution.

Congress also should amend the Presidential Records Act to give the archivist greater authority and to afford outside groups at least limited private rights of action. Currently the Presidential Records Act contains no enforcement scheme whatsoever. Fearing to tread on the constitutional prerogatives of the president, Congress has been reluctant to add any enforcement mechanisms to the Presidential Records Act, or to give the archivist any direct authority over how the president meets his or her obligations under the law. But requiring a president to have in place an effective record keeping system that meets basic criteria established by the archivist does not come close to encroaching on any constitutionally protected sphere of the president. The president is, after all, a caretaker of our nation's history.

At a bare minimum, Congress should amend the President Records Act to mandate effective record keeping of presidential records while a president is in office, with a direct oversight role for the archivist to ensure the White House has an appropriate system in place that meets this requirement. Congress also should provide for a private right of action so that outside groups can serve as a backstop when the archivist is unable or unwilling to act. When President Nixon left office and claimed his presidential records as his personal property, Congress acted to ensure that never again would our national history be at the whim or discretion of an individual president. More recent history shows us it is now time for Congress to act once again to safeguard our historical legacy.

I recall engaging in a vigorous internal debate nearly 20 years ago, while an attorney at the Department of Justice, over whether email was even a record that had to be preserved with all of its metadata. Today this issue is long settled as a matter of law, but as a matter of practice agencies continue to treat emails as readily discardable, even while their value has grown

exponentially. Just look at the currency Elena Kagan's federal and presidential electronic records have, as Congress evaluates her nomination for the Supreme Court. Congress may not be so fortunate in the future should a president nominate someone who was in the Bush White House during the period of missing emails.

Email communications have now become the accepted substitute for letters, phone calls, and even in-person meetings. Their value often lies in their reflection of unguarded truths or "smoking guns," and they range from a casual request for lunch to an elaborate justification for a major administration policy decision. They have shed light on countless decisions, and their value to history is no longer a matter for debate.

Without question, emails are the gold we mine for the answers to questions that perplex and worry us or the truth behind an administration's or agency's controversial decisions and actions. Yet we fail to handle these treasures with care, both at the presidential and agency level. Engraved on the exterior of the National Archives and Records Administration building in Washington, D.C. are the words of William Shakespeare, "What's past is prologue." This Committee, and Congress as a whole, must act to ensure our past will be available for future generations to study and learn from.

EXHIBIT A

Final Report

Mail Comparison

Prepared for

Executive Office of the President

Monday, 7 June 2010

Version 2.2

Prepared by

Aaron Margosis

Principal Consultant

aaronmar@microsoft.com

Microsoft | Services

88

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
15 April 2010	Aaron Margosis	1.0	N/A
21 April 2010	Zaheer Tanveer	1.2	Accepted OA Edits and Changes
2 June 2010	Aaron Margosis	2.0	Second analysis with corrected data
4 June 2010	Aaron Margosis	2.1	Revised and reorganized
7 June 2010	Aaron Margosis	2.2	Incorporated review comments

Reviewers

Name	Version approved	Position	Date

89

Table of Contents

1 PROJECT SUMMARY

In compliance with Presidential and Federal Records Management requirements, EOP retains a copy of every message that is sent or received on the network email system. Extensive analysis of historical data revealed that email volume was unexplainably lower than normal for certain EOP components on an unrelated collection of calendar days that occurred during President George W. Bush's administration. With this finding, the process used to save email for the days in question has been subject to intense review. A complex data restoration process was accomplished to recover email messages from backup data to ensure messages from low days were archived, and to enable independent evaluations of the overall archiving process. The purpose of the current project was to develop, complete, and provide results of a process that compares the email messages restored from backup data (the "PST set") to email messages in the EOP messaging PRA/FRA archive (the "EML set"). The analysis would try to determine whether the two sets were identical or whether either set contained messages not found in the other set.

The objectives for this project included:

- Determining a reliable basis for comparing messages between the two sets;
- Developing a means for performing those comparisons;
- Identifying the messages that appear in each set that are not found in the other set.

The scope explicitly excluded analysis of anything other than the email messages, such as vendor methodologies.

The first attempt to perform this analysis was flawed, as it was discovered after the final report had been submitted that the message sets involved in the comparison were incorrect. The PST set included messages from all 15 components for the 21 calendar days, instead of from just the components that were identified as having unexplained low email counts. It was also discovered that 12 of the 48 component days that were to be targeted for comparison did not correspond to any of the correct 48 component days identified earlier in the litigation. The entire analysis was started over after it was confirmed by the EOP and the National Archives and Records Administration (NARA) that the correct 48 component-day files for both data sets, and *only* the correct 48 component-day files, were included in the comparison.

After data cleanup and deduplication, the EML set contained 18,146 messages, while the PST set contained 164,780. Clearly, even if all messages in the EML set matched messages in the PST set, the latter would still contain many messages not found in the EML set. Ultimately, 11,399 messages were identified as being in both sets; 6747 messages in the EML set were not matched, while 153,381 messages in the PST set were not matched. However, the number of matches is undoubtedly low, although exactly how low is not clear. The EML and PST message sets had been processed by different mechanisms and techniques, leading to wide variations in data formatting and content. This disparity

made it impractical to exactly match up messages in the two sets that originally derived from a single email message.

2 DATA PROVIDED FOR ANALYSIS

There were 21 distinct calendar days for which one or more EOP components had an unexplained low number of emails. The components and their "low days" are identified in the following table – a total of 48 "component-days".

Component	Low days
CEA	1/16/2004, 1/17/2004, 1/18/2004, 1/28/2004, 2/2/2004
CEQ	12/20/2003, 1/16/2004, 1/17/2004, 1/18/2004, 2/2/2004, 2/8/2004
NSC	5/16/2004
OA	12/17/2003, 12/20/2003, 1/8/2004, 1/14/2004, 1/16/2004, 1/18/2004, 1/29/2004, 2/4/2004, 2/8/2004
OMB	1/29/2005
ONDCP	1/16/2004, 1/23/2004, 2/4/2004, 2/7/2004, 2/8/2004, 4/21/2005
OPD	8/6/2005
OSTP	1/16/2004, 1/17/2004, 1/18/2004, 2/7/2004
OVP	9/13/2003, 1/12/2004, 1/14/2004, 1/29/2004, 2/7/2004, 2/8/2004
PFIAB	4/11/2004
WHO	12/17/2003, 12/20/2003, 1/14/2004, 1/16/2004, 1/17/2004, 1/18/2004, 1/29/2004, 2/2/2004

Table 1. The 48 low component-days

The scope of this task involved analysis of email messages restored from backup data and stored in PST files against email messages extracted from the PRA/FRA archive and stored in EML files.

The set of messages stored in the PST files was programmatically assembled and was also supposed to be de-duplicated by the third party to include a single copy of all messages that were sent or received by the identified EOP components during the days for which there was an unexplained low number of email messages. The third party provided PSTs for 15 EOP components for each of the 21 calendar days,

for a total of 315 PST files. The PSTs representing the 48 component-days of interest were carefully copied to a separate folder for analysis, and the list of files triple-checked.

The set of messages extracted from the PRA/FRA archive by a different third party were stored in 19,880 EML files, each representing one email message, organized into a folder structure by EOP component and calendar day. Below the top "Data" folder there were 46 folders containing messages from each of the component-days in which there were messages. There were two component-days for which the EML set did not have any messages, so folders were not created for those two component-days. Of the 19,880 EML files, however, 246 files were found to be zero-length (empty). These were ignored, leaving 19,634 EML files to process.

In order not to risk losing any data, the existing PST and EML files were considered the authoritative data sources. Analysis was performed on them directly, and not after first converting them to another format. Because the EML files are ANSI text files, it was possible to mark them "read-only" and to guarantee that they were not modified during processing. Because MAPI (the Microsoft-defined "Messaging Application Programming Interface") requires that PST files be modifiable, and simply opening a PST file using MAPI changes it, care was taken to ensure that analysis software did not change message content, and that analysis be performed on copies of the files rather than on the originals.

94

3   DATA EXTRACTION AND COMPARISON TECHNIQUES

The first part of the project was to extract the information required for performing the comparisons from the data sources. Data from the source files was written to tab-delimited text files. These files were imported into tables on a SQL Server Enterprise database, where sorting and other manipulation and comparison tasks could be performed efficiently. The work was performed on a standalone Windows 7 x86 computer with 1GB RAM. The computer was not connected to any network, to help ensure that the sensitive email data would not be inadvertently transmitted or disclosed.

