THE NATIONAL ARCHIVES' ABILITY TO SAFEGUARD THE NATION'S ELECTRONIC RECORDS

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

FIRST SESSION

NOVEMBER 5, 2009

Serial No. 111–63

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

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.oversight.house.gov

U.S. GOVERNMENT PRINTING OFFICE

57–622 PDF WASHINGTON : 2010

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

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
MARK E. SOUDER, Indiana
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
ANH "JOSEPH" CAO, Louisiana

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
DIANE E. WATSON, California
HENRY CUELLAR, Texas

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

DARRYL PIGGEE, *Staff Director*

CONTENTS

THE NATIONAL ARCHIVES' ABILITY TO SAFEGUARD THE NATION'S ELECTRONIC RECORDS

THURSDAY, NOVEMBER 5, 2009

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 2:40 p.m., in room 2154, Rayburn House Office Building, Hon. Wm. Lacy Clay (chairman of the subcommittee) presiding.

Present: Representatives Clay, Driehaus, Watson, Cuellar, and McHenry.

Staff present: Darryl Piggee, staff director/counsel; Jean Gosa, clerk; Yvette Cravins, counsel; Frank Davis and Anthony Clark, professional staff members; Charisma Williams, staff assistant; Leneal Scott, information systems specialist (full committee); Adam Fromm, minority chief clerk and Member liaison; and Chapin Fay and Jonathan Skladany, minority counsels.

Mr. CLAY. The hearing will come to order. Good afternoon. And the Information Policy, Census, and National Archives Subcommittee of the Oversight and Government Reform Committee, will now come to order.

Without objection, the Chair 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 oversight hearing on the "National Archives' Ability to Safeguard the Nation's Electronic Records." The purpose of today's hearing is to examine the National Archives' policies and procedures to protect the Nation's ever-increasing store of electronic records.

We will consider several important topics, including an update on the theft or loss from NARA of a portable hard drive containing Clinton administration electronic records; possible breaches of electronic records containing personally identifiable information from NARA operating systems; and the status of the largest IT project in NARA's history, the Electronic Records Archives [ERA].

ERA, fully implemented, would cost well over a half a billion dollars. Over the last 10 years or more, NARA has tried with varied success not only to develop and test a system but even to define its scope.

This subcommittee is concerned that such a large and expensive information system is being developed in an agency that is already struggling with managing the security of the systems they currently operate. The theft or loss of the Clinton hard drive was very disturbing and we look forward to hearing the status of the agency's efforts to identify and notify any and all individuals whose PII may have been compromised.

It is more troubling, however, to hear of new instances of data breaches, or possible breaches. The circumstances and the agency's handling of them casts doubt on the National Archives' ability to understand and mitigate existing and emerging risk in order to properly safeguard the Nation's electronic records.

It is this subcommittee's hope that through our hearing today, we can gain a better understanding of NARA's information technology security, and provide the National Archives with some important information and direction they can use in order to increase IT security across the agency.

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

Statement
Of
Chairman Wm. Lacy Clay

Information Policy, Census, and National Archives Subcommittee
Oversight and Government Reform Committee

Hearing on: "The National Archives' Ability to Safeguard the Nation's Electronic Records"

Thursday, November 5, 2009
2154 Rayburn HOB
2:00 p.m.

Welcome to today's oversight hearing on "The National Archives' Ability to Safeguard the Nation's Electronic Records."

The purpose of today's hearing is to examine the National Archives', or NARA's, policies and procedures to protect the nation's ever-increasing store of electronic records. We will consider several important topics, including an update on the theft or loss from NARA of a portable hard drive containing Clinton Administration electronic records; possible breaches of electronic records containing Personally-Identifiable Information (P.I.I.) from NARA-operated systems; and the status of the largest IT project in NARA's history, the Electronic Records Archive, or E.R.A.

E.R.A., when fully implemented, will cost well over half a billion dollars. Over the last ten years or more, NARA has tried, with varied success, not only to develop and test this system, but even to define its scope. This Subcommittee is concerned that such a large and expensive information

system is being developed in an agency that is already struggling with managing the security of the systems they currently operate. The theft or loss of the Clinton hard drive was very disturbing, and we look forward to hearing the status of the agency's efforts to identify and notify any and all individuals whose P.I.I. may have been compromised.

It is more troubling, however, to hear of new instances of data breaches or possible breaches. The circumstances, and the agency's handling of them, cast doubt on the National Archive's ability to understand and mitigate existing and emerging risks in order to properly safeguard the nation's electronic records.

It is this Subcommittee's hope that through our hearing today we can gain a better understanding of NARA's information technology security, and provide the National Archives with some important information and direction they can use in order to increase IT security across the agency.

Mr. CLAY. I would like to introduce our panel. Our first witness will be Adrienne Thomas, the Acting Archivist of the United States. Prior to her appointment as Acting Archivist in December 2008, Ms. Thomas served as the Deputy Archivist of the United States. Ms. Thomas has been with the National Archives for 38 years, beginning as an Archivist trainee in the Office of Presidential Libraries, and subsequently holding a number of policy and administrative roles. And thank you for being here.

Our next witness is Paul Brachfeld, the Inspector General of the NARA Administration. Mr. Brachfeld previously worked for the Federal Communications Commission where he served as Assistant Inspector General for Audits. During his 8 years' tenure at the FCC, he also served 10 years as Acting Assistant Inspector General for Investigations. Mr. Brachfeld also served as Director of Audits for the Federal Election Commission Office of the Inspector General.

After Mr. Brachfeld, we will hear from David Powner, the Director of IT Management Issues at the GAO. Mr. Powner is currently responsible for a large segment of GAO's information technology work, including systems development, IT investment, management health IT, and Cyber Critical Infrastructure Protection Reviews. He has led teams reviewing major IT modernization efforts at Cheyenne Mountain Air Force Station, the National Weather Service, the FAA and the IRS. Thank you for being here, Mr. Powner.

And our final witness will be Alan Brill, the senior managing director for technology services at Kroll Ontrack, an industry leader in computer forensics and investigation. Mr. Brill is recognized internationally as a leader in his fields of security, computer forensics, and incident response. Mr. Brill founded Kroll Ontrack global high-technology investigation practice. He has an international reputation in the areas of computer communications security and technology crime investigation.

I thank all of you for being here today and appearing before us for 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. And let the record reflect that the witnesses answered in the affirmative. I ask that each of the witnesses now give a brief summary of their testimony. Please limit your summary to 5 minutes and your complete written statement will be included in the hearing record.

Before we go to Ms. Thomas, we would like to ask the ranking member if he has an opening statement.

Mr. MCHENRY. Thank you, Mr. Chairman, I do. Thank you so much for continuing to hold good hearings with this subcommittee. I appreciate your leadership.

In May of this year, this subcommittee first met to discuss the staggering negligence of National Archives staff in handling our Nation's valuable records, an issue that was only just coming to light at the time. We're back again. But back then we were shocked to hear that a 2 terabyte hard drive had disappeared from the Archives' storage room where it was kept in an unsecured location, accessible by many employees.

That device contained the personally identifiable information of hundreds of thousands of Clinton administration staff, Secret Service operating procedures, and other highly sensitive information. Although it was clear that there were endemic problems with National Archives' management, it appeared that this loss was an isolated incident and an Acting Archivist assured this committee that measures were being taken to address security concerns and prevent any further breaches.

That, unfortunately, is not the case. Now, 6 months down the road, we're back here again, with more news of lost electronic storage devices, one of which contains the personally identifiable information of our Nation's military veterans on a drive that was sent out to an outside contractor for maintenance and repair. What's more is that this breach occurred a year ago, in November 2008, and we're only hearing about it now. I'm practically speechless.

It is my sincerest hope that, Ms. Thomas, you will tell us today that the Archives is doing everything possible to ensure that these veterans do not become victims of identity theft.

The National Archives staff exposed this drive to loss or theft because they believed it was defective and beyond repair. Further—they further claim that sending a drive containing sensitive information to a third party doesn't constitute a breach of sensitive information, because the contractor is obligated to keep its contents private.

As the Inspector General of the National Archives will testify today, the data on this drive is actually retrievable, using free, publicly available software. In fact, some of my staff have performed procedures very similar to that. Exposing a drive like that to eyes outside of the National Archives is irresponsible, regardless of the technical definition of a breach.

The National Archives has further claimed to the subcommittee staff that breaches of this nature will not happen going forward, because a policy is now in place that prohibits drives from being sent out to contractors for repair. However, this policy was actually already in place at the time the drive with veterans' data was exposed. So that's nothing more than cover for the past and not real substantive change to ensure this doesn't happen in the future.

The policy also did not prevent the National Archives from sending yet another drive containing sensitive records to a contractor under similar circumstances in April 2009. That drive contained digitized employee files from the National Archives, GSA, and OPM. It is unacceptable that the NARA staff handle any storage devices this carelessly, but it is particularly disturbing that they are so haphazard with the Social Security and military identification numbers of our veterans who have sacrificed so much for this country.

National Archives already uses strict protocols to safeguard this information contained in Defense Department files in its possession. Had these same protocols been used for veterans' data, this incident would have been avoided, in my opinion.

What is clear is that there is a greater institutional problem at the Archives that must be fixed, and that is culture of blatant disregard. It's become very clear that the ongoing security breaches

are not the result of a lack of awareness of security procedure by staff, but a failure at the managerial level to enforce the procedure.

Finally, we will also hear from our witnesses about the National Archives' Electronic Records Archive. As in the case with NARA as a whole, the ERA is plagued with its own problems. The ERA, which is the Archives' strategic initiative to preserve uniquely valuable electronic records in the U.S. Government, is in the midst of a system development that is already running far over budget. When fully operational, it will cost $500 million more than projected.

The GAO has already been critical of this system, citing methodological weaknesses that could limit NARA's ability to accurately report on cost schedules and performances, and concluding that NARA lacks a proper contingency plan should the electronic record system fail. This really makes me question the investment overall.

I thank our witnesses for appearing today. I certainly appreciate and am very interested in Ms. Thomas' testimony about this recent security breach and what sort of measures are being taken, if any, to say that this will not happen in the future.

Thank you, Mr. Chairman, for your leadership and I yield back.

Mr. CLAY. Thank you, Mr. McHenry, for your opening statement.

[The prepared statement of Hon. Patrick T. McHenry follows:]

Statement of Ranking Member Patrick McHenry
Subcommittee on Information Policy, Census, and National Archives
"The National Archives' Ability to Safeguard the Nation's Electronic Records"
November 5, 2009

Thank you, Mr. Chairman, for holding this very important hearing.

In May of this year, this Subcommittee first met to discuss the staggering negligence of National Archives staff in handling our nation's valuable records, an issue that was only just coming to light at the time. Back then, we were shocked to hear that a 2 terabyte hard drive had disappeared from an Archives storage room where it was kept in an unsecure location accessible by countless employees. That device contained the personally identifiable information of thousands of Clinton Administration staff, Secret Service operating procedures, and other highly sensitive information.

Although it was clear that there were endemic problems with NARA's management, it appeared this loss was an isolated incident and the Acting Archivist assured this committee that

measures were being taken to address security concerns and prevent any further breaches.

That, unfortunately, is not the case. Now, six months down the road, we're back here again with ***more*** news of mishandled electronic storage devices – one of which contains the personally identifiable information of our nation's veterans on a drive that was sent to an outside contractor for maintenance and repair. What's more is that this breach occurred a year ago in November of 2008 and we're only hearing about it now. I'm practically speechless. It is my sincerest hope that Acting Archivist Thomas will tell us today that the Archives is doing everything possible to ensure these veterans do not become victims of identity theft.

NARA staff exposed this drive to loss or theft because they believed it was defective and beyond repair. NARA further claims that sending a drive containing sensitive information to a third party doesn't constitute a "breach" of sensitive information because the contractor is obligated to keep its contents private. As the Inspector General of the National Archives will testify

today, the data on this drive is actually retrievable using free, publicly available software. Exposing a drive like that to eyes outside NARA is irresponsible, regardless of the technical definition of a breach.

NARA has further claimed to Subcommittee staff that breaches of this nature will not happen going forward because a policy is now in place that prohibits drives from being sent out to contractors for repair. However, this policy was actually ***already*** in place at the time the drive with veterans' data was exposed.

The policy also did not prevent NARA from sending yet another drive containing sensitive records to a contractor under similar circumstances in April 2009. That drive contained digitized employee files from NARA, GSA, and OPM.

It is unacceptable that NARA staff handle ***any*** storage devices this carelessly, but it's particularly disturbing that they are so haphazard with the Social Security and military identification numbers of veterans who have sacrificed so much

for our country. NARA already uses strict protocols to safeguard the information contained in Department of Defense files in its possession – had these same protocols been used for veterans' data, this incident would have been avoided.

What is clear is that there is a greater institutional problem at the Archives that must be fixed, and that is a culture of blatant disregard. It's become pretty clear that the ongoing security breaches are not the result of a lack of *awareness* of security procedure by staff, but a failure at the managerial level to *enforce* procedure.