3.1   EML Data Extraction Techniques

The EML files were ANSI text files, comprised of Internet message headers as documented in RFC 2822, followed by an empty line followed by message content. All information of interest is in the message headers. Note that these headers are P2 headers used for display purposes and are not the SMTP P1 headers that are used for actual routing. P2 headers are not required to be accurate or reflect the actual sender and recipient information. P1 headers are typically not visible or retained in email messages. The P2 headers were extracted using PowerShell scripts and written out in tab-delimited text file format. For each file, the values for the headers shown in the following table were extracted, along with the full path of the EML file. In addition, because the component-day was represented in the folder hierarchy in which the EML files were stored, the component-day was derived from the file path captured as a separate "ComponentDay" field.

Because it was already known, based on results from the earlier analysis project, that data cleanup would be required, that data cleanup was performed by the PowerShell scripts at the time of extraction. That data cleanup is described in a later section.

Header Name	Notes
From:	The display name of the purported sender.
To:	The displayed "To" line of the message.
CC:	The displayed "CC" line of the message.
Subject:	The Subject line of the message.

Header Name	Notes
Date:	The timestamp reflecting when the message was purportedly sent. This is usually set by the client software composing the message. The standard suggests that the time zone offset be expressed as a numeric offset. A number of messages expressed the time zone offset using text such as "EST"; the extraction script needed to special-case these entries to convert them to numeric offsets. Time stamps were converted to Universal (UTC) time when written to the CSV file.
Sent:	A "Sent:" header, if found, was considered equivalent to a "Date:" header.
Message-ID:	The Internet Message-ID of the message.

Table 2. Fields extracted from messages in EML files

3.2 PST Data Extraction Techniques

PST files were enumerated and processed by custom-written C++ code. Each PST's folder hierarchy was recursively enumerated, and data extracted from any messages found within them. The PSTs were generally found to contain over a thousand folders each, most of which were empty. For each message found within these folders, the extraction utility wrote out the following MAPI properties to the CSV file, along with the full path of the PST file and the folder path within the PST:

MAPI Property	Notes
PR_SENDER_NAME	Contains the message sender's display name. Most closely corresponds to the "From:" header in the EML files.
PR_DISPLAY_TO	Contains an ASCII list of the display names of the primary message recipients, separated by semicolons. Most closely corresponds to the "To:" header in the EML files.
PR_DISPLAY_CC	Contains an ASCII list of the display names of any carbon copy (CC) message recipients, separated by semicolons. Most closely corresponds to the "CC:" header in the EML files.
PR_SUBJECT	Contains the Subject of the message. Corresponds to the "Subject:" header in the EML files.

MAPI Property	Notes
PR_CLIENT_SUBMIT_TIME	The date and time the message sender submitted the message. (See notes below about the collection of timestamp properties.)
PR_CREATION_TIME	The creation date and time for the message. (See notes below about the collection of timestamp properties.)
PR_LAST_MODIFICATION_TIME	The date and time the object was last modified. Modifications can include a message being marked "read" or "unread". (See notes below about the collection of timestamp properties.)
PR_MESSAGE_DELIVERY_TIME	The date and time that the message was delivered. (See notes below about the collection of timestamp properties.)
PR_INTERNET_MESSAGE_ID	The Internet Message-ID of the message.
PR_MESSAGE_CLASS	Identifies the sender-defined message class, such as IPM.Note which indicates a normal email message, or IPM.Schedule.Meeting.Resp.Pos which indicates an acceptance of a meeting request.

Table 3. Properties extracted from messages in PST files

The utility also wrote detailed diagnostic output including the names of all folders traversed and the number of items within each folder. The diagnostic output was used to verify that the processing of each PST file completed successfully.

Four timestamp properties associated with each message, if found, were extracted and written to the CSV file in Universal (UTC) time. Not all of the properties were set for all messages, but PR_CLIENT_SUBMIT_TIME was always set. These four properties were collected so that it could be determined through experimentation which property most closely corresponded with the "Date:" header in the EML files after data collection. As expected, the PR_CLIENT_SUBMIT_TIME was found to be the most appropriate field to use. For emails that originated externally, the PR_CLIENT_SUBMIT_TIME appeared to be set from the "Date:" header set by the email client software. The other three properties were ultimately ignored in the message comparisons.

There were several reasons for using custom code rather than acquiring and using a commercial product. First, there was no budget, schedule or defined process for evaluating and purchasing a commercial product, and in fact the Statement of Work (SOW) under which this work was performed called for the development of a utility. Second, it was not clear that commercial products would extract the data in the required format, or that additional coding wouldn't be required to convert a commercial product's output to the necessary format. Finally, the Microsoft developer who performed the work has

97

significant MAPI experience and has access to the top MAPI experts in the world whenever questions arise.

98

4   PROJECT RESULTS

4.1   Data Extraction

The 48 PST files contained a total of 340,224 messages for which data was extracted to separate CSV files, one per component-day.

Data from the 19,634 EML files that were not zero-length (empty) were extracted, cleaned, and written into a single CSV file.

4.2   Initial Message Analysis and Data Cleanup

The project design envisioned comparing messages using one of two techniques. The most reliable comparison was originally anticipated to be the Internet "Message-ID" header as described in RFC 2822. For cases where a Message-ID was not found, comparison would be performed on the "From", "To", "CC", "Subject" and timestamp fields. There turned out to be significant challenges with both of these techniques.

Based on results from the earlier analysis, it was known that both data sets would require cleanup and deduplication. In addition, it had been suggested that the PST files might have been built to include messages from the day preceding and the day following the component-day, in order to ensure that messages were not excluded because of time zone issues. Therefore, a PowerShell script was used to inspect the messages in each of the PST-derived CSV files to verify whether their timestamps fell within the expected time range for the component day. It was found that with few exceptions, the timestamps of messages ranged from 5:00am UTC of the component day to 4:59am UTC of the day following the component day. With two component days (ONDCP April 21, 2005, and OVP September 13, 2003) the messages ranged from 4:00am UTC to 3:59am UTC of the following day. This is explainable by the fact that Eastern Standard Time is UTC-05 and Eastern Daylight Time is UTC-04. Ultimately, only four messages were found to be outside the expected timestamp range for their component-days. These were removed from the set before further processing.

The earlier analysis effort showed the need for data cleanup to make message comparison more reliable. First, formatting of sender and recipient fields was inconsistent between data sets and sometimes within a data set. This is believed to have been caused by the different sets having been restored from different sources using different techniques, and converted to different formats (PST vs. EML). Some specifics:

- Sometimes names were quoted with single quotes, sometimes with double quotes, sometimes not at all.
- Quoting was sometimes further encoded with a backslash preceding the quote character.
- Sometimes names were followed by an email address; other times, not.

- Sometimes, an address consisting only of an email address would be within angle brackets (e.g., <someone@sample.com>) and other times not.
- In the PST set, multiple To or CC recipients were typically separated by semicolons; in the EML set, they were always separated with commas. Note that commas were also common within a display name when formatted as "Last, First", making reliable programmatic parsing of these To and CC lines extremely difficult at best.

Overall, it must be noted that the formatting of display names in email messages – including Sender, To and CC fields – does not have to accurately reflect the actual sender and recipients, or even be well-formed. As mentioned earlier, they are for display purposes and are not used in actual email routing. However, this makes programmatic comparison of messages that were restored from different sources and using different techniques very difficult. Furthermore, because of the tremendous variability in recipient lists, the same level of cleanup that was possible with the Sender Name was not possible with the To or CC fields. For example, while there is always only one sender, there can be zero or more items in the To and CC fields. It is not practical to determine programmatically whether a comma is separating multiple recipients or the last name and first name of a single recipient.

According to the RFC, the Message-ID header is an identifier that the mail server to which the message is submitted is supposed to ensure is unique; and once a particular message has a Message-ID assigned to it, that Message-ID should remain associated with the message and never be changed. In practice, the specification appears not to have been closely followed in all cases. Mass-mailers often reuse the same Message-ID for unrelated messages. Certain obviously non-unique Message-IDs had to be filtered out of the extracted data as part of data cleanup. In particular, three Message-IDs were observed being reused in many cases: `<1@no.return.address>`, `<2@no.return.address>`, and `<3@no.return.address>`. Also, in numerous cases, messages that matched on all other fields were found to have been assigned new Message-IDs at some point, presumably by a forwarding server or other processing agent. And in other cases, items (particularly meeting requests and responses) had identical Message-IDs, senders and timestamps, but different recipients. Ultimately, it was decided that matching or deduplicating strictly on Message-ID values was not reliable and was discarded as a comparison technique.

Finally, leading and trailing spaces in the Subject line were found not to be consistent between the sets following data extraction.

To resolve all these issues, data cleanup was performed on both the EML and PST data prior to importing into the database. PST data was processed as follows:

- In the Sender, To and CC fields, backslashes, single quote characters (apostrophes), and double quote characters were removed.
- In the Sender, To and CC fields, semicolons were replaced with commas to improve matching with EML data.

- Leading and trailing spaces were removed from the Subject.
- If the Message-ID was <1@no.return.address>, <2@no.return.address>, or <3@no.return.address>, the Message-ID was removed from the record.

EML data was processed as follows:

- In the From, To and CC fields, backslashes, single quote characters (apostrophes), and double quote characters were removed.
- In the From, To and CC fields, any semicolons were replaced with commas.
- If the From field began with < and ended with >, those two characters were removed. (In all of these cases, the remaining data was an email address.)
- If the From field contained text followed by a space and a <, (e.g., "Aaron Margosis <aaronmar@microsoft.com>", the space, angle bracket and everything after it was removed (leaving only the name).
- If the Message-ID was <1@no.return.address>, <2@no.return.address>, or <3@no.return.address>, the Message-ID was removed from the record.

In spite of the expectation that the PST files contained only deduplicated messages, the opposite was in fact true. The vast majority of messages appeared twice in each PST file: once in some nested subfolder, and then the same message appearing in a top level folder called either "1_AllMessages" or "1_All Messages", depending on the PST file. Duplicate copies of messages could also appear in multiple components on the same day. For example, if a single message were sent to recipients in multiple components, the same message could have been captured in different component-day sets. The EML set also had duplicates, but comparatively far fewer than the PST set did.

To deduplicate these messages, the PST-sourced data was exported from the database to a CSV file, sorted on SenderName, then ClientSubmitTime, Subject, To, CC, SourceFile, SourceFolder and Message-ID. This CSV file was then processed with a PowerShell script that compared each row to the message from the previous row, ignoring the SourceFile, SourceFolder and Message-ID fields. If two rows were identical in all other respects, only the first copy was written to a new CSV file. The content of this CSV file was then imported into a new database table. Similarly, the EML-sourced data was exported to a CSV file, sorted on FROM, DATE, SUBJECT, TO, CC, ComponentDay, SOURCEFILE, and MESSAGEID. Sequential rows were compared on the FROM, DATE, SUBJECT, TO and CC fields; where multiple rows had the same values on these fields, only the first copy was retained.

Following this data cleanup and deduplication, there were 164,780 PST messages, and 18,146 EML messages. The message counts are shown by component day in the table below. Note that due to the inclusion of the SourceFile (PST) and ComponentDay (EML) fields in the sorting order, duplicates across components consistently retained the copy in the alphabetically earlier component, and that due to the inclusion of SourceFolder in the PST sorting order, the copy from the alphabetically earlier folder was consistently retained (typically "1_All Messages" or "1_AllMessages").

101

The following table lists the number of messages in each component day for the PST and EML sets following deduplication. Note that the numbers of emails in both the PST and EML sets in this table are less than the number of emails restored and archived, respectively, because identical emails that appeared in two or more different components were de-duplicated and removed for purposes of this comparison.

Component-Day	PST Set	EML Set	Difference
CEA 1/16/2004	1119	28	1091
CEA 1/17/2004	102	2	100
CEA 1/18/2004	94	0	94
CEA 1/28/2004	1253	58	1195
CEA 2/2/2004	1096	108	988
CEQ 12/20/2003	51	3	48
CEQ 1/16/2004	1106	33	1073
CEQ 1/17/2004	65	2	63
CEQ 1/18/2004	54	0	54
CEQ 2/2/2004	1371	137	1234
CEQ 2/8/2004	54	1	53
NSC 5/16/2004	113	305	-192
OA 12/17/2003	6774	275	6499
OA 12/20/2003	851	16	835
OA 1/8/2004	3634	922	2712
OA 1/14/2004	4462	465	3997
OA 1/16/2004	3867	120	3747
OA 1/18/2004	370	11	359
OA 1/29/2004	4526	931	3595
OA 2/4/2004	4154	401	3753
OA 2/8/2004	310	22	288
OMB 1/29/2005	215	1105	-890
ONDCP 1/16/2004	868	16	852
ONDCP 1/23/2004	802	173	629
ONDCP 2/4/2004	1000	38	962
ONDCP 2/7/2004	28	4	24
ONDCP 2/8/2004	43	2	41
ONDCP 4/21/2005	2047	457	1590
OPD 8/6/2005	3	11	-8
OSTP 1/16/2004	1376	15	1361
OSTP 1/17/2004	96	1	95
OSTP 1/18/2004	92	2	90
OSTP 2/7/2004	151	3	148

Component-Day	PST Set	EML Set	Difference
OVP 9/13/2003	208	15	193
OVP 1/12/2004	3632	580	3052
OVP 1/14/2004	3447	581	2866
OVP 1/29/2004	1790	97	1693
OVP 2/7/2004	86	4	82
OVP 2/8/2004	77	7	70
PFIAB 4/11/2004	3	5	-2
WHO 12/17/2003	16170	657	15513
WHO 12/20/2003	1220	35	1185
WHO 1/14/2004	21375	2457	18918
WHO 1/16/2004	20327	593	19734
WHO 1/17/2004	2558	59	2499
WHO 1/18/2004	2653	44	2609
WHO 1/29/2004	20040	4233	15807
WHO 2/2/2004	29047	3112	25935
TOTAL	**164780**	**18146**	

Table 4. Count of deduplicated messages in each of the 48 component-days, and differences between the sets

4.3   Message Comparison

Based on the deduplicated message counts it was very clear that at a minimum there would be many messages in the PST set not found in the EML set. However, it was observed in a few samples that even with data cleanup, comparison would continue to be hampered by different formatting; e.g., a pair of messages from the two sets that on visual inspection had originally derived from the same single email message could not be programmatically determined to be the same, since the "To" field on one copy showed only the recipients' display names and on the other, only their email addresses.

Message comparison was performed by comparing the five fields listed in the table below for equality. Note that these fields involve only message attributes, and not the EOP component that a message was associated with. Therefore, a message in the PST set could match a message in a different component in the EML set (but on the same day). The deduplication ensured that a message in one set would match at most one message in the other set. Without deduplication, a single message in one set could match multiple messages in the other set, and match totals would not add up correctly.

PST Field	EML Field
SenderName	FROM
To	TO

CC	CC
Subject	SUBJECT
ClientSubmitTime	DATE

Table 5. Fields used to compare messages in the two sets

Messages that matched were exported to a CSV file using the SQL query below. 11,399 matching messages were identified and exported. The output included the matching fields, as well as the Message Class, the source file and folder from the PST message, and the ComponentDay and full path to the source file from the EML set.

```
SELECT
        e.[FROM]              [From]
       ,e.[TO]               [To]
       ,e.[CC]               [CC]
       ,e.[SUBJECT]          [Subject]
       ,e.[DATE]             [Date]
       ,p.[MessageClass]     PST_MessageClass
       ,e.[SOURCEFILE]       EML_Filename
       ,e.[ComponentDay]     EML_ComponentDay
       ,p.[SourceFile]       PST_SourceFile
       ,p.[SourceFolder]     PST_SourceFolder
  FROM [MailComparison2].[dbo].[EmlDataFromDataDedupIgnoreMsgID] e
  INNER JOIN
[MailComparison2].[dbo].[PstDataFromDataCleanup3_IgnoreMsgID] p
  ON
       e.[FROM] = p.[SenderName] AND
       e.[TO] = p.[To] AND
       e.[CC] = p.[CC] AND
       e.[SUBJECT] = p.[Subject] AND
       e.[DATE] = p.[ClientSubmitTime]
```