Finally, we will also hear from our witnesses about NARA's Electronic Records Archive. As is the case with NARA as a whole, the ERA is plagued with problems. The ERA, which is the Archives' "strategic initiative to preserve uniquely valuable electronic records of the U.S. government," is in the midst of system development and is already running far over budget. When fully operational, it will have cost $500 million dollars more than projected. The GAO has already been critical of this system, citing "methodological weaknesses that

could limit NARA's ability to accurately report on cost schedules and performance" and concluding that NARA lacks a proper contingency plan should the electronic record system fail. According to his testimony, Inspector General Brachfeld has even been voicing profound concerns about the ERA since 2002. This really makes me question the investment.

I thank our witnesses for appearing today and I am very interested to hear from Ms. Thomas about these most recent security breaches and what sort of measures are being taken – if any, I think it's fair to say – to prevent a recurrence.

Mr. CLAY. I also want to recognize four special guests that we have here today in the front row, who are here to see their government in action. One is Dr. Kelly Woestman of Pittsburgh State University, as well as Jerry Handfield, the State Archivist for the State of Washington, Andy Maltz, who is the director of Science and Technology Council for the Pickford Center for Motion Picture Study, and David McMillen, NARA external affairs liaison.

Welcome to all of you and all the other ladies and gentlemen in the audience today.

Ms. Thomas we will begin it with your testimony.

STATEMENTS OF ADRIENNE THOMAS, ACTING ARCHIVIST OF THE UNITED STATES, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION; PAUL BRACHFELD, INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION; DAVID POWNER, DIRECTOR, GOVERNMENT ACCOUNTABILITY OFFICE, INFORMATION TECHNOLOGY MANAGEMENT ISSUES; AND ALAN E. BRILL, KROLL ONTRACK, SENIOR MANAGING DIRECTOR FOR TECHNOLOGY SERVICES

STATEMENT OF ADRIENNE THOMAS

Ms. THOMAS. Chairman Clay, Ranking Member McHenry, and members of subcommittee, thank you for this opportunity to discuss the National Archives and Records Administration's safeguarding of electronic records.

At NARA we recognize that the challenge of securing IT systems and devices, particularly in regard to protecting personally identifiable information, is never-ending and always changing. We know that no agency will ever be perfect, but we're committed to doing the best job that we can, learning from our own mistakes and the mistakes of others.

I appreciate Paul Brachfeld, NARA's Inspector General, and David Powner of the Government Accountability Office are appearing alongside me today. NARA's Office of the Inspector General has reported a number of vulnerabilities and made important recommendations on how we can improve our security. In response to their work we've declared a material weakness with respect to IT security, and we are taking corrective actions.

Later in my testimony, I will update you on the Electronic Records Archives which regularly receives useful guidance from the GAO and has from the very start of the ERA development.

In late September, I was briefed by the Inspector General on an allegation that NARA may have improperly disclosed sensitive personally identifiable information when a defective disk drive from a veterans' information data base was sent to an authorized contractor for repair in the fall of 2008, rather than being destroyed and disposed of at a NARA facility, according to a new policy that had been issued by the CAO in August 2008.

The defective disk drive supports the case management reporting system [CMRS]. CMRS is used by NARA's Military Personnel Record Center to track over a million requests annually for the personnel records of veterans, but the system hardware resides in College Park, MD.

On October 9th we learned that an additional hard drive at our National Personnel Record Center in St. Louis was returned to a vendor in April 2009. The drive is from a system that is used to digitize official personnel files of current government employees, and we believe it contained digitized files and an associated index of current employees' records from NARA, the General Services Administration and the Office of Personnel Management.

NARA and the Inspector General continue to review these incidents. However, at this time, there is no evidence that the defective disk drives were ever in unauthorized hands or that any PII was accessed from these disks. And my staff and I have concluded that there was no PII breach.

We have implemented many recommendations made by the Inspector General to improve PII security at the NPRC, including removing older data from the CMRS system, performing annual reviews of CMRS user accounts, compiling updated key inventories to better protect PII stored on paper, and issuing policy changes to require verification of data before providing military records to next of kin.

In light of these two hard drive maintenance incidents, we are taking a comprehensive look at the internal security controls related to the protection of PII within IT systems across NARA. We have undertaken an agency-wide systematic review of the storage and protection of PII that includes a review of data base encryption within the system, a review of our tape backup procedures, a review of all of our computer acquisition and maintenance contracts to ensure that sensitive data protection is properly addressed, and a review of our internal PII awareness and training processes and procedures.

We are also ensuring that we use National Security Agency-approved media, sanitation, and destruction procedures, and have engaged expert consultants to review our IT security incident response procedures.

In order to identify ways to improve security and internal controls with regards to electronic records, NARA has conducted an internal audit to identify how well our ITT security program is functioning. This audit identified 29 recommendations for improvement in NARA's IT security program. Since then, we have doubled our IT security staff and much progress has been made in the area of strengthening our IT security controls.

My written testimony describes many additional corrective actions that NARA is undertaking to improve IT security. Most of the original 25—29 recommendations have been completed, and we continue to work on the remaining actions.

You also asked that I provide an update on our response to the external hard drive containing copies of Clinton administration Executive Office of the President data that we discovered missing in March 2009 from NARA's College Park facility. The drive is still missing. It contains names, dates of birth, and Social Security numbers of people who worked in the Clinton Executive Office of the President, visited the White House complex, or submitted personal information to the White House in pursuit of a job or a political appointment.

To date, NARA has mailed approximately 26,000 breach notification letters to individuals whose names and Social Security numbers are on the hard drive. We have offered these individuals 1 year of free credit monitoring. So far, 1,685 persons have taken advantage of the offer. Our contractors are continuing to search the hard drive for additional names of individuals whose identity might have been compromised. We anticipate mailing an additional 120,000 letters in the coming weeks.

Finally, you asked that I report on the status of the Electronic Records Archives [ERA]. ERA is a comprehensive systematic and dynamic means for providing electronic records that would be free from independent—from dependence on any specific hardware or software. The primary purpose of this first-of-a-kind system is to take in, store, and provide access to records that are born digital, by which we mean the permanent archival electronic records created by executive branch agencies, the Congress, Federal courts, and the Office of the President.

We are currently beginning year 5 and increment 3 of this 7-year, 5-increment system development project. NARA staff is now using increment 1 to ingest electronic records from legacy NARA systems and to schedule transfer records from four agencies serving a pilot capacity for ERA.

Increment 2 of ERA provided support for the transfer of the electronic Presidential records from the Executive Office of the Bush administration so that we could preserve and make these records accessible for archival processing. Increment 2 was delivered in December 2008 to enable NARA to begin the ingest of 72.32 terabytes of data that legally transferred to NARA as of January 20, 2009. Ingest of these unclassified electronic records was completed in October 2009.

Funding in NARA's 2010 budget is dedicated to increment 3 of NARA, which includes a congressional records instance to provide simplified storage and access capabilities for the electronic records of Congress. This part of increment 3 is on schedule and will be delivered to NARA in February 2010.

Increment 3 also provides the capability for the public to accept access records in ERA. The subcommittee should know, however, that the start of increment 3 development has not been as smooth as desired. NARA has raised several concerns with the contractor related to analysis, design, and architectural foundation issues. The contractor was receptive to NARA's input and has taken concrete steps to make improvements in process, deliverables and staff. At present, the contractor believes it can deliver increment 3 as scheduled. But you can rest assured that NARA will continue to monitor progress to ensure that increment 3 will be delivered within cost and schedule.

In summary, ERA is operating in the way that we now expect it to at this point in the project. Federal and Presidential records are stored in the ERA, which operates securely at a facility on the grounds of U.S. Navy's Allegheny Ballistic Lab in Rocket Center, WV. Hardware and software failures have been minimum. We have a staged plan to open the system up to Federal agencies. The problems we encounter are common to major IT systems development, but I am confident in the ability of the ERA program office to man-

age the development of ERA to a successful conclusion and to plan for the ongoing operational phase of ERA after 2012.

Mr. Chairman—that concludes my testimony. I would like to thank you for inviting me here today and for the helpful oversight and guidance you and the members of this subcommittee provide to NARA.

Mr. CLAY. Thank you so much.

[The prepared statement of Ms. Thomas follows:]

TESTIMONY
OF
ADRIENNE THOMAS
ACTING ARCHIVIST OF THE UNITED STATES

INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES SUBCOMMITTEE

OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

THURSDAY, NOVEMBER 5, 2009
2154 RAYBURN HOB
2:00 P.M.

"THE NATIONAL ARCHIVES' ABILITY TO SAFEGUARD THE NATION'S ELECTRONIC RECORDS"

Chairman Clay, Ranking Member McHenry, and Members of the Subcommittee, I am Adrienne Thomas, Acting Archivist of the United States. Thank you for this opportunity to appear before you to discuss the National Archives and Records Administration's (NARA) safeguarding of electronic records. At NARA, we recognize that the challenge of securing information technology (IT) systems and devices – particularly in regard to protecting personally identifiable information (PII) – is never- ending and always changing. We know that no agency will ever be perfect, but we are committed to doing the best job that we can and learning from our own mistakes and the mistakes of others. Just last week, my staff attended the CIO Council's annual Privacy Summit, where privacy and information security officials from agencies across the government discussed their experiences, shortfalls, and solutions to the constant challenges that we all face.

I appreciate that Paul Brachfeld, NARA's Inspector General, and David Powner of the Government Accountability Office (GAO) are appearing here along side me. NARA's Office of the Inspector General (OIG) has reported a number of vulnerabilities and made important recommendations on how we can improve our security. In response to their work, we have declared a material weakness with respect to IT security, and we are taking corrective actions, which I will outline in more detail below. Later in my testimony I will update you on the Electronic Records Archives (ERA), which regularly receives useful guidance from the GAO.

As you know Mr. Chairman, this year we suffered the unresolved loss of an external hard drive that contained copies of backup information from the Clinton Administration, for which we have been sending breach notification letters. We have also recently learned that two failed disk drives of IT systems that contain PII were returned to our maintenance contractors even after we had established an enhanced "keep disk" policy to keep and destroy such disks in-house. While we have no reason to believe that these latter two incidents resulted in a breach of PII, they have raised understandable concerns and highlight the need for increased vigilance. I will discuss these incidents and our responses to them in more detail below.

You have also asked that I report on the status of the Electronic Records Archives (ERA), which is still in the process of being developed under a contract with Lockheed Martin. As my staff reported to your staff last week, we are beginning year five and increment three of this seven year and five phase project. We have completed the first two increments, which allowed for base processing and ingest of electronic federal records and for ingest and access to electronic presidential records of the George W. Bush Administration. Since the well-known delay that occurred in 2007, the contract has generally proceeded as expected. Of course, given the highly complex nature of this project, there have been and will continue to be periods of frustration and disagreement with our contractor. To borrow a passage from the book The Art of Project Management: "No matter what you do, how hard you work, or who you work with, things will still go wrong. The best team in the world, with the best leaders, workers, morale and resources will still find themselves in difficult and unexpected situations." It is NARA's responsibility to stay on top of this contract and to hold the contractor accountable, and I believe we are doing that effectively.

NARA's Handling of Defective Hard Drives

In late September, I was briefed by the Inspector General about an allegation that NARA had improperly disclosed sensitive, personally identifiable information (PII) about veterans. The disclosure, it was alleged, occurred when a defective disk drive that contained PII from a veterans information database was sent for repair to a contractor in the fall of 2008.

The defective disk was one of several in a RAID array (Redundant Array of Independent Disks) that supports an Oracle database, the Case Management and Reporting System (CMRS). The CMRS system is used by NARA's Military Personnel Records Center (MPRC, which is a part of the National Personnel Records Center) to track over a million requests annually for veterans' personnel records. MPRC, as the Chairman knows, is in St. Louis, and is NARA's largest

regional facility; it contains over 55.5 million personnel and medical case files and 39 million auxiliary records. The CMRS system servers, however, are housed at our College Park, MD facility. The CMRS was developed in response to a 1997 Business Process Reengineering project to automate end-to-end case processing for military records, and has significantly improved the records services we provide to our nation's veterans by reducing the backlogs experienced in years past.

In accordance with our established internal policy for handling potential information breaches, we conducted a review of the alleged breach of PII. Since there is no evidence that the defective disk drive was ever in unauthorized hands or that any PII about veterans was ever accessed from the disk, my staff and I have concluded that there was no PII breach. A breach of PII occurs when unauthorized individuals have access to sensitive personal information. In this case, we have no reason to believe that any one other than authorized individuals and contractors had access to the defective disk, in accordance with the maintenance contract. The contract included appropriate privacy protection requirements, which also applied to all subcontractors; there is no evidence that the contractors that handled the disk engaged in any improper activity.

The National Archives has long conducted maintenance for unclassified computer hardware using standards consistent with the rest of the Federal government and the private sector. Such standards include utilizing authorized computer maintenance contractors to monitor, fix, and replace this equipment, and placing appropriate management controls on the contractors to protect sensitive data that may have remained on defective magnetic computer storage components that were returned for repair or disposal. The defective CMRS disk drive was handled in accordance with these processes and controls.

In the summer of 2008, in response to guidance from the Office of Management and Budget (OMB) advising Federal agencies on how to protect PII, the National Archives enhanced its PII policy to require that defective or otherwise decommissioned storage media that contained sensitive data, such as PII, be destroyed and disposed of at a NARA facility, rather than being returned to maintenance vendors as had been done previously. It is clear now that this new policy was not communicated to our staff and contractors as effectively as it should have been. However, there is no evidence that the return of this drive resulted in an unauthorized breach of any personal privacy information of veterans. Nor did this action violate the Privacy Act or OMB guidance.

Following the review of this incident, NARA checked with regional facilities across the agency to determine if any other disk drives from systems that contain PII had been sent back to a vendor. On October 9, senior officials at

NARA Headquarters learned that an additional defective hard drive at our National Personnel Records Center (NPRC) in St. Louis, MO, was returned to a vendor in April 2009, again contrary to the policy that NARA had put in place in the Summer of 2008 (we also learned that a defective disk drive from this system was returned in April 2008, before the new policy was in place).

The drive is from a system that is part of the Federal Records Centers' Document Conversion Unit (DCU), which is operated by the NPRC, in collaboration with the Office of Personnel Management (OPM), to digitize Official Personnel Files (OPFs) of current government employees. We believe that in April the system contained digitized OPFs, and an associated index file, of current employee records from NARA, the General Services Administration (GSA), and OPM, and we have informed those agencies about this issue. The system did not contain information on veterans' records.

As with the CMRS disk drive, the defective DCU drive was part of a RAID array, which was returned to the vendor through a maintenance/warranty provision of the existing contract. NARA procured the system in 2006 from Dell Computers under a GSA contract that requires conformance with Federal Information Processing Standards (FIPS), including FIPS-Pub 200, and by reference NIST Special Pub 800-53, which contains media sanitation and disposal controls.

NARA and the OIG are continuing to review the incidents. At this time, however, NARA has no reason to believe that there was a breach of PII or that any unauthorized access to PII occurred.

I would also like to update you on the actions we have taken in response to the external hard drive containing copies of Clinton Administration Executive Office of the President (EOP) data that we discovered missing in March 2009 from NARA's College Park, Maryland facility. The drive is still missing. It contains names, dates of birth, and social security numbers of persons who worked in the Executive Office of the President during the Clinton Administration, visited the White House complex, or just submitted personal information to the White House in pursuit of a job or political appointment.

To date, the National Archives has mailed approximately 26,000 breach notification letters to individuals whose names and social security numbers are on the hard drive. We are offering these individuals one year of free credit monitoring. About 10 percent of those notified have taken advantage of this offer. The Archives continues to maintain a Privacy Breach Response Hotline for these individuals to call with questions.

Our forensic contractor is continuing to search the hard drive for additional names of individuals whose identity might have been compromised. We anticipate mailing an additional 120,000 letters in the coming weeks. As more names are discovered, additional letters will be sent. However, because of the extremely large volume of data on the drive, we do not know yet the total number of individuals whose privacy has been affected.

Corrective Actions

As I said in the beginning of my testimony, NARA is always looking for ways to improve security and internal controls with electronic records.

NARA has conducted an internal audit to identify how well our IT security program was functioning. This audit identified 29 recommendations for improvement in NARA's IT security program. Based on this internal audit and the recommendation of the OIG, NARA chose to declare a material weakness associated with the IT security program. Since then we have doubled our IT Security Staff (in NARA organizational code NHI) and much progress has been made in the area of strengthening our IT security controls. The accomplishments since the completion of the assessment are summarized below:

- Developed an Information Assurance (IA) Program Plan that includes Plan of Action and Milestones (POA&M) for the IT Material Weakness and supporting work breakdown structure (WBS). This Plan is updated annually.
- Added new security staff to handle workload relating to resolution, implementation, and management of the IT Material Weakness audit findings. The NHI organization chart and responsibilities have been documented.
- Defined and published Information System Security Officer (ISSO) and system owner roles and responsibilities. All 49 ISSOs and 49 system owners have reviewed and acknowledged (via signature) their roles and responsibilities.
- Conducted NH Technical Review Group (TRG) Meetings every week with POA&Ms reviewed and updated every fifth week with NH senior Management. NH TRG 81 such meetings were held in FY08 and FY09.
- Conducted NH TRG Meetings as needed to review business cases and system development lifecycle (SDLC) deliverables (e.g., Preliminary Design Reviews for ITY systems). These reviews are conducted from a security / NHI perspective.
- Provided input and review of pending IT operations Request for Change (RFC)/Request for Work (RFW) every five weeks as part of the NH TRG Meetings.
- Conducted monthly Architectural Review Board (ARB) Meetings to review and develop recommendations to Information Technology Executive Committee

(ITEC) for approval/non-approval of proposed business cases. 22 ARB Meetings were held in FY08 and FY09.

- Developed and delivered Certification and Accreditation (C&A) packages for IT Systems.
- Developed and conducted Business Impact Assessments. The information gathered was then used to update system Contingency Plans.
- Continued Intrusion Detection System (IDS) Monitoring, including delivery of weekly summary reports and three daily reports – an increase from a single daily report.
- Conducted external and internal monthly vulnerability assessments.
- Provided security costs and implications template updates for abbreviated and full product plans in NARA 801 (Capital Planning and Investment Control Process). This update has been approved by our policy organization, posted to our intranet site, and is now required for all new product plans. The pending update to NARA 801 also includes IT security considerations and cost identification.
- Conducted annual agency Information Assurance training for every IT user. Users who did not take the training had their accounts suspended until completion of the course.
- NARA recently issued NARA Directive 1608, Protection of Personally Identifiable Information (PII).
- Installed encryption software on all deployed laptop computers.
- Initiated a project to enable secure centralized file backup for our IT systems.

In light of the two hard drive maintenance incidents we are taking a comprehensive look at internal security controls related to the protection of PII within IT systems across all NARA locations. We have undertaken an agency-wide systematic review on the storage and protection of PII that includes: a review data base encryption within the systems, a review of our tape backup procedures, a review of all of our computer acquisition and maintenance contracts to ensure that sensitive data protection is properly addressed, and a review of our internal PII awareness and training processes and procedures to ensure they are sufficient. We also plan to make sure that we are using National Security Agency approved media sanitation and destruction procedures and have engaged expert consultants to review our IT security incident response procedures.

In addition, the OIG has made recommendations to NPRC to improve PII security. The following have been implemented:

- Removed data regarding 4.6 million fulfilled service requests from the CMRS. Only current year fulfilled requests are now maintained; older data will be removed annually. The removed data is stored offline. This data must be kept to

- Implemented quarterly reminders to CMRS users to establish "strong" passwords and regularly update them. The project to upgrade CMRS (to a new Siebel version) now includes a requirement for automated password change protocols. The CMRS upgrade will be implemented by December 31, 2010.
- Perform annual reviews of CMRS user accounts, and remove inactive accounts.
- Assess options to limit users' ability to perform extracts of the CMRS database, except as needed to perform official functions.
- Assess options to enable audit logging to capture database queries that fall outside established boundaries for normal user activity. Implement a solution as part of the CMRS upgrade.
- Issued policy change, staff training, and online procedural guidance to require verification of death before providing military records to next of kin.
- Compiled update key inventories to better protect PII stored on paper.
- Established plan to inspect facilities of contractor responsible for secure disposal and recycling of paper from the Center.

The Electronic Records Archives

The Electronic Records Archives (ERA) is a comprehensive, systematic, and dynamic means for preserving electronic records that will be free from dependence on any specific hardware or software and will improve preservation of, and access to, electronic records into the future. The ERA system and personnel are located at the Allegany Ballistics Lab, a secure site of the U.S. Navy in Rocket Center, WV. ERA was designed, and is being built, to ingest, store, and access "born digital" historic materials, by which we mean permanent electronic records created by Executive Branch agencies, the Congress, the Federal Courts, and the Office of the President. Broadly speaking, ERA will enable NARA to do three main things:

- Bring electronic records in using the archival practices of developing appropriate disposition authority, accessioning, ingesting, extracting metadata, and managing the workflow surrounding all of the above.
- Safely store and insure the integrity of electronic records.
- Provide access to electronic records to record seekers far and wide while providing a means to manage the need for appropriate redactions of sensitive material.

The most fundamental characteristic of ERA is that it must be able to evolve over time to allow new types of electronic records to be brought into ERA

and preserved. ERA will be built to guarantee that the electronic records are not corrupted or distorted by changes in technology. Eventually, the user will be able to view the authentic records, regardless of whether or not the software used to create the records is still available.

The ERA program began in FY 2002, with an appropriation of approximately $16 million, which funded the establishment of the ERA Program Management Office (PMO). In FY 2003, a request for proposals was issued for design and development of the system. In FY 2004, NARA awarded contracts for System Analysis and Design of the system to two vendors. In FY 2005, NARA selected Lockheed Martin Corporation to begin development of Increment 1. System development funds were first provided in FY 2004. System development funds from FY 2004 through FY 2010 are estimated at $258.88 million. FY 2010 funding is estimated at $85.5 million. (When added to annual funds for operations of the Program Management Office, full program appropriations for the period FY 2002 – FY 2010 total $391.1 million.)

ERA, as with any large IT development program, continuously faces risks, adversities and unexpected situations that must be mitigated. The ERA Program Management Office has been vigilant during the course of the program in monitoring contract performance. A synopsis of the most difficult situation follows.

- During FY 2005 and FY 2006, Lockheed Martin, the development contractor, produced detailed versions of the design documents necessary to support software development. Software coding for the first release began in the summer of FY 2006. By December 2006, however, NARA's review of test results indicated an unacceptably high level of problems with the software. At that time, the ERA Program Management Office began reporting the results of its analyses at its monthly status updates to NARA Management, OMB and GAO.

- Throughout the period December through May 2007, the contractor repeatedly assured the Government that the program was on track for mediating the software testing problems and that there would be no negative impact on schedule or cost for final deployment of Increment 1. However, during that time period, NARA's independent review of testing data indicated increasingly unacceptable results, and NARA's projections of schedule delays and cost overruns continued to increase. In early May 2007, the contractor confirmed NARA's estimates and testing evaluations. As a result, the contractor informed NARA that it was unable to meet the Test Readiness Review and Initial Operating Capability (IOC) date as originally defined. The contractor took corrective actions that included key staff changes, additional program and baseline controls and several steps to improve quality assurance and audit processes.

- In response to the contractor's acknowledgement that the IOC deadline would not be met, NARA issued a Cure Notice to the contractor on July 27, 2007 that requested specific steps for the contractor to meet to continue the project and a plan to help mitigate additional costs associated with the schedule slippage.

- On August 16, 2007, the contractor submitted a "Forward Plan" in response to the Government's Cure Notice. The plan proposed to deliver Increment 1 in three incremental software drops leading to Initial Operating Capability in May 2008. After review, the Government recognized that the IOC date would need to be June 30, 2008 to accommodate adequate time for government acceptance testing and security certification and accreditation.

- The new development approach included three checkpoints at which the NARA assessed the contractor's progress towards IOC, and determined whether to continue with the contract until the next software drop. The checkpoints represented "go/no-go" decision points at which the NARA determined whether to proceed or begin actions to terminate the contract.
- The contractor delivered Increment 1 for Initial Operating Capability on June 25, 2008.

NARA staff is now using Increment 1 to ingest electronic records from legacy NARA systems into ERA and to schedule and transfer records from four agencies serving in a pilot capacity. Those agencies are:

- Patent and Trademark Office – Patent Application Case Files
- Bureau of Labor Statistics – Records schedules, economic data and electronic journals
- National Nuclear Safety Administration – Scientific data, geospatial information systems' records
- Naval Oceanographic Office – ship records, computer assisted design files

These four agencies were selected based on the agency's records/number of approved schedules; the presence of experienced Records Officers with adequate training; the involvement of agency Information Technology staff for security, transfer, and network/system capabilities. ERA successfully delivered Instructor-led classroom training to 120 NARA staff and a Records Officer from each of the pilot agencies.

A second pilot is scheduled for early FY 2010. Twenty-five agencies have been identified as suitable candidates, of which eight have already been approved for involvement in the pilot. Those agencies are:

- National Oceanographic and Atmospheric Administration
- U.S. Mint
- Navy Headquarters
- Air Force
- Nuclear Regulatory Commission
- Social Security Administration
- U.S. Geographic Service
- U.S. Coast Guard

Other agencies interested in the pilot are pending concurrence with NARA. It is anticipated that the second pilot will run through December 2010. Based on results and success of the second pilot, NARA will open up the use of ERA to additional agencies, on a voluntary basis, approximately six months after the start of Phase 2. The target date for mandatory use of ERA by all agencies to schedule records will be July 2011.

Increment 2: The Records from the Executive Office of the President of the George W. Bush Administration

Increment 2 of ERA was dedicated to providing support for the transfer of electronic Presidential records from the Executive Office of the President of the George W. Bush Administration so that we could preserve and make these records accessible for archival processing. We are obligated under the Presidential Records Act (PRA) to respond to special access requests from the incumbent and former Presidents, Congress, and the Courts for Presidential records as soon as we take legal custody of them. (The PRA restricts public access of Presidential records for five years after the end of the administration). In addition, NARA needed the ability to establish initial intellectual control over these records to facilitate their processing. Therefore, one of the requirements for ERA was that it should be able to load the huge volume of unclassified Bush Presidential electronic records in the shortest time frame possible. Our goal was to load into ERA the unclassified electronic Presidential records identified as records to us by the White House by the end of September 2009, with the prioritized datasets loaded and searchable first. I should note that the classified Bush Presidential electronic records transferred to us are secured in stand-alone systems until ERA can support a classified instance.