The 6,747 EML messages that didn't match corresponding messages in the PST set were exported to a CSV file using the SQL query below. The output included the full path to the EML file, the ComponentDay, FROM, TO, CC, Subject, Date and Message-ID fields:

```
SELECT [SOURCEFILE]
      ,[ComponentDay]
      ,[FROM]
      ,[TO]
      ,[CC]
      ,[SUBJECT]
      ,[DATE]
      ,[MESSAGEID]
  FROM [MailComparison2].[dbo].[EmlDataFromDataDedupIgnoreMsgID]
EXCEPT
      SELECT e1.[SOURCEFILE]
            ,e1.[ComponentDay]
            ,e1.[FROM]
            ,e1.[TO]
```

```
                ,e1.[CC]
                ,e1.[SUBJECT]
                ,e1.[DATE]
                ,e1.[MESSAGEID]
        FROM [MailComparison2].[dbo].[EmlDataFromDataDedupIgnoreMsgID]
el
        INNER JOIN
[MailComparison2].[dbo].[PstDataFromDataCleanup3_IgnoreMsgID] p1
        ON
                e1.[FROM] = p1.[SenderName] AND
                e1.[TO] = p1.[To] AND
                e1.[CC] = p1.[CC] AND
                e1.[SUBJECT] = p1.[Subject] AND
                e1.[DATE] = p1.[ClientSubmitTime]
```

The 153,381 PST messages that didn't match corresponding messages in the EML set were exported to a CSV file using the SQL query below. The output included the name of the PST file, the folder in the PST file, the message class, the Sender Name, To, CC, Subject, ClientSubmitTime and Message-ID fields.

```
SELECT [SourceFile]
        ,[SourceFolder]
        ,[MessageClass]
        ,[SenderName]
        ,[To]
        ,[CC]
        ,[Subject]
        ,[MessageID]
        ,[ClientSubmitTime]
    FROM [MailComparison2].[dbo].[PstDataFromDataCleanup3_IgnoreMsgID]
EXCEPT
        SELECT p1.[SourceFile]
                ,p1.[SourceFolder]
                ,p1.[MessageClass]
                ,p1.[SenderName]
                ,p1.[To]
                ,p1.[CC]
                ,p1.[Subject]
                ,p1.[MessageID]
                ,p1.[ClientSubmitTime]
        FROM
[MailComparison2].[dbo].[PstDataFromDataCleanup3_IgnoreMsgID] p1
        INNER JOIN
[MailComparison2].[dbo].[EmlDataFromDataDedupIgnoreMsgID] e1
        ON
                e1.[FROM] = p1.[SenderName] AND
                e1.[TO] = p1.[To] AND
                e1.[CC] = p1.[CC] AND
                e1.[SUBJECT] = p1.[Subject] AND
                e1.[DATE] = p1.[ClientSubmitTime]
```

105

Further queries were executed to determine how many messages from each component-day matched
or failed to match from the PST and EML sets. Those results are shown in the table below.

Component-Day	PST Set	PST Not Matched	PST Delta (number matched)	EML Set	EML Not Matched	EML Delta (number matched)
CEA 1/16/2004	1119	1112	7	28	21	7
CEA 1/17/2004	102	100	2	2	0	2
CEA 1/18/2004	94	94	0	0	0	0
CEA 1/28/2004	1253	1208	45	58	13	45
CEA 2/2/2004	1096	1031	65	108	43	65
CEQ 12/20/2003	51	48	3	3	0	3
CEQ 1/16/2004	1106	1092	14	33	19	14
CEQ 1/17/2004	65	65	0	2	2	0
CEQ 1/18/2004	54	54	0	0	0	0
CEQ 2/2/2004	1371	1299	72	137	64	73
CEQ 2/8/2004	54	54	0	1	1	0
NSC 5/16/2004	113	57	56	305	249	56
OA 12/17/2003	6774	6548	226	275	45	230
OA 12/20/2003	851	843	8	16	8	8
OA 1/8/2004	3634	2932	702	922	220	702
OA 1/14/2004	4462	4091	371	465	92	373
OA 1/16/2004	3867	3780	87	120	33	87
OA 1/18/2004	370	364	6	11	5	6
OA 1/29/2004	4526	4256	270	931	658	273
OA 2/4/2004	4154	3912	242	401	159	242
OA 2/8/2004	310	296	14	22	8	14
OMB 1/29/2005	215	75	140	1105	965	140
ONDCP 1/16/2004	868	868	0	16	16	0
ONDCP 1/23/2004	802	745	57	173	116	57
ONDCP 2/4/2004	1000	999	1	38	37	1
ONDCP 2/7/2004	28	28	0	4	4	0
ONDCP 2/8/2004	43	43	0	2	2	0
ONDCP 4/21/2005	2047	1903	144	457	313	144
OPD 8/6/2005	3	3	0	11	11	0
OSTP 1/16/2004	1376	1370	6	15	9	6
OSTP 1/17/2004	96	96	0	1	1	0
OSTP 1/18/2004	92	91	1	2	1	1
OSTP 2/7/2004	151	150	1	3	2	1
OVP 9/13/2003	208	202	6	15	9	6

106

Component-Day	PST Set	PST Not Matched	PST Delta (number matched)	EML Set	EML Not Matched	EML Delta (number matched)
OVP 1/12/2004	3632	3181	451	580	129	451
OVP 1/14/2004	3447	3016	431	581	133	448
OVP 1/29/2004	1790	1721	69	97	22	75
OVP 2/7/2004	86	84	2	4	2	2
OVP 2/8/2004	77	76	1	7	6	1
PFIAB 4/11/2004	3	2	1	5	4	1
WHO 12/17/2003	16170	15685	485	657	176	481
WHO 12/20/2003	1220	1194	26	35	9	26
WHO 1/14/2004	21375	19432	1943	2457	533	1924
WHO 1/16/2004	20327	19911	416	593	177	416
WHO 1/17/2004	2558	2516	42	59	17	42
WHO 1/18/2004	2653	2623	30	44	14	30
WHO 1/29/2004	20040	17313	2727	4233	1515	2718
WHO 2/2/2004	29047	26818	2229	3112	884	2228
TOTAL	**164,780**	**153,381**	**11,399**	**18146**	**6,747**	**11,399**

Table 6. Messages matched and not matched in the two sets, by component-day

While most matching messages matched within "component-days", messages can and did match across components. For example, consider the counts on January 29, 2004 for OA, OVP and WHO, which are broken out in this smaller table:

Component-Day	PST Set	PST matched	EML Set	EML matched	PST-EML match diff
OA 1/29/2004	4526	270	931	273	-3
OVP 1/29/2004	1790	69	97	75	-6
WHO 1/29/2004	20040	2727	4233	2718	9
				TOTAL	**0**

Table 7. Analysis of differences in match counts across component-days

Analysis showed that the 75 matching messages associated with OVP from the EML set matched the 69 messages from the PST set for OVP, as well as six messages from the PST set for WHO. The 2727 messages from the PST set for WHO matched all 2718 WHO messages from the EML set, the six from OVP, and three more from OA. Because of the deduplication, each message would match at most only one message from the other set.

Mr. CLAY. Thank you so much, Ms. Weismann.

We will go to the question and answer period and I recognize the ranking member from North Carolina.

Mr. MCHENRY. Ms. Weismann, I appreciate your testimony. In your written testimony you have a recommendation for how we can actually ensure that the President is required to keep the data that he is required to keep. I appreciate what you are saying; I think you make very valid points about the last administration, about their lack of transparency. My question to you is what can we put in place now so that doesn't happen again?

Ms. WEISMANN. Well, this is where I think you can consider amendments to both the Federal Records Act and the Presidential Records Act. I mean, in part through our litigation, the White House now has in place what is an effective recordkeeping system, but this has been a problem that has plagued us through many presidencies, and we have no assurance, especially as technology changes, that the next president will be out of compliance once again, and that is why we think it is imperative that, at a minimum, you give the Archivist some oversight and responsibility to at least ensure that the President has in place an appropriate system.

I understand and appreciate the constitutional problems with dictating to the President what he or she must save and cannot save specifically, but I don't think you come close to those problems if you are trying to just enforce the responsibility that they have a system in place.

Mr. MCHENRY. So that means enhancing the Archivist's role?

Ms. WEISMANN. Yes. At present, the Archivist basically has no role while a President is in office.

Mr. MCHENRY. Aside from outside groups, who is the cop here to ensure that these records are kept?

Ms. WEISMANN. There really is no cop, and that is part of the problem.