Our work with the records involves two basic processes: the first is to load the records into ERA, so that the records can be managed within our system environment to ensure we can preserve the original bit streams of the records; the second is the work necessary to make the records searchable and accessible by our

archivists. Of the 77 TB of data that were identified and transferred to us as unclassified electronic records, we completed loading approximately 72.3 TB of Presidential records into ERA by early October. The remaining 4.7 TB represents federal records from the Federal components of the Executive Office of the President that will be loaded into Base ERA.

The 72.3 TB of Presidential records amount to approximately 266 million digital objects, of which more than 218 million records (208.8 million Bush Presidential records and 10 million Cheney Vice Presidential) are searchable and accessible by our staff. The 218 million records include the e-mail records identified for us to transfer, the digital photos from the Bush Administration, and a series of other key systems. The remaining 48 million records are mostly comprised of files found in the shared network drives from the White House. These remaining records have been loaded into the system and Lockheed Martin is currently developing an interface that will allow our archivists to browse and search this heterogeneous collection of records.

These figures do not include the Bush White House emails that are still part of an ongoing restoration project being managed by the EOP's Office of Administration, which will be loaded into ERA once the project has concluded. Nor do these figures include:

- Certain audiovisual records such as those generated by the White House Communications Agency that were transferred to NARA on DVDs in proprietary formats.
- Tens of thousands of disaster recovery backup tapes that were transferred to us as part of the transition.
- Electronic media interspersed and transferred as part of the Bush and Cheney textual records, e.g., CDs packed into boxes.

Because ERA is the exclusive means for us to search and provide access to these electronic records, our archivists have made extensive use of the system. To date, more than 28,000 searches for records, including photos, have been executed in the system by NARA archivists (each request can involve numerous searches into the system). Testing takes place in a different system than our live system. Finally, it should be noted that Lockheed Martin successfully delivered the Increment 2 capabilities on schedule and under the budget baseline.

FY 2010 Plans

Funding in NARA's FY 2010 budget is dedicated to Increment 3 of ERA, which includes:

- A Congressional Records Instance to provide simplified storage and access capabilities for electronic records of the Congress (which will also be used for Supreme Court records and donated materials received under deeds of gift).
- A public access system, capable of providing to the public the tools needed to search and access publicly available electronic records that have loaded into ERA.
- Augmentation of the base system architecture to allow for system evolution through newly available commercial technology, which will improve the flexibility and scalability of the base system. The use of commercial off the shelf technology increases the flexibility of the system, because it can support changes without the need for extensive custom code rework. New indexing, search, and storage mechanisms enable the system to grow to meet anticipated load increases with minimal changes to the system architecture. In addition, the augmentation provides the foundation for public access and preservation.
- Implementation of a preservation framework for insertion of preservation technologies as they become available.
- Establishment of a customer acceptance lab.
- Operations and Maintenance.

Planning for Increment 4 is beginning. Specific functions to be developed for Increment 4 include:

- Insertion of emergent technology into the Preservation Framework developed as part of Increment 3 in order to support preservation business capabilities.
- Implement and expand access capabilities.

- Extend base capabilities to provide business functions deferred from prior Increments, as well as the ability to manage restricted records.
- Subsume legacy systems such as the Accession Management Information System (AMIS), Archival Processing System (APS), Archival Electronic Records Inspection and Control system (AERIC), and Access to Archival Databases (AAD).
- Back Up and Restore Capabilities.

- Initiation of the effort to provide an instance of ERA for national security-classified records.

- Operations and Maintenance.

Concerns As We Move Forward

Throughout the development of ERA, NARA has expressed concerns to the contractor about the quality of the software it is developing. Software testing by both the contractor and NARA test teams has found higher then desired software defects. Thus far, thorough testing has mitigated problems. However, NARA continues to demand improvements in software development at the initial stages that would help eliminate software defects and rework. The contractor is taking additional steps to improve in this area, but the ERA PMO will remain concerned until positive results are observed.

The Subcommittee should also know that the start of Increment 3 development has not been as smooth as desired. NARA has raised several concerns with the contractor related to analysis, design, and architectural foundation issues. The contractor was receptive to NARA's input and has taken concrete steps to make improvements in process, deliverables, and staff. At present, the contractor believes it can deliver Increment 3 as scheduled, but you can rest assured that NARA will continue to monitor progress to ensure that this increment will be delivered within cost and schedule. We believe that this is part of the normal give and take between the agency and its contractor that occurs with any large-scale contract, particularly one such as ERA that involves extremely complex and cutting edge technologies.

In summary, ERA is operating in the way that we expected it to at this point in the contract. Federal and Presidential records are stored in an electronic archives located at Rocket Center, West Virginia. Hardware and software failures have been minimal. We have a staged plan to open the system up to Federal agencies. The problems we encounter are common to major IT programs, but I am confident in the ability of the ERA program office that is vigilantly overseeing the work of the contractor.

Mr. Chairman, this concludes my testimony. I would like to thank you again for inviting me here today and for the helpful oversight and guidance you and the members of this Subcommittee provide to NARA. I am happy to answer your questions.

Mr. CLAY. Mr. Brachfeld, you may proceed.

STATEMENT OF PAUL BRACHFELD

Mr. BRACHFELD. Mr. Chairman and members of the subcommittee, I thank you for the opportunity to testify today.

NARA's core mission is to safeguard and preserve the records of our democracy to make them available for this and future generation of Americans. The challenge is daunting and becoming more complex each day in this, the Digital Age. Yet fundamental truisms still exist in many areas. One fundamental truism, as solid as granite, is that sound internal controls should be the foundation upon which all systems and operations are based.

For a decade as a NARA Inspector General, I have had a front-row seat observing internal control weaknesses and internal control deficiencies that have resulted in the loss of Federal funds and property, compromised the successful delivery of contractual services and deliverables, impaired operations, and subjected information to include electronic records maintained in NARA's systems and facilities to compromise.

However, I am hopeful. I believe that under the leadership of a new Archivist, NARA has the opportunity to elevate security to the upper tier of our organizational mission.

The staff in my office is committed to assisting management in this effort. We also look forward to working with the new Archivist with an eye toward strengthening a role NARA plays in ensuring Federal records created by all three branches of government are properly identified, scheduled, accessioned, and ultimately injected into a functional electronic records archive.

Today, at the request of the committee Chair, I will focus upon the exposure resulting from the compromise of records that placed personally identifiable information [PII], of our Nation's veterans, Federal employees, and millions of our Americans at risk. In the past year alone, OIG investigators and auditors have performed work specific to the following: the loss of a computer hard drive from Archives to College Park, populated with millions of records from the Clinton White House. Within this population are tens of thousands of records containing PII as well as other potentially sensitive information.

The loss of government control over a hard drive we suspect contained millions of PII records of our Nation's veterans.

Inappropriate controls over information stored in the automated case management system used in St. Louis to track and process electronic mail-based requests for official military personnel files. System vulnerabilities leave veterans' PII susceptible to unauthorized disclosure.

The improper transmission of veterans' records over an extended period of time by personnel at the National Personnel Records Center which exposed veterans' PII to potential compromise.

The donation and surplus of laptops that were not degaussed or scrubbed which, at least in one case contained files of the former Director of the Information Security and Oversight Office. Among these files was PII-specific and national security officials from the Clinton administration.

The loss or theft of hundreds of pieces of IT equipment, written off for the period of fiscal year 2002 to 2006, had had capacity to store information.

Inappropriate packaging of two backup hard drives containing limited PII at the FDR Presidential Library, resulting in their loss during shipping. OIG investigators subsequently recovered one of the two.

Additionally, this committee was recently notified of another incident in St. Louis, MO in which failed hard drives from a drive array used to store PII information for thousands of Federal employees inappropriately left NARA's physical control. The array contained mirror images of official personnel files and related information of employees from three agencies.

These cases worked by OIG staff within the past year are individually egregious, and collectively represent an agency that is not meeting a core tenet of its mission to safeguard the records of our democracy. While each case of data breach, loss, or under risk of loss, represents a unique stanza; the chorus of the song remains the same.

As an agency, NARA lacks a viable, robust risk identification and mitigation strategy, and we all paid for this shortcoming.

In testimony before this committee on July 30th, I provided details to the internal control weaknesses which result in the loss of a hard drive containing two terabytes of Clinton Presidential records. Internal control weaknesses, lapses, and exercise of questionable judgment tied to other incidents I have spoken of today, regularly leave me and my staff frustrated and bewildered.

Allow me to elaborate. Specifics of the case involving the hard drive potentially holding millions of our Nation's veterans' PII, NARA officials contracting for what to do with these type of hard drives initially had two choices. It needs to be clear that often there is nothing substantially wrong with failed drives and they are perfectly useful for many applications.

Accordingly, one contract choice, the secured data option, would let NARA physically keep all drives identified as failing or failed.

The second choice of the vendor providing a new drive, but then the vendor would take back that drive with the information on it. The vendor would then test the drive to see if anything was wrong with it, and if there was, it could be economically repaired and reused. However, if it cost more to fix than the drive was worth, the drive could be recycled for metals.

NARA opted for choice two. Thus NARA decided to allow the populated and potentially readable drive to leave NARA control. However, as drives actually started to fail, NARA was given a second chance to correct this decision and was presented with a third choice. NARA could keep the failed drive and pay approximately $2,000 for each new drive on a one-by-one basis. Unfortunately, NARA once again chose to let these populated drives leave their control.

The trail specifically described was subsequently found to be untraceable and we cannot get possession back. Accordingly, I cannot tell the committee today whether a breach, as defined by data being accessed by unauthorized parties, occurred. But I can state emphatically that NARA's actions to create the risk of such a

breach and a lack of due diligence to protect this information cannot be ignored and should not be marginalized.

While I have been informed that this situation I just described has now been fixed contractually, I believe select narrow managers, from the top down, do not recognize the risk factors existing in today's environment. Failing to define the risk, would you not deploy and make the security first decisions necessary to adjust to real and potential risk before unfortunate and irreversible events transpire?

In the brief time allotted to me, I would also note—specifically; it relates to the ERA program—that I have had professional skepticism about ERA since the first meeting I attended in 2002. Fearing a worst-case scenario, I went to then-Archivist Carlin on April 30, 2002, seeking audit staff resources to provide independent, objective, and skilled oversight over ERA. Per my notes he responded, "I could give you 50 people and you still couldn't cover it. So you think you can do it with two?"

In December 2003, failing to obtain any ERA dedicated audit resources, I made a formal request, to the OMB Director stating ERA is a challenge we are not equipped to address within our existing fiscal constraints. We are simply unable to provide the necessary coverage to this mission-critical program. Failure to fund this initiative will not allow me to obtain persons with the skills necessary to independently evaluate and report upon the progress of ERA. Likewise we'll not be able to support this program of real time, potentially resulting in less than optimal results. This is a risk that this Nation should not face.

As I testify today, I continue to have profound concerns over the status of the ERA program. My concerns are rarely reflected by management, who throughout program life have expressed abundant optimism. For example, in April 2007, ACERA meeting minutes, the ERA director stated—technical director stated—that the program is succeeding. Yet OIG auditors were finding this rosy scenario to be anything but the truth.

In a management letter to the Archivist on January 13, 2007, we accurately defined the ERA programs as one "beset by delivery delays, cost overruns and staffing shake-ups." History shows we were correct.

At the very next ACERA meeting in November 2007, the minutes report that same ERA technical director made a 100-degree course correction by defining that sound engineering methods were not followed in many areas. Lockheed allowed the schedule to become the priority, rather than ensuring that requirements were being met in a satisfactory manner ultimately has failed. NARA issued a curing notice to lock in 2007.

Shortly thereafter, in testimony before a subcommittee of the Senate Committee on Homeland Security and Government Affairs, on May 14, 2008, Archivist Weinstein stated We discovered belatedly that we may not have the A team from Lockheed Martin, and Lockheed Martin acknowledged this fact. And so we got the A team, and the A team has been performing effectively.

I am not sure as to the basis for this testimony, which was perhaps designed to allay the concerns espoused by Senators at this hearing. Seventeen months have passed, we are now in fiscal year

2010, and key staff in NARA and LMC have come and gone. New voices replace old voices and optimism ebbs and flows.

At a time when NARA officials publicly voice confidence that full operating capability will be met by March 2012, a senior working within the ERA program office spoke to me just last week of ongoing contract performance and deliverable deficiencies. Perhaps the A team is sliding down the alphabetic scale.

The Acting Archivist told me last week the Chief Information Officer has been made aware of ongoing deficiencies. However senior NARA management never brought such information to my attention nor disclosed it to the auditors assigned to this program area.

As engaged as I have been, I do not know what capabilities and capacities will reside in ERA when the contractors throw another party, turn in their badges, shake hands and exit the door.

Such a statement should be viewed as troubling to all NARA stakeholders, and particularly this committee. It is my hope that through this testimony and the support of a new Archivist, we will begin to see improvements in our system of internal controls, and that those who fail to discharge their duties will face appropriate sanctions.

I thank you for this opportunity and I look forward to responding to your questions, thank you.

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

[The prepared statement of Mr. Brachfeld follows:]

Statement

Of

Mr. Paul Brachfeld

Inspector General

National Archives and Records Administration

Information Policy, Census, and National Archives Subcommittee

Oversight and Government Reform Committee

Thursday, November 5, 2009

2154 Rayburn HOB

2:00 p.m.

"The National Archives' Ability to Safeguard the Nation's Electronic Records"

Mr. Chairman and Members of the Subcommittee, I thank you for offering me the opportunity to testify today.

NARA's core mission is to safeguard and preserve the records of our democracy to make them available for this and future generations of Americans. The challenge is daunting and becoming more complex each day in this the digital age. Yet, fundamental truisms still exist in many areas. One fundamental truism as solid as granite, is that sound internal controls should be the foundation upon which all systems and operations are based.

For a decade as the NARA Inspector General I have had a front-row seat observing internal control weaknesses and internal control deficiencies that have: resulted in loss of federal funds and property; compromised the successful delivery of contractual services and deliverables; impaired operations and subjected information - to include electronic records maintained in NARA systems and facilities - to compromise. However, I am hopeful; I believe under the leadership of a new Archivist, NARA has the opportunity to elevate security to the upper tier of our organizational mission. The staff of my office is committed to assisting management in this effort. We also look forward to working with the new Archivist with an eye toward strengthening the role NARA plays in ensuring federal records created by all three branches of government are properly identified, scheduled, accessioned and ultimately ingested into a functional Electronic Records Archive.

Today at the request of the Committee Chair I will focus upon the exposure resulting from the compromise of records that place the Personally Identifiable Information, commonly known as

PII, of our nation's veterans, federal employees and millions of other Americans at risk. In the past year alone OIG investigators and auditors have performed work specific to the following:

► The loss of a computer hard drive from Archives II in College Park populated with millions of records from the Clinton White House. Within this population are tens of thousands of records containing PII as well as other potentially sensitive information.

► The loss of government control over a hard drive we suspect contained millions of PII records of our nation's veterans.

► Inappropriate controls over information stored in the automated case management system used in St. Louis to track and process electronic mail-based requests for Official Military Personnel Files. System vulnerabilities leave veterans' PII susceptible to unauthorized disclosure.

► The improper transmission of veterans' records over an extended period of time by personnel at the National Personnel Records Center which exposed veteran's PII to potential compromise.

► The donation and surplus of laptops that were not degaussed or scrubbed which, in at least in one case, contained files of the former Director of the Information Security and Oversight Office. Amongst these files was PII specific to senior national security officials from the Clinton administration.

► The loss or theft of hundreds of pieces of IT equipment written-off for the period of FY 2002-2006 that had capacity to store information.

► Inappropriate packaging of two back-up hard drives containing limited PII at the FDR Presidential Library resulted in their loss during shipping. OIG investigators subsequently recovered one of the two.

Additionally, this Committee was recently notified of another incident in St. Louis, Missouri, in which failed hard drives from a drive array used to store PII information for thousands of Federal employees inappropriately left NARA's physical control. The array contained mirrored images of Official Personnel Files and related information for employees of three federal agencies.

These cases worked by OIG staff within the past year are individually egregious and collectively represent an agency that is not meeting a key tenet of its mission – to safeguard the records of our democracy. While each case of data breach, loss or undue risk of loss represents a unique stanza, the chorus of the song remains the same. As an agency NARA lacks a viable, robust risk identification and mitigation strategy, and we all pay for that shortcoming.

In testimony before this Committee on July 30th I provided details as to internal security control weaknesses which resulted in the loss of the hard drive containing two terabytes of Clinton presidential records. Internal control weaknesses, lapses and exercises of questionable judgment tied to other incidents I have spoken of today regularly leave me and my staff frustrated and bewildered. Allow me to elaborate, specific to the case involving the hard drive potentially

holding millions our nation's veteran's PII. NARA officials contracting for what to do with these types of hard drives initially had two choices. It needs to be clear that often there is nothing substantially wrong with "failed" drives and they are perfectly useable for many applications. Accordingly, one contract choice, the secure data option, would let NARA physically keep all drives identified as failed or failing. The second choice had the vendor provide a new drive, but then the vendor would take back the drive with information on it. The vendor would then test the drive to see if anything was really wrong with it, and if it was if it could be economically repaired and reused. However, if it cost more to fix the drive than it was worth, the drive could be recycled for metals. NARA opted for choice two. Thus NARA decided to allow the populated and potentially readable drive to leave NARA's control. However, as drives actually started to "fail" NARA was given a second chance to correct this decision and was presented with a third choice. NARA could keep the "failed" drive and pay approximately $2000 for each new drive on a one-by-one basis. Unfortunately, NARA once again chose to let these populated drives leave their control. The trail specific to this drive was subsequently found to be untraceable, and we cannot get possession back. Accordingly, I cannot tell the Committee today whether a breach, as defined by data being accessed by unauthorized parties, actually occurred. But I can state emphatically that NARA's actions to create the risk of such a breach and the lack of due diligence to protect this information cannot be ignored and should not be marginalized.

While I have been informed that the situation I just described has now been fixed contractually, I believe select NARA managers from the top down do not recognize the risk factors existing in today's environment. Failing to define the risk we do not deploy and make the security-first

decisions necessary to address real and potential risks before unfortunate, and irreversible events transpire.

In the brief time allotted to me I would also note specifically as it relates to the Electronic Records Archive Program that I have had professional skepticism about the ERA since the very first meeting I attended in 2002. Fearing a worst-case scenario I went to then Archivist Carlin on April 30, 2002 seeking audit staff resources to provide independent, objective and skilled oversight over ERA. Per my notes he responded, and I quote, "I could give you 50 people and you still couldn't cover it so you think you can do it with two?" In December 2003 failing to obtain any ERA dedicated audit resources I made a formal request to the OMB Director stating:

> ERA is a challenge we are not equipped to address within our existing fiscal constraints. We are simply unable to provide the necessary coverage to this mission critical program. Failure to fund this initiative will not allow me to obtain persons with the skills necessary to independently evaluate and report upon the progress of the ERA. Likewise, we will not be able to support this program in real time potentially resulting in less then optimum results. This is a risk that this nation should not have to face.

As I testify today I continue to have profound concerns over the status of the ERA program. My concerns are rarely reflected by management who throughout program life have expressed abundant optimism. For example, in the April 2007 ACERA Meeting minutes the ERA Technical Director "stated that the program is succeeding." Yet OIG auditors were finding this

rosy scenario to be anything but the truth. In a Management Letter to the Archivist on July 13, 2007 we accurately defined the ERA program as one "beset by delivery delays, cost overruns and staffing shake-ups." History shows we were correct. At the very next ACERA meeting in November 2007, the minutes report the ERA Technical Director made a 180 degree course correction by defining that:

> [S]ound engineering methods were not followed in many areas ... Lockheed allowed the schedule to become the priority rather than ensuring that the requirements were being met in a satisfactory manner. Ultimately this failed. NARA issued a "cure notice" to Lockheed in August 2007.

Shortly thereafter in testimony before a subcommittee of the Senate Committee on Homeland Security and Government Affairs on May 14, 2008, Archivist Weinstein stated:

> We discovered belatedly that we may not have had the A Team from Lockheed Martin and Lockheed Martin acknowledged that fact. And so we got the A Team and the A Team has been performing effectively.

I am not sure as to the basis for this testimony which was perhaps designed to allay the concerns espoused by Senators at that hearing. Seventeen months have since passed, we are now in FY 2010, and key staff in NARA and LMC have come and gone. New voices replace old voices and optimism ebbs and flows. At a time when NARA officials publicly voice confidence that full operational capability will be met by March 2012, a senior worker within the ERA program

office spoke to me just last week of ongoing contractor performance and deliverable deficiencies. Perhaps the "A" Team is sliding down the alphabetic scale. The Acting Archivist told me last week the Chief Information Officer has been made aware of ongoing deficiencies, however senior NARA management never brought such information to my attention, nor disclosed it to the auditors assigned to this program area. As engaged as I have been, I do not know what capabilities and capacity will reside in ERA when the contractor throws another party, turns in their badges, shakes hands, and exits the door. Such a statement should be viewed as troubling to all NARA stakeholders and particularly this Committee.

It is my hope that through this testimony and with the support of a new Archivist we will begin to see improvements in our systems of internal controls and that those who fail to discharge their duties will face appropriate sanctions.

I thank you for this opportunity and look forward to responding to your questions.

Mr. CLAY. Mr. Powner, you're up.

STATEMENT OF DAVID POWNER

Mr. POWNER. Chairman Clay, Ranking Member McHenry, and members of the subcommittee, we appreciate the opportunity to testify this afternoon on NARA's electronic records archive system. This $550 million system is intended to preserve and provide access to massive amounts of electronic records and is an investment critical to NARA's mission.

To date, NARA has spent more than half of the $550 million and has deployed two of the five planned increments. This afternoon, Chairman Clay, I will comment on NARA's performance with the first two increments, existing project management concerns, plans for increments 3 through 5 and recommendations for improvement.

Starting with performance of the first two increments, increment 1 was late, over budget, and did not provide the functionality promised. Specifically, initial operating capability with four pilot agencies was scheduled for September 2007, but was delayed 9 months to June 2008. This delay resulted in the cost overrun of $20 million. But even more troubling is the fact that planned functionality was not delivered and deferred to later increments.

These delays also squashed NARA's plans to use ERA to receive the electronic Presidential records of the outgoing Bush administration in January 2009. Instead, a separate commercial system with a different architecture from ERA was used to archive the Bush records. And although NARA certified the second increment in December 2008, the 73 terabytes of Presidential records were not ingested into the system until September 2009. The first two increments are basically different systems, and integrating these systems in later increments will need to be addressed.

Managing a project this large requires sound project management discipline that includes overseeing contractor performance to ensure that what the government is paying for is delivered at the agreed-to cost and on time. To date, the ERA program does not have a good track record here. When we looked into this last year, we found several weaknesses in NARA's practice. For example, we found contractor reports on program funds spent without work completed, and work completed and funds spent on work that was not in the work plans. NARA is working to improve the management processes so that the cost schedule and technical performance can be closely monitored in the remaining three increments over the next 3 years.

Regarding the remaining three increments, we have reported and made recommendations to NARA that their outyear increments need to be clearly defined as to what specific functions will be delivered when and at what cost. For example, NARA has significant work ahead in the outyear increments that include expanding beyond the four pilot agencies, handling classified information, providing public access capability, and expanding functionality like access and preservation capabilities. Such detailed plans are essential if this project is to achieve full operating capability by 2012 at the $550 million price tag.

Moving forward, NARA needs to closely monitor not only the cost of each increment, but also needs to monitor the functionality deliv-

ered. Our recommendation to bolster the program's use of earned value management should help, if effectively implemented.

The program also needs to ensure integration plans are in place to merge the differing architectures used in the ERA base system and the Presidential record system. And also NARA needs to define in great detail the functions to be delivered in increments 3 through 5. This includes aligning detailed requirements and the cost with each increment. Failing to address these recommendations will clearly jeopardize the chances of achieving full operating capability by 2012.

Mr. Chairman, this concludes my statement. Thank you for your oversight of this project, and I look forward to your questions.

Mr. CLAY. Thank you so much Mr. Powner.

[The prepared statement of Mr. Powner 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

For Release on Delivery
Expected at 2 p.m. EST
November 5, 2009

NATIONAL ARCHIVES

Progress and Risks in Implementing its Electronic Records Archive Initiative

Statement of David A. Powner, Director
Information Technology Management Issues

GAO-10-222T

November 5, 2009

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-10-222T, a testimony before the Subcommittee on Information Policy, Census, and National Archives, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Since 2001, the National Archives and Records Administration (NARA) has been working to develop a modern Electronic Records Archive (ERA) system, a major information system that is intended to preserve and provide access to massive volumes of all types and formats of electronic records. The system is being developed incrementally over several years, with the first two pieces providing an initial set of functions and additional capabilities to be added in future increments. NARA plans to deploy full system functionality by 2012 at an estimated life-cycle cost of about $550 million.

NARA originally planned to complete the first segment of ERA in September 2007. However, software and contracting problems led the agency and its contractor Lockheed Martin to revise the development approach. The revised plan called for parallel development of two different increments: a "base" ERA system with limited functionality and an Executive Office of the President (EOP) system to support the ingestion and search of records from the outgoing Bush Administration.

GAO was asked to summarize NARA's progress in developing the ERA system and the ongoing risks the agency faces in completing it. In preparing this testimony, GAO relied on its prior work and conducted a preliminary review of NARA's fiscal year 2010 ERA expenditure plan.