Mr. MCHENRY. So it falls to outside groups.

Ms. WEISMANN. Well, even for outside groups there is no role, because the courts have held that, with some limited exceptions, because the statute doesn't really spell out a role for outside groups, that we have no ability essentially to sue. Now, there are some limited exceptions. But if you have a President who completely ignores his responsibilities, I think it would fall to Congress, through legislation, to correct the situation.

Mr. MCHENRY. Is this a systemic issue that is made worse by different administrations, but at root is a systemic issue throughout the Federal Government?

Ms. WEISMANN. Yes, it is a systemic issue throughout the government, without question, and I think this leads to our second point, as to why we need some legislative fixes to the Federal Records Act, because the roles and responsibilities that the Archivist has even in that arena I think are still limited. And I think the best example of that is the fact that this critical self-assessments, the Archivist really has no legal way to compel agencies to comply.

And in that arena, as well, the courts have recognized very limited roles for outside groups like mine, so there too we are in favor of expanding private rights of action, but we also think that you

can beef up the administrative enforcement mechanisms under the Federal Records Act that will give the Archivist greater authority.

Mr. McHENRY. Would you be willing to submit your recommendations to this committee?

Ms. WEISMANN. Absolutely.

Mr. McHENRY. I certainly appreciating hearing those. Do you think our Presidential library system, as constructed now, makes it more difficult for you to retrieve those records going back years?

Ms. WEISMANN. I think there are a lot of reasons why they are difficult to retrieve. I mean, I think too often each Presidential library tends to operate as an individual fiefdom, and I also think you have problems with the state of records that vary dramatically between administrations. I mean, I think if we can get to a place where we are systematizing, if that is a word, both what Presidents are creating and how we are preserving them and what agencies, we will overcome that battle.

Mr. McHENRY. Absolutely.

And that goes right into, Dr. Hunter, your definition of record. Basically, the Federal Government is using the 1950's definition, when the rest of society is using a much more updated version, is that right?

Dr. HUNTER. The Federal definition actually is the same one that most States use. Most States adopted the Federal definition. Private sector doesn't have to. Many private sector organizations use a very similar definition. But in the world of digital recordkeeping, there are others who are looking at it, saying that we are spending more time trying to slice something very thin that may not be worth the effort; that we have to manage it anyway, especially if we are in a discovery environment. We have to find it no matter what it is called.

So, therefore, perhaps we need to look at the fundamental and try to minimize that sorting and slicing and dicing that isn't really giving us much advantage.

Mr. McHENRY. How far behind do you think the Federal Government is in keeping records, compared to the private sector, compared to private institutions?

Dr. HUNTER. Well, if we were doing this in front of some private sector people, they would be saying the Federal Government may be ahead of where they are.

Mr. McHENRY. Really?

Dr. HUNTER. I think my point is that this is very difficult——

Mr. McHENRY. How would you say that? Is it in terms of the technology of the Federal Government uses, or is it the policies or is it the people? What is the advantage?

Dr. HUNTER. This is very difficult work, and as I say in the written testimony, this is a line responsibility. So some private sector organizations have been able to push that responsibility in the same way that human resources policies, people are accountable for complying with that; fiscal policies, there are cops, to use your word, who make certain that front-line managers comply with those policies; if those same cops are able to say are you complying with the records management policy.

So in some ways, in some private sector areas with compliance they have been able to do better. There are some private sector

areas that would love to be able to have, from the previous panel, to have an organization like the Department of Defense to push for its business purposes a standard with the full package that then becomes adopted otherwise. So this is just very difficult work that must succeed as an individual line responsibility, and it is harder in the Federal Government, perhaps, because there are more people with that responsibility.

Mr. MCHENRY. Thank you. Thank you for your testimony.

Mr. CLAY. Thank you, Mr. McHenry.

Dr. Hunter, I found your example of the Indiana University archives working on an electronic records study with an NHPRC grant interesting. We continue to be amazed by the scope and importance of this vital program. You mentioned that you do not think NARA should conduct audit reviews. Can you explain why not?

Dr. HUNTER. NARA, I believe, certainly has the responsibility and should do audits, but all day long I have been hearing the question of is NARA, as an entity, and in the private sector we have the same issue, is the records management department, when it says you are not following orders, do they have the clout, are they the cop to force a change in practice. And perhaps one solution legislatively is to make NARA a bigger sheriff in this, to give them more authority.

Another potential solution would be to look at the other sheriffs who are there with the other line responsibilities and see perhaps a strategic partnership might be the more cost-effective way to go. So certainly I don't think NARA has the responsibility, but I am asking all parties to consider what might be the best cost-effective way to discharge that responsibility.

Mr. CLAY. Thank you for that response. Can you please elaborate on the role of records liaisons and how you recommend agencies can be encouraged to utilize them?

Dr. HUNTER. Records liaisons very often, again, at the grassroots level, as opposed to the agency head level, there needs to be someone in every office who knows what is going on with the records and needs to be empowered to do what is right and efficient with those records. Sometimes those people are well trained and they are enthusiastic, and other times they are people who someone may think they have some more time on their hands, so they can do this as well.

But again, that responsibility for that key role at the Department level, this will break down unless the people are properly trained, but there also is a system of accountability that, in the human resources environment, that the job descriptions reflect this responsibility; that they are evaluated on it; that their manager, in turn, is evaluated on what they do.

So that is why I talk about this as being hard work. At some point it does get down to the level of who is the records liaison, the person responsible for the digital system or the paper-based system. Do they know what they are doing and are they rewarded for taking the initiative and doing it right, or does no one even notice that?

Mr. CLAY. Thank you for that response.

Ms. Brock, your impression of records liaisons?

Ms. BROCK. Traditionally, records liaison officers are at too low a level to make a difference. What we really need is information management officers, professionals who understand the scope, breadth, and depth of the mission and the opportunities there.

Mr. CLAY. How can Federal agencies use ARMA International's principles-based approach, using generally accepted recordkeeping principles to improve their records management program?

Ms. BROCK. Chairman Clay, thank you for asking me that. There are basic competencies in these principles: accountability, transparency, integrity, protection, compliance, availability, retention, and disposition. And we have five different levels of compliance with each. We could use this as a scorecard for judging programs and for what they should be aiming to achieve for compliance. I also see that we can use these principles to design our training, to actually buildup our programs, and to monitor and direct how we conduct our procurements for these tools to handle our records.

Mr. CLAY. Thank you for that response.

Let me ask Ms. Weismann what specific amendments to the Federal Records Act do you recommend to expand the Archivist oversight and enforcement responsibilities?

Ms. WEISMANN. Well, I think, first of all, they need to be given the authority and clear responsibility to conduct themselves an investigation when they have evidence that there has been a violation of the Records Act. I think, as I outlined in my testimony, the next step would be not only to make that public, but when they find such evidence, we would recommend that it be mandated a referral to the agency inspector general.

And I think this is addressing in part something Dr. Hunter said about looping in others. There already is, within each agency, an inspector general that has authority to conduct investigations and has experience with that; and I think that the findings of that should be made public. And, again, this is where we think if the agency still chooses to do nothing in the face of evidence of a problem, that there should be a private right of action.

We have listened very carefully over the years to NARA's view on its authority, for example, and responsibility to conduct investigations. CREW actually brought a lawsuit against NARA a year or so ago based on their failures in 2000 to conduct investigations of agencies, and we dropped our lawsuit after we met with them and they outlined for us their plan to do the self-assessment and a multi-phase plan that also includes inspections of agencies. And we are truly heartened by the renewed vigor that Dr. Ferriero is trying to bring to NARA, and I think he really is committed to these principles.

But the problem is that we have seen in NARA, under other archivists, that it has taken a very passive role and a very passive role of what its responsibilities are, so we think it is really critical that the responsibility and obligation, as well as the authority to oversee agencies, has to be made explicit in the legislation.

Mr. CLAY. And I certainly appreciate what you are saying; we need to bolster their authority through laws.

Ms. WEISMANN. Exactly.

Mr. CLAY. Out of curiosity, how would you treat the Federal Election Commission records and the candidate filings the same as

all other Federal records, or do you see a need for some type of special treatment there?