View GAO-10-222T or key components. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

NATIONAL ARCHIVES

Progress and Risks in Implementing its Electronic Records Archive Initiative

What GAO Found

NARA has completed two of five planned increments of ERA, but has experienced schedule delays and cost overruns, and several functions planned for the system's initial release were deferred. Although NARA initially planned for the system to be capable of ingesting federal and presidential records in September 2007, the two system increments to support those records did not achieve initial operating capability until June 2008 and December 2008, respectively. In addition, NARA reportedly spent about $80 million on the base increment, compared to its planned cost of about $60 million. Finally, a number of functions originally planned for the base increment were deferred to later increments, including the ability to delete records and to ingest redacted records. In fiscal year 2010, NARA plans to complete the third increment, which is to include new systems for Congressional records and public access, and begin work on the fourth.

GAO's previous work on ERA identified significant risks to the program and recommended actions to mitigate them. Specifically, GAO reported that NARA's plans for ERA lacked sufficient detail to, for example, clearly show what functions had been delivered to date or were to be included in future increments and at what cost. Second, NARA had been inconsistent in its use of earned value management (EVM), a project management approach that can provide objective reports of project status and early warning signs of cost and schedule overruns. Specifically, GAO found that NARA fully employed only 5 of 13 best practices for cost estimation that address EVM. Further, NARA lacked a contingency plan for ERA to ensure system continuity in the event that normal operations were disrupted. For example, NARA did not have a fully functional backup and restore process for the ERA system, a key component of contingency planning for system availability.

To help mitigate these risks, GAO recommended that NARA:

- include details in future ERA expenditure plans on the functions and costs of completed and planned increments;
- strengthen its earned value management process following best practices; and
- develop and implement a system contingency plan for ERA.

NARA reported in its most recent expenditure plan that it had taken actions to address these recommendations.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing on the National Archives' (NARA) Electronic Records Archive system (ERA). Since 2001, NARA has been working to develop this system which is intended to preserve and provide access to massive volumes of all types and formats of electronic records by automating NARA's records management and archiving life cycle. The system is to consist of

- infrastructure elements, such as hardware and operating systems;
- business applications that will support the transfer, preservation, dissemination, and management of all types of records and the preservation of and online access to electronic records; and
- a means for public access via the Internet.

In view of its complexity, the system is being developed incrementally over several years; the first two pieces (or increments) of the ERA system provided an initial set of functions for managing federal and presidential records. NARA plans to add additional capabilities in future increments.

As agreed, my testimony today will summarize NARA's progress in developing the ERA system and the ongoing risks NARA faces in successfully completing it. My comments today are based on our prior work in this area,[1] as well as a preliminary review of NARA's fiscal year 2010 ERA expenditure plan. Our work was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis

[1]See GAO, *Electronic Records Archives: The National Archives and Records Administration's Fiscal Year 2009 Expenditure Plan*,GAO-09-733 (Washington, D.C.: July 24, 2009); *Information Management: Challenges in Implementing an Electronic Records Archive*, GAO-08-738T (Washington, D.C.: May 14, 2008); *Information Management: The National Archives and Records Administration's Fiscal Year 2007 Expenditure Plan*, GAO-07-987 (Washington, D.C.: July 27, 2007); and *Electronic Records Archives: The National Archives and Records Administration's Fiscal Year 2006 Expenditure Plan*, GAO-06-906 (Washington, D.C.: Aug. 18, 2006).

for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The ability to find, organize, use, share, appropriately dispose of, and save records—the essence of records management—is vital for the effective functioning of the federal government. In the wake of the transition from paper-based to electronic processes, records are increasingly electronic, and the volumes of electronic records produced by federal agencies are vast and rapidly growing, providing challenges to NARA as the nation's recordkeeper and archivist.

Besides sheer volume, other factors contributing to the challenge of electronic records include their complexity and their dependence on software and hardware. Electronic records come in many forms: text documents, e-mails, Web pages, digital images, videotapes, maps, spreadsheets, presentations, audio files, charts, drawings, databases, satellite imagery, geographic information systems, and more. They may be complex digital objects that contain embedded images (still and moving), drawings, 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).

In addition, the computer operating systems and the hardware and software that are used to create electronic documents can become obsolete. If they do, they may leave behind records that cannot be read without the original hardware and software. Further, the storage media for these records are affected by both obsolescence and decay. Media may be fragile, have limited shelf life, and become obsolete in a few years. For example, few computers today have disk drives that can read information stored on 8- or 5¼-inch diskettes, even if the diskettes themselves remain readable.

Another challenge is the growth in electronic presidential records. The Presidential Records Act[2] gives the Archivist of the United States responsibility for the custody, control, and preservation of presidential records upon the conclusion of a President's term of office. The act states that the Archivist has an affirmative duty to make such records available to the public as rapidly and completely as possible consistent with the provisions of the act.

In response to these widely recognized challenges, the Archives began a research and development program to develop a modern archive for electronic records. In 2001, NARA hired a contractor to develop policies and plans to guide the overall acquisition of an electronic records system. In December 2003, the agency released a request for proposals for the design of ERA. In August 2004, NARA awarded two firm-fixed-price[3] contracts for the design phase totaling about $20 million—one to Harris Corporation and the other to Lockheed Martin Corporation. On September 8, 2005, NARA announced the selection of Lockheed Martin Corporation to build the ERA system. The contract with Lockheed is a cost-plus-award-fee contract[4] with a total value through 2012 of about $317 million. As of April 2009, the life-cycle cost for ERA through March 2012 was estimated at $551.4 million; the total life-cycle cost includes not only the development contract costs, but also program management, research and development, and program office support, among other things. Through fiscal year 2008, NARA had spent about $237 million on ERA, including about $112 million in payments to Lockheed Martin.

The purpose of ERA is to ensure that the records of the federal government are preserved for as long as needed, independent of the

[2]44 U.S.C. 2203(f)(1).

[3]According to the Federal Acquisition Regulation, a firm-fixed-price contract provides for a price that is not subject to any adjustment on the basis of the contractor's cost experience in performing the contract. This type of contract places on the contractor maximum risk and full responsibility for costs and resulting profit or loss.

[4]A cost-plus-award-fee contract is a cost reimbursement contract that provides for a fee consisting of a base amount fixed at the inception of the contract plus an award amount that may be given based upon a judgmental evaluation by the government of contract performance.

original hardware or software that created them. ERA is to provide the technology to ensure that NARA's electronic records holdings can be widely accessed with the technology currently in use.

The system is to enable the general public, federal agencies, and NARA staff to search and access information about all types of federal records, whether in NARA custody or not, as well as to search for and access electronic records stored in the system. Using various search engines, the system is to provide the ability to create and execute searches, view search results, and select assets for output or presentation.

NARA currently plans to deliver ERA in five separate increments:

- Increment 1, also known as the ERA base, included functions focused on the transfer of electronic records into the system.
- Increment 2 includes the Executive Office of the President (EOP) system, which was designed to handle electronic records from the White House at the end of the previous administration. The EOP system uses an architecture based on a commercial off-the-shelf product that supplies basic requirements, including rapid ingest of records and immediate and flexible search of content. Increment 2 also includes basic case management for special access requests.[5]
- According to NARA's 2010 ERA expenditure plan, Increment 3 is to include new Congressional and Public Access systems. It is also to augment the base system with commercial off-the-shelf technology to increase flexibility and scalability. NARA plans to complete this increment by June 2010.
- Increments 4 and 5 are to provide additional ERA functionality, such as backup and restore functions and wider search capabilities, and provide full system functionality by 2012.

[5]These are requests NARA receives from the current and former administrations, Congress, and the courts for access to presidential records.

NARA Has Completed Two of Five ERA Increments, but Also Experienced Schedule Delays and Cost Overruns While Deferring Functionality

NARA's progress in developing ERA includes achieving initial operating capability for the first two of its five planned increments. However this progress came after NARA had experienced significant project delays and increased costs. NARA also deferred functions planned for Increment 1 to later increments.

As we reported in 2007,[6] the initial operating capability for Increment 1 was originally scheduled to be achieved by September 2007. However, the project experienced delays due to factors such as low productivity of contractor software programmers, difficulties in securing an acceptable contract to prepare the site that was to house the system, and problems with software integration. These delays put NARA's initial plan to use ERA to receive the electronic presidential records of the Bush Administration in January 2009 at risk.

In response, NARA and Lockheed Martin agreed to a revised schedule and strategy that called for the concurrent development of two separate systems, which could later be reintegrated into a single system:

- First, they agreed to continue development of the original system but focused the first increment on the transfer of electronic records into the system. Other initially planned capabilities were deferred to later increments, including deleting records from storage, searching item descriptions, and ingesting records redacted outside of the system. NARA now refers to this as the "base" ERA system. Initial operating capability for this increment was delayed to June 2008.
- Second, NARA conducted parallel development of a separate increment-dedicated initially to receiving electronic records from the outgoing Bush Administration in January 2009. This system,

[6]GAO 07-987.

referred to as the Executive Office of the President (EOP) system, uses a different architecture from that of the ERA base: it was built on a commercial product that was to provide the basic requirements for processing presidential electronic records, such as rapid ingestion of records and the ability to search content. NARA believed that if it could not ingest the Bush records in a way that supported search and retrieval immediately after the transition, it risked not being able to effectively respond to requests from Congress, the new administration, and the courts for these records—a critical agency mission.

As we reported earlier this year,[7] NARA certified that it achieved initial operating capability for Increment 1 in June 2008, following its revised plan. According to NARA's 2010 expenditure plan, this increment cost $80.45 million to deliver, compared to a planned cost of $60.62 million.

NARA also reported that it completed Increment 2 on time in December 2008 at a cost of $10.4 million (compared to a planned cost of $11.1 million). However, it was not functioning as intended because of delays in ingesting records into the system. Specifically, before the transition, NARA had estimated that the Bush electronic records would be fully ingested into EOP, where they would be available for search and retrieval, by May 2009. However, as of April 27, only 2.3 terabytes of data were fully ingested into the EOP system. This constituted about 3 percent of all Bush Administration unclassified electronic records.[8] NARA later estimated that ingest of all 78.4 terabytes of unclassified records would not be complete until October 2009. In its recently released 2010 expenditure plan, NARA reported that the Bush records were fully ingested into EOP by September 2009.

[7]GAO-09-733.

[8]NARA's original EOP plans included a National Security System. NARA subsequently deferred the capability to ingest classified national security data, stating that the volume to be transferred from the Bush Administration did not support the establishment of a full scale classified EOP system as planned. Instead, NARA migrated the classified data from the Bush Administration to an existing classified NARA presidential library system.

NARA officials attributed EOP ingest delays, in part, to unexpected difficulties. For example, according to NARA officials, once they started using the EOP system, they discovered that records from certain White House systems were not being extracted in the expected format. As a result, the agency had to develop additional software tools to facilitate the full extraction of data from White House systems prior to ingest into EOP. In addition, in April 2009, NARA discovered that 31 terabytes of priority data that had been partially ingested between December 2008 and January 2009 were neither complete nor accurate because they were taken from an incomplete copy of the source system.

Because the records had not been ingested into the EOP system, NARA had to use other systems to respond to requests for presidential records early in 2009. As of April 24, 2009, NARA had received 43 special access requests for information on the Bush Administration. Only one of these requests used EOP for search, and no responsive records were found. To respond to 24 of these requests, NARA used replicated systems based on the software and related hardware used by the White House for records and image management. NARA's current expenditure plan reports that after completing ingest of the Bush electronic records in September 2009, it retired the replicated systems.

In fiscal 2010, NARA plans to complete Increment 3 and begin work on Increment 4. According to its 2010 expenditure plan, Increment 3 will cost $42.2 million and be completed in the fourth quarter of fiscal year 2010. It is to provide new systems for congressional records and public access, as well as improvements to the existing base system and the incorporation of several deferred functions, such as the ability to delete records and search and view their descriptions. Fiscal year 2010 work on Increment 4 is to consist primarily of early planning, analysis, and design.

NARA Faces Several Significant Risks to the Successful Completion of ERA

Despite the recent completion of the first two ERA increments, NARA faces several risks that could limit its ability to successfully

complete the remaining three increments by 2012. These risks include the lack of specific plans describing the functions to be delivered in future increments, inconsistent application of earned value management (a key management technique), and the lack of a tested contingency plan for the ERA system.

First, NARA's plans for ERA have lacked sufficient detail. For several years, NARA's appropriations statute has required it to submit an expenditure plan to congressional appropriations committees before obligating multi-year funds for the ERA program, and to, among other conditions, have the plan reviewed by GAO. These plans are to include a sufficient level and scope of information for Congress to understand what system capabilities and benefits are to be delivered, by when and at what costs, and what progress is being made against the commitments that were made in prior expenditure plans. However, several of our reviews have found that NARA's plans lacked sufficient detail.[9] Most recently, we reported in July that NARA's 2009 plan did not clearly show what functions had been delivered to date or what functions were to be included in future increments and at what cost.

For example, the fiscal year 2009 plan did not specifically identify the functions provided in the two completed increments. In addition, while the plan discussed the functions deferred to later increments, it did not specify the cost of adding those functions at a later time. Additionally, NARA's 2009 plan lacked specifics about the scope of improvements planned for Increment 3. For example, it described one of the improvements as extend storage capacity but did not specify the amount of extended storage to be provided. Also, NARA's plan did not specify when these functions will be completed or how much they would cost. NARA officials attributed the plan's lack of specificity to ongoing negotiations with Lockheed Martin.