Ms. WEISMANN. I don't think there is any need for special treatment. And I recognize the sort of complexities in relying on a definition of what is a record and what isn't, but in large extent, within the Federal Government, each agency is going to decide what is a record based on its central mission, and I think there is already enough within the law itself to cover what entities like the Federal Election Commission should be preserving. So I don't necessarily see a basis for special treatment; I think it is more an issue of compliance.

Mr. CLAY. OK. Thank you very much.

We will now go to the gentlewoman from the District of Columbia, Ms. Norton.

Ms. NORTON. Thank you, Mr. Chairman. I do think this is a very important hearing. I regret that I was unable to be here for its beginning, and have only been able to come to hear part of what our second panel has had to say. I must say first that I really think that the government's responsibility for recordkeeping differs markedly from the private sector. The private sector shreds. The private sector wants to get rid of a lot of stuff, especially if they think we are coming.

But, actually, it is efficient for them to get rid of a great deal of what they have, and they are at pains to do it. They, of course, have to have some records, and they figure out, because it is an expense to keep records. They probably are better at figuring out which ones to keep and which ones not to keep, given the expense associated with it.

The Federal Government, on the other hand, has a governmental responsibility to maintain records that others would consider trivial, and somebody has to decide where that line gets drawn. This is often the history of important events are hidden in very small and seemingly trivial communications.

I was impressed by the figures provided us before this hearing, that almost 80 percent of agencies are either at high or moderate risk of improper destruction of records. That is very scary, the word destruction. That brought me to an interest I have had in the growing role of emails. There are some agencies, like those in the private sector, that communicate almost exclusively through emails. It is becoming often here, as elsewhere, the central mode of communication. Are there special challenges that are unique to email in recordkeeping by government? Ms. Brock or anyone else.

Ms. BROCK. Yes, ma'am, there are special challenges in managing email. Email has many components that can be hard to capture as a group. It is very hard to tell whether an email is a record or is not. For example, in GAO's Report 08742, our National Archives and selected agencies need to strengthen email management. They include this wonderful flowchart on whether or not it is an email, and it starts with, "is it a record" and it is ends with, "if in doubt, ask your records officer."

Now, if we each had one of these stickers on our computer, we would go crazy. But it does give us a flowchart for determining records status.

We do indeed conduct our entire lives on email, and the separation between reference, record, and personal correspondence is also very fuzzy.

Ms. NORTON. Somebody has to figure it out so there is some uniformity here. Of course, these agencies are very different, and you do not expect absolute uniformity, but you have to have some baseline to begin with as new forms of communication emerge. God help us when twittering becomes a major mode of communication.

Thank you very much, Mr. Chairman.

Mr. CLAY. Thank you, Ms. Norton.

Having no other questions, that will conclude this hearing. The hearing is adjourned.

[Whereupon, at 4:02 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

Wm. Lacy Clay, Chairman
Information Policy, Census, and National Archives
Subcommittee
Of the
Oversight and Government Reform Committee

Thursday, June 17, 2010
2154 Rayburn House Office Building
2:00 p.m.

"Federal Electronic Records Management: A Status Report"

ARMA International's

Information

Governance

Maturity

Model

GARP
ARMA INTERNATIONAL
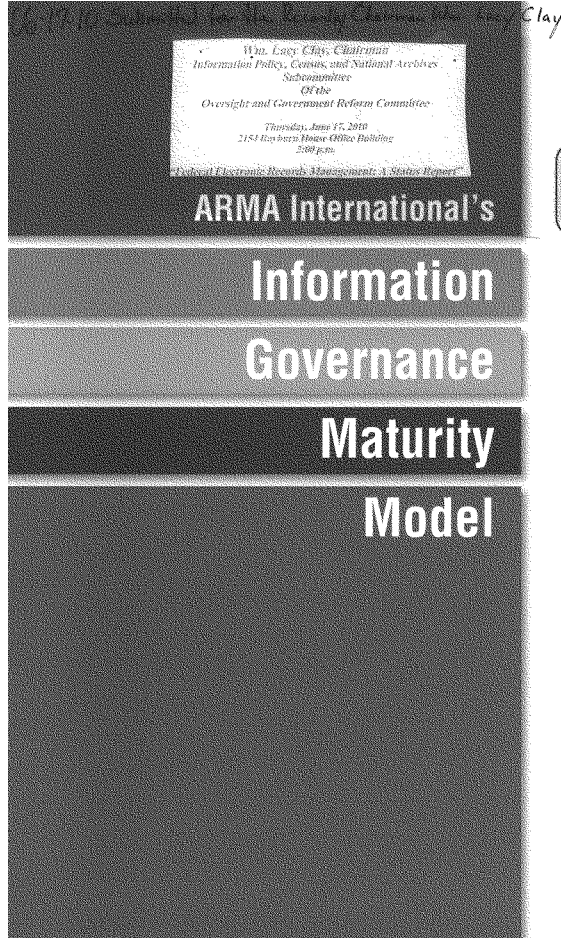
Information is one of the most vital, strategic assets organizations possess. They depend on information to develop products and services, make critical strategic decisions, protect property rights, propel marketing, manage projects, process transactions, service customers, and generate revenues. This critical information is contained in the organizations' business records.

It has not always been easy to describe what "good recordkeeping" looks like. Yet, this question gains in importance as regulators, shareholders, and customers are increasingly concerned about the business practices of organizations.
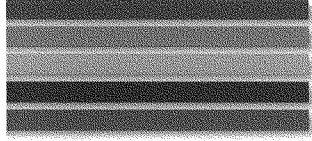
Generally Accepted Recordkeeping Principles® (GARP®) can guide:

- CEOs in determining how to protect their organizations in the use of information assets;

- Legislators in crafting legislation meant to hold organizations accountable; and

- Records management professionals in designing comprehensive and effective records management programs.

The GARP® principles identify the critical hallmarks of information governance, which Gartner describes as an accountability framework that "includes the processes, roles, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals."As such, they apply to all sizes of organizations, in all types of industries, and in both the private and public sectors. Multi-national organizations can also use GARP® to establish consistent practices across a variety of business units.

How to Use the Maturity Model

The Information Governance Maturity Model will assist an organization in conducting a preliminary evaluation of its recordkeeping programs and practices. Thoughtful consideration of the organization's practices should allow users to make an initial determination of the maturity of their organization's information governance.

Initially, it is not unusual for an organization to be at differing levels of maturity for the eight principles. It is also important to note that the maturity model represents an initial evaluation. In order to be most effective, a more in-depth analysis of organizational policies and practices may be necessary.

The maturity model will be most useful to leaders who wish to achieve the maximum benefit from their information governance practices. Effective information governance requires a continuous focus. But in order to get started, organizations can look to the steps below:

1. Identify the gaps between the organization's current practices and the desirable level of maturity for each principle.

2. Assess the risk(s) to the organization, based on the biggest gaps.

3. Determine whether additional information and analysis is necessary.

4. Develop priorities and assign accountability for further development of the program.

ARMA International has a variety of resources and assessment tools available that will help organizations take the next steps in improving their information governance practices. They can be located at *www.arma.org/GARP*.

A Picture of Effective Information Governance

The Information Governance Maturity Model begins to paint a more complete picture of what effective information governance looks like. It is based on the eight GARP® principles as well as a foundation of standards, best practices, and legal/regulatory requirements.

The maturity model goes beyond a mere statement of the principles by beginning to define characteristics of various levels of recordkeeping programs. For each principle, the maturity model associates various characteristics that are typical for each of the five levels in the model:

- **LEVEL 1 (Sub-Standard):** This level describes an environment where recordkeeping concerns are either not addressed at all, or are addressed in a very ad hoc manner. Organizations that identify primarily with these descriptions should be concerned that their programs will not meet legal or regulatory scrutiny.

- **LEVEL 2 (In Development):** This level describes an environment where there is a developing recognition that recordkeeping has an impact on the organization, and that the organization may benefit from a more defined information governance program. However, in Level 2, the organization is still vulnerable to legal or regulatory scrutiny since practices are ill-defined and still largely ad hoc in nature.

- **LEVEL 3 (Essential):** This level describes the essential or minimum requirements that must be addressed in order to meet the organization's legal and regulatory requirements. Level 3 is characterized by defined policies and procedures, and more specific decisions taken to improve recordkeeping. However, organizations that identify primarily with Level 3 descriptions may still be missing significant opportunities for streamlining business and controlling costs.