[9]See GAO-06-906 and GAO-09-733.

Another risk is NARA's inconsistent use of earned value management (EVM).[10] NARA's 2009 expenditure plan stated that, in managing ERA, the agency used EVM tools and required the same of its contractors. EVM, if implemented appropriately, can provide objective reports of project status, produce early warning signs of impending schedule delays and cost overruns, and provide unbiased estimates of a program's total costs. We recently published a set of best practices on cost estimation that addresses the use of EVM.[11] Comparing NARA's EVM data to those practices, we determined that NARA fully addressed only 5 of the 13 practices. For example, we found weaknesses within the EVM performance reports, including contractor reports of funds spent without work scheduled or completed, and work completed and funds spent where no work was planned. In addition, the program had not recently performed an integrated cost-schedule risk analysis. This type of analysis provides an estimate of the how much the program will cost upon completion and can be compared to the estimate derived from EVM data to determine if it is likely to be sound. NARA officials attributed these weaknesses, in part, to documentation that did not accurately reflect the program's current status.

Another significant risk is the lack of a contingency plan for ERA. Contingency planning is a critical component of information protection. If normal operations are interrupted, network managers must be able to detect, mitigate, and recover from service disruptions while preserving access to vital information. Therefore, a contingency plan details emergency response, backup operations, and disaster recovery for information systems. Federal guidance recommends 10 security control activities related to contingency planning, including developing a formal contingency plan, training

[10]EVM is a project management tool that integrates the technical scope of work with schedule and cost elements for investment planning and control. It compares the value of work accomplished in a given period with the value of the work expected in that period. Differences in expectations are measured in both cost and schedule variances. The Office of Management and Budget requires agencies to use EVM in their performance-based management systems for the parts of an investment in which development effort is required or system improvements are under way.

[11]GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March, 2009).

employees on their contingency roles and responsibilities, and identifying a geographically separate alternative processing site to support critical business functions in the event of a system failure or disruption.[12]

An internal NARA review found weaknesses in all 10 of the required contingency planning control activities for ERA. As of April 2009, NARA had plans to address each weakness, but had not yet addressed 10 of the 11 weaknesses. In addition, NARA reported that the backup and restore functions for the commercial off-the-shelf archiving product used at the ERA facility in West Virginia tested successfully, but there were concerns about the amount of time required to execute the process. In lab tests, the restore process took about 56 hours for 11 million files.[13] This is significant because, while the backup is being performed, the replication of data must be stopped; otherwise it could bring the system to a halt. Subsequently, NARA officials stated that they have conducted two successful backups, but the restore process had not been fully tested to ensure that the combined backup and restore capability can be successfully implemented.

Implementation of GAO's Recommendations Could Reduce Risks

To help mitigate the risks facing the ERA program, we previously recommended that NARA, among other things:

- include more details in future ERA expenditure plans on the functions and costs of completed and planned increments;
- strengthen its earned value management process following best practices; and
- develop and implement a system contingency plan for ERA.

[12]National Institute of Standards and Technology, Recommended Security Controls for Federal Information Systems, Special Publication 800-53 Revision 1 (Gaithersburg, MD: December 2006).

[13]NARA estimates that it has received more than 300 million files from the Bush Administration.

In its 2010 expenditure plan, NARA reported that it had taken action to address our recommendations. For example, NARA reported that a test of the ERA contingency plan was completed on August 5, 2009, and the plan itself finalized on September 16, 2009. We have not yet fully-reviewed this plan or the results of the reported test. However, if NARA fully implements our recommendations, we believe the risks can be significantly reduced.

In summary, despite earlier delays, NARA has made progress in developing the ERA system, including the transfer of Bush administration electronic records. However, future progress could be at risk without more specific plans describing the functions to be delivered and the cost of developing those functions, which is critical for the effective monitoring of the cost, schedule, and performance of the ERA system. Similarly, inconsistent use of key project management disciplines like earned value management would limit NARA's ability to effectively manage this project and accurately report on its progress.

Mr. Chairman, this concludes my testimony today. I would be happy to answer any questions you or other members of the subcommittee may have.

Contact and Staff Acknowledgments

If you or your staff have any questions about matters discussed in this testimony, please contact David A. Powner at (202) 512-9286 or pownerd@gao.gov. The other key contributor to this testimony was James R. Sweetman, Jr., Assistant Director.

Mr. CLAY. Mr. Brill you have 5 minutes.

STATEMENT OF ALAN E. BRILL

Mr. BRILL. Thank you, sir. Chairman Clay, Ranking Member McHenry, members of the committee and members of the staff, good afternoon. My name is Alan Brill. I'm currently senior managing director for secure information services at Kroll Ontrack. I am not here today as a representative of Kroll Ontrack, but as an individual to share whatever knowledge and experience I have in the fields of information security, data protection and data recovery, to assist the subcommittee with the vital work it performs. And I'm grateful to you for the opportunity to speak today.

A substantial proportion of the information that is being created within our government is generated, exchanged, and stored digitally. It is produced and stored on computers ranking from the desktop or laptop computers of individuals, to the massive processing arrays in networks of large agencies. It is also a simple fact that most of the data that is created, and which may have historical import for extended periods of time, will never in the course of normal use be printed.

How do we safely and efficiently preserve electronic records when the technologies involved in producing and storing those records is clearly evolving at a breakneck speed?

I've been involved in the security and recovery of data from computers for more than 40 years. My recent experience has involved working with private-sector organizations to safeguard sensitive data and help those organizations respond to data security incidents. I've learned a few lessons that I hope will be helpful to the subcommittee when it considers how best to carry out its oversight role in assuring the preservation of electronic records which are a vital part of our national heritage.

First, don't assume that the devices currently used to store data will be commonly used, or even reasonably available in the future. Above all else, we must ensure not only that we can store the data but that we can completely and accurately access it on the physical media that we preserve. This means that we either have to also preserve workable reading mechanisms or periodically transfer the data to contemporary storage media, as new storage technology obsoletes the old.

Don't assume data can't be restored, even if the storage medium appears to be damaged. Consider a quick example. Following the tragic loss of the Space Shuttle Columbia in 2003, NASA located a hard drive in the debris field. The Glenn Research Center sent it to my organization for examination. Although the electronics on that drive had been literally fried, the case burned and plastic from the innards of the device had melted onto the surface of the drives, we were able to rebuild the mechanical components, clean the disk and recover over 99 percent of the data, which turned out to be vital for completing a long-term experiment in basic physics.

With today's technology, unless the media containing the data is utterly destroyed, the data is at least potentially recoverable. I believe that the best practice is that when a device contains sensitive data, assume it might be potentially recoverable, unless you have

taken proper systems steps to render that data permanently unreadable.

Third, what you see is very often not all that you can get. There are a number of data fields that are automatically created and maintained by the program that all of us use. Some are obvious. The date and time that a file was originally written, how many times it was edited, when it was last opened, but it can contain more. It may contain a record of changes made in the course of revision and review. This information is called metadata. It is important to the understanding of the file with which it is associated.

People think that things like this are a brand-new issue, Mr. Chairman, but they are not. If you look at Abraham Lincoln's handwritten manuscript of the Gettysburg Address, you can see how he edited it, what it looked like before he made the changes, what he crossed out and what he added. The same can often be done with digital records through examination of the metadata, but only if that metadata is preserved. Unfortunately, unless care is taken in regard to the preservation process, metadata can inadvertently be changed or lost. To ignore metadata is to constrain future understanding of the file.

Next, ensuring data security must be more than an afterthought. There is a cost to data protection, but, planned effectively, those costs can be controlled. There will always be a tradeoff between cost and protection.

While I'm not an expert in the various security standards that are used by Federal agencies, I found there are a number of centers of knowledge that can be an immense value in understanding the risks and alternatives. The work of professionals at NIST comes to mind. I have no doubt that this subcommittee is aware of the ongoing work there to identify risks, protective measures, and to provide publications that help professionals and managers in both the public and private sector to do a better job of security sensitive data.

Sir, the cost of not protecting data appropriately can be very, very high. What is the cost to future knowledge if electronic records of today's decisions and activities are lost through security failures?

I believe that the expertise exists to assist and advise our government on this complete and continually changing issue. There are many specialists like myself who recognize that service on advisory councils and other appropriate mechanisms is really part of our civic and professional personal duty. Why not call on this pool of knowledge?

If we don't collect data and collect it properly, if we don't maintain it in a usable and complete form, and if we don't safeguard it appropriately, it won't be there for the benefit of future generations.

Finally, we must assure that both public and private sector organizations have a plan for exactly what they will do if there is a data protection incident. Trying to develop a crisis management plan in the middle of a crisis is difficult at best. Recognizing that incidents can occur, and if they do occur, is far more effective in terms of responding to the incident.

I want to thank the subcommittee for inviting me here today. Sir, over the years I've had the opportunity to work with informa-

tion security professionals in government, at the FBI, the Defense Department, the Secret Service, I am very proud of the work that they do. Their public service at a time when they could earn far more in the private sector is a measure of devotion. Anything that we in the private sector can do to add to the knowledge, to make sure that we keep up with the changes, is more than just something that could be done; it's something that ought to be done.

Thank you very much for inviting me here today, sir.

Mr. CLAY. Thank you, too, Mr. Brill, especially for your passion in regard to this subject. And we appreciate your service.

[The prepared statement of Mr. Brill follows:]

Congress of the United States

House of Representatives

One Hundred Eleventh Congress

Committee on Oversight and Government

Subcommittee on Information Policy, Census and National Archives

"The National Archives' Ability to Safeguard the Nation's Electronic Records"

Thursday, November 5, 2009 at 2:00 P.M.

2154 Rayburn House Office Building

Testimony of

Alan E. Brill

Chairman Clay, Ranking Member McHenry, and Members of the Subcommittee. My name is Alan Brill. I am currently a Senior Managing Director at Kroll Ontrack, but I am here not here today as a representative of Kroll Ontrack, but as an individual, to share whatever knowledge and experience I have in the fields of information security, data protection and data recovery to assist the Subcommittee with the vital work it performs I am grateful for the opportunity to speak with you.

The reality is that in today's environment, a substantial proportion of the information that is being created within our government is generated, exchanged and stored digitally. It is produced and stored on computers, be they the desktop or laptop computers of individuals or the massive processing arrays and networks of large agencies. It is also a simple fact that most of the data that is created, and which

may have import for extended periods will never in the course of normal use be printed. How do we safely and efficiently preserve electronic records when the technology involved in producing and storing those records changes at what certainly seems to me to be accelerating and certainly a breathtaking rate. Consider that the first computer I used at the Pentagon in 1968 had a total memory size of two thousand characters. Today, my wristwatch has exponentially more than that. Storage has evolved from being measured in kilobytes, went through megabytes pretty quickly, got to gigabytes, and is now moving on to terabytes. In my firm's data center, we measure our storage capacity in petabytes. One petabyte is equal to one million gigabytes.

I've been involved in the security and recovery of data from computers for more than 40 years. My recent experience has involved working with private sector organizations to safeguard sensitive data and to help those organizations respond to data security incidents. I've learned a few lessons that I hope will be helpful to the Subcommittee when it considers how best to carry out its oversight role in assuring the preservation of records which are a vital part of our national heritage.

1. Don't assume that the devices currently used to store data will be commonly used – or even reasonably available – into the future. I could name a wide range of storage media ranging from 8-inch diskettes I to 7-track magnetic tapes to Magnetic Card Selectric Typewriter cards, to dozens of other formats that are no longer with us. It is very easy to confuse the storage of information with the storage of media containing information. This is not a new concept of course. Paper records have to be stored in a manner that protects the ability to read the information they contain. Magnetic and optical media also have environmental requirements. I've seen tapes stored in tropical climates that actually have moss growing on the reels. Above all else, we must ensure that we can access the information stored on the media we use to preserve important information. This means that we either have to preserve the reading mechanisms (and be prepared to develop interfaces from what will be essentially antique devices to the computers of the future) or periodically transfer the data to contemporary media, as new storage technology obsoletes the old. If we don't pay heed to this, the information may be in our warehouses, but it will be as unreadable as if it were in an ancient language that cannot be translated. Put another way, you might have a great collection of 8-track audio tapes, but you're going to have a problem playing them unless you've preserved player hardware as well, or transferred the data to some other format.