- **LEVEL 4 (Proactive):** This level describes an organization that is initiating information governance program improvements throughout its business operations. Information governance issues and considerations are integrated into business decisions on a routine basis, and the organization easily meets its legal and regulatory requirements. Organizations that identify primarily with these descriptions should begin to consider the business benefits of information availability in transforming their organizations globally.

- **LEVEL 5 (Transformational):** This level describes an organization that has integrated information governance into its overall corporate infrastructure and business processes to such an extent that compliance with the program requirements is routine. These organizations have recognized that effective information governance plays a critical role in cost containment, competitive advantage, and client service.

ARMA International's Information Governance Maturity Model

GARP® Principle	LEVEL 1 (Sub-Standard)	LEVEL 2 (In Development)
Accountability A senior executive (or person of comparable authority) oversees the recordkeeping program and delegates program responsibility to appropriate individuals. The organization adopts policies and procedures to guide personnel, and ensure the program can be audited.	No senior executive (or person of comparable authority) is responsible for the records management program. The records manager role is largely non-existent or is an administrative and/or clerical role distributed among general staff.	No senior executive (or person of comparable authority) is involved in or responsible for the records management program. The records manager role is recognized, although he/she is responsible for tactical operation of the existing program. In many cases, the existing program covers paper records only. The information technology function or department is the de facto lead for storing electronic information, but this is not done in a systematic fashion. The records manager is not involved in discussions of electronic systems.
Transparency The processes and activities of an organization's recordkeeping program are documented in a manner that is open and verifiable and is available to all personnel and appropriate interested parties.	It is difficult to obtain information about the organization or its records in a timely fashion. No clear documentation is readily available. There is no emphasis on transparency. Public requests for information, discovery for litigation, regulatory responses, or other requests (e.g., from potential business partners, investors, or buyers) cannot be readily accommodated. The organization has not established controls to ensure the consistency of information disclosure. Business processes are not well-defined.	The organization realizes that some degree of transparency is important in its recordkeeping for business or regulatory needs. Although a limited amount of transparency exists in areas where regulations demand transparency, there is no systematic or organization-wide drive to transparency.
Integrity A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.	There are no systematic audits or defined processes for showing the origin and authenticity of a record. Various organizational functions use ad hoc methods to demonstrate authenticity and chain of custody, as appropriate, but their trustworthiness cannot easily be guaranteed.	Some organizational records are stored with their respective metadata that demonstrate authenticity; however, no formal process is defined for metadata storage and chain of custody. Metadata storage and chain of custody methods are acknowledged to be important, but are left to the different departments to handle as they determine is appropriate.
Protection A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.	No consideration is given to record privacy. Records are stored haphazardly, with protection taken by various groups and departments with no centralized access controls. Access controls, if any, are assigned by the author.	Some protection of records is exercised. There is a written policy for records that require a level of protection (e.g., personnel records). However, the policy does not give clear and definitive guidelines for all records in all media types. Guidance for employees is not universal or uniform. Employee training is not formalized. The policy does not address how to exchange these records between employees. Access controls are still implemented by individual record owners.

© 2010 ARMA International
Note: Records management terms used in the GARP® Information Governance Maturity Model are defined in the *Glossary of Records and Information Management Terms, 3rd Edition* (ARMA International, 2007).

3

LEVEL 3 (Essential)	LEVEL 4 (Proactive)	LEVEL 5 (Transformational)
The records manager is an officer of the organization and is responsible for the tactical operation of the ongoing program on an organization-wide basis. The records manager is actively engaged in strategic information and record management initiatives with other officers of the organization. Senior management is aware of the program. The organization has defined specific goals related to accountability.	The records manager is a senior officer responsible for all tactical and strategic aspects of the program. A stakeholder committee representing all functional areas and chaired by the records manager meets on a periodic basis to review disposition policy and other records management-related issues. Records management activities are fully sponsored by a senior executive.	The organization's senior management and its governing board place great emphasis on the importance of the program. The records management program is directly responsible to an individual in the senior level of management, (e.g., chief risk officer, chief compliance officer, chief information officer) OR, A chief records officer (or similar title) is directly responsible for the records management program and is a member of senior management for the organization. The organization's stated goals related to accountability have been met.
Transparency in recordkeeping is taken seriously and information is readily and systematically available when needed. There is a written policy regarding transparency. Employees are educated on the importance of transparency and the specifics of the organization's commitment to transparency. The organization has defined specific goals related to transparency.	Transparency is an essential part of the corporate culture and is emphasized in training. The organization monitors compliance on a regular basis.	The organization's senior management considers transparency as a key component of information governance. The organization's stated goals related to transparency have been met. The organization has implemented a continuous improvement process to ensure transparency is maintained over time. Software tools that are in place assist in transparency. Requestors, courts, and other legitimately interested parties are consistently satisfied with the transparency of the processes and the response.
The organization has a formal process to ensure that the required level of authenticity and chain of custody can be applied to its systems and processes. Appropriate data elements to demonstrate compliance with the policy are captured. The organization has defined specific goals related to integrity.	There is a clear definition of metadata requirements for all systems, business applications, and paper records that are needed to ensure the authenticity of records. Metadata requirements include security and signature requirements and chain of custody as needed to demonstrate authenticity. The metadata definition process is an integral part of the records management practice in the organization.	There is a formal, defined process for introducing new record-generating systems and the capture of their metadata and other authenticity requirements, including chain of custody. This level is easily and regularly audited. The organization's stated goals related to integrity have been met. The organization can consistently and confidently demonstrate the accuracy and authenticity of its records.
The organization has a formal written policy for protecting records and centralized access controls. Confidentiality and privacy are well defined. The importance of chain of custody is defined, when appropriate. Training for employees is available. Records and information audits are only conducted in regulated areas of the business. Audits in other areas may be conducted, but are left to the discretion of each function area. The organization has defined specific goals related to record protection.	The organization has implemented systems that provide for the protection of the information. Employee training is formalized and well documented. Auditing of compliance and protection is conducted on a regular basis.	Executives and/or senior management and the board place great value in the protection of information. Audit information is regularly examined and continuous improvement is undertaken. The organization's stated goals related to record protection have been met. Inappropriate or inadvertent information disclosure or loss incidents are rare.

ARMA International's Information Governance Maturity Model

GARP® Principle	LEVEL 1 (Sub-Standard)	LEVEL 2 (In Development)
Compliance The recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies.	There is no clear definition of the records the organization is obligated to keep. Records and other business documentation are not systematically managed according to records management principles. Various groups of the organization define this to the best of their ability based on their interpretation of rules and regulations. There is no central oversight and no consistently defensible position. There is no defined or understood process for imposing "holds."	The organization has identified the rules and regulations that govern its business and introduced some compliance policies and recordkeeping practices around those policies. Policies are not complete and there is no apparent or well-defined accountability for compliance. There is a hold process, but it is not well-integrated with the organization's information management and discovery processes.
Availability An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.	Records are not readily available when needed and/or it is unclear who to ask when records need to be produced. It takes time to find the correct version, the signed version, or the final version, if it can be found at all. The records lack finding aides: indices, metadata, and locators. Legal discovery is difficult because it is not clear where information resides or where the final copy of a record is located.	Record retrieval mechanisms have been implemented in certain areas of the organization. In those areas with retrieval mechanisms, it is possible to distinguish between official records, duplicates, and non-record materials. There are some policies on where and how to store official records, but a standard is not imposed across the organization. Legal discovery is complicated and costly due to the inconsistent treatment of information.
Retention An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.	There is no current documented records retention schedule. Rules and regulations that should define retention are not identified or centralized. Retention guidelines are haphazard at best. In the absence of retention schedules, employees either keep everything or dispose of records based on their own business needs, rather than organizational needs.	A retention schedule is available, but does not encompass all records, did not go through official review, and is not well known around the organization. The retention schedule is not regularly updated or maintained. Education and training about the retention policies are not available.
Disposition An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.	There is no documentation of the processes, if any, that are used to guide the transfer or disposition of records. The process for suspending disposition in the event of investigation or litigation is non-existent or is inconsistent across the organization.	Preliminary guidelines for disposition are established. There is a realization of the importance of suspending disposition in a consistent manner, repeatable by certain legal groupings. There may or may not be enforcement and auditing of disposition.

© 2010 ARMA International

Note: Records management terms used in the GARP® Information Governance Maturity Model are defined in the *Glossary of Records and Information Management Terms, 3rd Edition* (ARMA International, 2007).

5

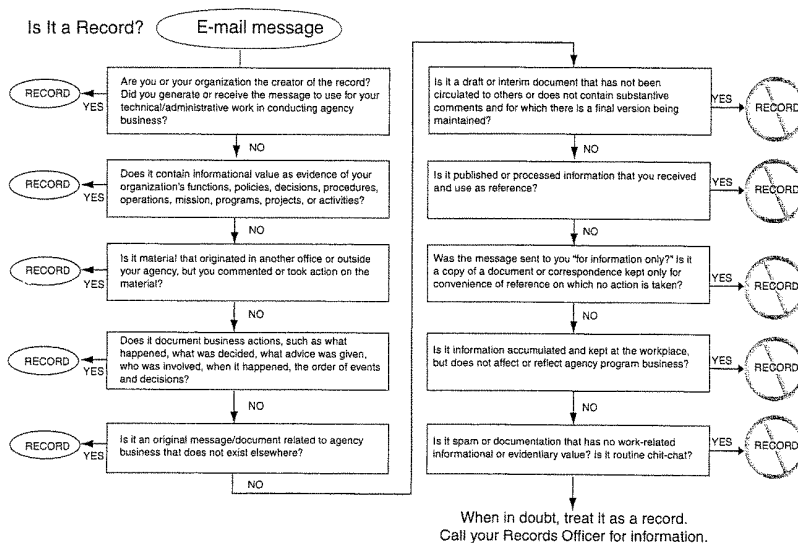| LEVEL 3 (Essential)	LEVEL 4 (Proactive)	LEVEL 5 (Transformational)
The organization has identified all relevant compliance laws and regulations. Record creation and capture are systematically carried out in accordance with records management principles. The organization has a strong code of business conduct which is integrated into its overall information governance structure and recordkeeping policies. Compliance and the records that demonstrate it are highly valued and measurable. The hold process is integrated into the organization's information management and discovery processes for the "most critical" systems. The organization has defined specific goals related to compliance.	The organization has implemented systems to capture and protect records. Records are linked with the metadata used to demonstrate and measure compliance. Employees are trained appropriately and audits are conducted regularly. Records of the audits and training are available for review. Lack of compliance is remedied through implementation of defined corrective actions. The hold process is well-managed with defined roles and a repeatable process that is integrated into the organization's information management and discovery processes.	The importance of compliance and the role of records and information in it are clearly recognized at the senior management and board levels. Auditing and continuous improvement processes are well-established and monitored by senior management. The roles and processes for information management and discovery are integrated. The organization's stated goals related to compliance have been met. The organization suffers few or no adverse consequences based on information governance and compliance failures.
There is a standard for where and how official records and information are stored, protected, and made available. Record retrieval mechanisms are consistent and contribute to timely records retrieval. Most of the time, it is easy to determine where to find the authentic and final version of any record. Legal discovery is a well-defined and systematic business process. The organization has defined specific goals related to availability.	There are clearly defined policies regarding storage of records and information. There are clear guidelines and an inventory that identifies and defines the systems and their information assets. Records and information are consistently and readily available when needed. Appropriate systems and controls are in place for legal discovery. Automation is adopted to facilitate the implementation of the hold process.	The senior management and board levels provide support to continually upgrade the processes that affect record availability. There is an organized training and continuous improvement program. The organization's stated goals related to availability have been met. There is a measurable ROI to the business as a result of records availability.
A formal retention schedule that is tied to rules and regulations is consistently applied throughout the organization. The organization's employees are knowledgeable about the retention schedule and they understand their personal responsibilities for records retention. The organization has defined specific goals related to retention.	Employees understand how to classify records appropriately. Retention training is in place. Retention schedules are reviewed on a regular basis, and there is a process to adjust retention schedules as needed. Records retention is a major corporate concern.	Retention is an important item at the senior management and board levels. Retention is looked at holistically and is applied to all information in an organization, not just to official records. The organization's stated goals related to retention have been met. Information is consistently retained for appropriate periods of time.
Official procedures for records disposition and transfer are developed. Official policy and procedures for suspending disposition have been developed. Although policies and procedures exist, they are not standardized across the organization. Individual departments have devised alternative procedures to suit their particular business needs. The organization has defined specific goals related to disposition.	Disposition procedures are understood by all and are consistently applied across the enterprise. The process for suspending disposition due to legal holds is defined, understood, and used consistently across the organization. Electronic information is expunged, not just deleted, in accordance with retention policies.	The disposition process covers all records and information in all media. Disposition is assisted by technology and is integrated into all applications, data warehouses, and repositories. Disposition processes are consistently applied and effective. Processes for disposition are regularly evaluated and improved. The organization's stated goals related to disposition have been met.

120
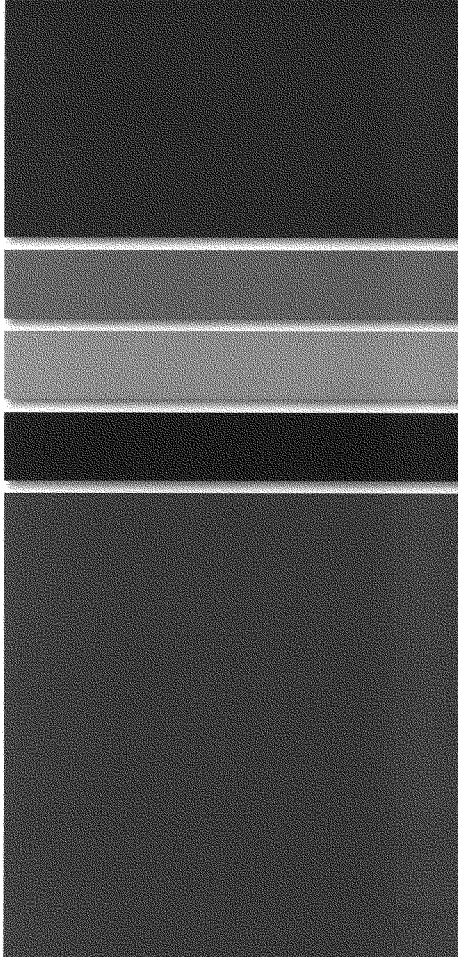
06-17-10 Submitted For The Record by Chairman Wm. Lacy Clay

Wm. Lacy Clay, Chairman
Information Policy, Census and National Archives
Subcommittee
Of the
Oversight and Government Reform Committee

Thursday, June 17, 2010
2154 Rayburn House Office Building
2:00 p.m.

"Federal Electronic Records Management: A Status Report"

Figure 1: Example Decision Tree for Determining Whether an E-Mail Message Is a Record

Is It a Record? — E-mail message

RECORD YES — Are you or your organization the creator of the record? Did you generate or receive the message to use for your technical/administrative work in conducting agency business?

NO

RECORD YES — Does it contain informational value as evidence of your organization's functions, policies, decisions, procedures, operations, mission, programs, projects, or activities?

NO

RECORD YES — Is it material that originated in another office or outside your agency, but you commented or took action on the material?

NO

RECORD YES — Does it document business actions, such as what happened, what was decided, what advice was given, who was involved, when it happened, the order of events and decisions?

NO

RECORD YES — Is it an original message/document related to agency business that does not exist elsewhere?

NO

Is it a draft or interim document that has not been circulated to others or does not contain substantive comments and for which there is a final version being maintained? YES RECORD

NO

Is it published or processed information that you received and use as reference? YES RECORD

NO

Was the message sent to you "for information only?" Is it a copy of a document or correspondence kept only for convenience of reference on which no action is taken? YES RECORD

NO

Is it information accumulated and kept at the workplace, but does not affect or reflect agency program business? YES RECORD

NO

Is it spam or documentation that has no work-related informational or evidentiary value? Is it routine chit-chat? YES RECORD

When in doubt, treat it as a record.
Call your Records Officer for information.

Source: NARA Toolkit for Managing Electronic Records. Adapted from Anna W. Nusbaum, Sandia National Laboratories.

Second, the transmission data associated with an e-mail record—including information about the senders and receivers of messages, the date the message was sent, and any attachments to the messages—provide context that may be crucial to understanding the message. Thus, as NARA's e-mail regulations and guidance reflect, transmission data must be retained, and attachments are defined as part of the e-mail record.

Third, a given message may be part of an exchange of messages between two or more people within or outside an agency, or even of a string (sometimes branching) of many messages sent and received on a given