2. Don't assume that data cannot be restored, even if the storage medium appears to be damaged or beyond repair. The technology of data and media recovery has advanced quickly. Take a quick example. Following the tragic loss of the Space Shuttle Columbia in 2003, NASA located 3 hard drives in the debris field. The Glenn Research Center sent them to my firm for examination. Two were beyond hope. The surfaces containing the data had been heated to the point that, in fact, no data remained. On the third drive, plastic had melted onto the drive surfaces. We rebuilt the mechanical components, cleaned the disks, and were able to recover over 99% of the data, which turned out to be vital for completing a long-term physics experiment. With today's technology, unless the media containing the data is utterly destroyed, the data is at least potentially recoverable, potentially readable. And this can be true even for disks that are part of large storage arrays. There are many variations of such arrays, and how they store data. I fully understand that because some storage arrays distribute data across many disk volumes, so that if one disk fails it can be replaced and the data automatically restored to it by the computer using copies on other disks, there is sometimes the belief that individual disks can't be read. That without the whole of the array, one disk is useless. But in many cases, that is not true. It is quite often possible to read the disk and to see at least some of the data that it may contain. Does this mean that it is impossible to completely erase data from a disk drive? No. There are a number of ways to wipe data from a disk very effectively. I know that when I am moving to a new laptop computer, for example, after I have transferred the data that I need, I use software to completely wipe out the information on the drive. Until I do that, I try to protect it with whole disk encryption software, and a number of other safeguards. I believe that best practice is that when a device contains sensitive data that is even potentially recoverable, it must be handled appropriately, and that before the device is decommissioned or discarded, the data must be destroyed through physical or other means. Disks can be cut or smashed. CDs or DVDs can be destroyed with a few seconds of microwave energy. Degaussers can quickly and irrevocably destroy data. But as the disk from the space shuttle showed, data can be tough to destroy. If it's being done, it has to be done right, and such destruction should be documented.
3. What you see is often not all that you can get. Computer programs don't just contain the data that we think about. We all use word processors. And we know that they create files that contain the words we write. But they contain more. There are a number of data fields that are automatically created and maintained by the program. Some are obvious – the date and time the file was originally written, how many times it was edited, when it was last opened. But it can

contain more. For example, it may contain a record of changes made in the course of revision and review. Other information is maintained by the computer's operating system. When you see a list of files, you know that you often see the creation date and size. This specialized information is called metadata, and it is important to the understanding of the underlying data. This is not a new issue. When we look at Abraham Lincoln's handwritten manuscript of the Gettysburg Address, we can see how he edited it, what it looked like before he made the changes. The same can be seen through examination of metadata, but only if it is preserved. Unfortunately, unless care is taken in regard to the processes by which data is preserved, metadata can be inadvertently changed or lost. Our courts recognize this. They have held that merely printing and storing a document may not be enough to properly preserve its value. The metadata can be vital in establishing the authenticity of an electronic document. A will purportedly dated July 1, 2003 might be questioned, for example, if examination of the digital file showed that the file wasn't created until 2005. So data preservation must also take into consideration how to best preserve not only the basic document – the words in an email or the numbers in a spreadsheet, but the metadata as well. To ignore metadata is to contstrain our understanding of the file. Preserving this metadata is not particularly difficult, but it does require a detailed technical understanding of how various copying or preservation processes affect metadata so that the proper methodology can be selected.

4. Ensuring data security must be more than an afterthought. There is no question that there is a cost to data protection. Planned effectively, these costs can be controlled. There is always a trade-off between cost and protection. Identifying the level of protection that is reasonable and appropriate to the data being protected is not necessarily easy. Protective measures that are sufficient today may be insufficient tomorrow as threats mature and evolve. Perhaps the best way to summarize it is to say that if you are complacent about information security, assuming that whatever you're doing today is sufficient and appropriate, and will stay that way, you're setting yourself up for an unpleasant surprise. This is a lesson that has been very publically and painfully learned by organizations across the globe in recent years. While I am not an expert in the various security standards that are used by federal agencies, I have found that there are a number of centers of knowledge which can be of immense value in understanding the risks and alternatives. The work of the professionals at NIST come to mind. I have no doubt that this Subcommittee is aware of the ongoing work there to identify risks, protective measures and to provide publications that can help professionals and managers in both the public and private

sector to do a better job of securing sensitive data. The other reality is that the cost of not protecting data appropriately can be very high. What is the cost of compromising millions of credit card records? Or sensitive medical information? What is the cost to future knowledge if electronic records of today's decisions and activities are lost through security failures, or through permitting security needs to change while protective measures stagnate?

5. Finally, I believe that the expertise exists to assist and advise our government on this complex and continually changing issue. There are many specialists like myself who recognize that service on advisory councils and other appropriate mechanisms is part of our civic and professional duty. Why not call on this pool of knowledge. The reality is this: If we don't collect data and collect it properly, if we don't maintain it in a usable and complete form, and if we don't safeguard it appropriately, it won't be there for the benefit of future generations. Technology is making it possible to not only collect vast amounts of data, but to index it and make it more accessible and useful than ever before. I believe this can be done without undue risk to our privacy and security, if the risks are recognized and there is a commitment to protecting that privacy and taking the right steps to have reasonable security. Can we guarantee 100% security? Of course not, but we can minimize the incidents through the use of encryption, access controls and logging, making sure that users have access to only the information they need, and other techniques. Equally important, we must assure that both public and private sector organizations have a plan for what they will do if there is a data protection incident. Trying to develop a crisis management plan in the middle of a crisis is difficult at best. Recognizing that incidents can occur, and preparing for them is far more effective.

I want to thank the Subcommittee for inviting me here today. I'm fortunate to have had the opportunity to work with information security colleagues in federal service, including the FBI, Secret Service, Inspector General offices and Department of Defense, among other agencies, and I hope you appreciate their service as much as I do. They are fine professionals who could probably earn more in the private sector, but who recognize the value of public service. The subject of today's hearing is important, and the public is well-served by the Subcommittee's interest and focus on this area.

Thank you.

Mr. CLAY. I thank the entire panel for their testimony.

I also want to welcome our newest member to the subcommittee, the gentleman from Texas, Mr. Henry Cuellar. Welcome aboard and we look forward to your involvement in the subcommittee. We will go into the question-and-answer period, and we will recognize the gentleman from Ohio for 5 minutes to begin the questioning.

Mr. DRIEHAUS. Thank you very much, Mr. Chairman, and I thank you for calling this hearing and I appreciate very much the testimony.

This certainly hits home to me. I remember when I was a State Representative, and one of my colleagues called me and recited my Social Security number to me after looking at a county—I believe it was the county auditor or the county recorder or something like that, the Clerk of Courts, whose son had developed a new Web site. They decided it would be great if we scanned every document in the county that came through the Clerk of Courts and they scanned it onto the Web site, not thinking that, you know, perhaps some of these parking tickets out there—and mine was a traffic violation—contained some sensitive information.

But what it brought to mind was that there was no standard operating procedure at all in the county, in the State, anywhere, when it came to not just archiving the data but dealing with the data at all. And so, Mr. Brachfeld, when I hear your testimony, it strikes me as very concerning.

Earlier this year I introduced legislation dealing with classification of documents, because there is no standard operating procedure in the Federal Government when it comes to standard classifications. We find that, you know, the Federal Government exists in silos, and there are different standard operating procedures when it deals to just classifying documents and classifying certain information.

So if you could help me, Mr. Brachfeld, I am very interested—any of you—as to our status as a Federal Government. In terms of coming up with standard procedures for dealing with sensitive documentation and sensitive information, not only how do we collect it but how was it dealt with, and certainly when it was archived, how do we then deal with this archive? Give us a score as to how we are in standardizing this as a process.

Mr. BRACHFELD. Actually the focus of my work is doing investigations and audits. In terms of policy and procedures and classification of documents, that's not my bailiwick.

Mr. DRIEHAUS. Not just classification. I'm talking about the sensitive information that you were talking about and how vulnerable we are to losing that information. It strikes me that within departments we don't have standard operating procedures to deal with this appropriately. I'm wondering if you have any observations as to how far we've come or how far we still have to go in terms of the various departments in collecting and classifying and archiving that data?

Mr. BRACHFELD. I think there are standards available. For example, in the cases I was talking about specific to the loss of data and the breach of data, there is, as Mr. Brill noted as well, there's NIST standards; OMB puts out regulations requirements; agencies establish and define their own internal requirements. The problem is, it

shouldn't just be a paper exercise where you can hold up to the world that we have policies and we have procedures, and then you can put your head on your pillow and think that you can rest assured.

No, you have to actually train people and you have to actually hold people to those standards, and you have to test and you have to drill down, you have to ensure they are enforced and protected at all times.

I think that's what happened many times in Federal agencies, at least through my 30 years now of experience, which is that it is easy to write policy, especially in this day and age, to get contractors and pay them to write policy for you. But to actually instill that work ethic, to actually instill those morals, to actually enforce the proper treatment of records and protection of records, that's the problem.

And that's where in my testimony I talk about where I believe that NARA has fallen short in terms of lack of training, lack of oversight, and then lack of appropriate action when people violate NARA policy and procedures which were drafted in response to OMB requirements. So we don't have a pass and we don't have a buy. These are things we should be doing, and these are things that we fail to do at the National Archives.

Mr. DRIEHAUS. So it is not just a matter of standardization. It is a matter of following through and making sure that the processes are being followed and enforced if they are not followed.

Mr. BRACHFELD. That's correct. And that's why as an Inspector General, I'm first of all very happy to be testifying today and get the attention to this subject. I am also proud of my staff, that we're putting forward very sound recommendations that, should management opt to accept them and adopt them, I think will bring far increased levels of internal control security, and maybe we won't be here next year talking about further breaches. Maybe we'll actually have a pretty tight shop if we do some of the stuff we're recommending.

Mr. DRIEHAUS. Well, I guess following up on the issue of holding people accountable, Ms. Thomas, when you were here in July with regard to the theft of the Clinton administration hard drive, you at the time stated that you would act with swift and appropriate disciplinary action if we found out that there were people to be held accountable. Have you followed up on that, and what steps have been taken?

Ms. THOMAS. Well, at this point in time, we have held off on taking disciplinary actions, although we are ready to do so basically at the request of the Inspector General, so that they can finish their investigation. But once that is finished and they give us the go-ahead, then disciplinary actions will be taken.

Mr. DRIEHAUS. So the disciplinary action is pending?

Ms. THOMAS. Pending.

Mr. DRIEHAUS. That's all, Mr. Chairman.

Mr. CLAY. Thank you, Mr. Driehaus. Mr. McHenry, you may proceed for 5 minutes.

Mr. MCHENRY. Thank you, Mr. Chairman.

Ms. Thomas, how long have you been in your current position?

Ms. THOMAS. As Acting Archivist? Since mid-December of last year.

Mr. MCHENRY. OK. And I ask that just for context, so that is on the record. You know, this committee—I don't think Congress looks at you as the culprit here, but we're asking for your assistance in—well, in light of the fact the Senate has not acted upon the President's nomination of the next Archivist of the United States. But having said that, what policies have changed in light of this additional security breach with the loss of these Veterans' records?

Ms. THOMAS. Mr. Congressman, I think I have to say that our own determination is that we used a governmentwide contract, that other agencies used, that have the appropriate privacy protections written into the contract. And so that our use of that contract was a valid way of sending back a disk.

Now, we've cited that we need to be beyond what's acceptable. And we've adopted a policy; the CIO has, of not sending disks back to the vendor. But we do not believe that any breach has actually occurred, because the material was in the hands of authorized people all along the process.

Mr. MCHENRY. So you have changed policy in that you don't send out——

Ms. THOMAS. We——

Mr. MCHENRY. If I may finish.

Ms. THOMAS. I'm sorry.

Mr. MCHENRY. The two choices, Mr. Brachfeld, you testified the two choices were to secure the data and keep even a failed disk on hand, or send it back and replace it. Those were the two choices. Now you've switched; is that correct?

Ms. THOMAS. The new policy that's been adopted or in place by the CIO is that we will not send any disks back to the contractor.

Mr. MCHENRY. Mr. Brachfeld, thank you for your testimony. You've always been very direct, as all Inspectors General are supposed to be, and we certainly appreciate your work.

Has your office commented previously about this policy of sending these drives out to contractors and getting them back?

Mr. BRACHFELD. It simply never should have happened. Let me read you a sentence, sir, or two. This is when one of the contractors'—the most recent case is Dell. This is what Dell said. "Dell assumes no responsibility for the destruction of data returned on such drives. Dell strongly encourages you to remove all confidential, proprietary, or personal information from any storage device before it is returned to Dell." We didn't do that.

I brought with me a properly scrubbed, sanitized—this is a drive right here. This drive for the purpose of this hearing, this drive has veterans' information for millions of veterans. It's mobile. I'm carrying it. It is a mobile device. It's game, set, match.

If you go to NIST standards or if your go to OMB requirements or if you go to NARA's own internal policy and procedures, once you have PII data stored on a mobile device, it must be encrypted. It must be encrypted, simple fact.

Furthermore, should you ship that or lose custody or give up custody and control, it must be scrubbed, wiped, degaussed. In neither case that we're talking about today was that done. This data went out.

Now it's true. There is a language, boilerplate language, that NARA found about 3 or 4 weeks ago in a contract, and that's what they feel comfortable in telling you; that the vendor, once they received this drive, was supposed to maintain the confidentiality of the data.

But let's go with the first case, the CMRS drive. It didn't just go to one vendor; it went to two, then three, then four. It followed a food chain. First it went back to the company we had a contract with. They sent it to another company to analyze the data on the drive and see if the drive sectors failed. Then it went to another company. And, finally, the fourth stop was a scrap company for the metal scrap.

Now, that's pretty far down the food chain to lose control. We don't know who had access to that within that company. We don't know if it was stored physically in a safe location. We don't know if somebody was embedded in one of these companies who might see this as an opportunity to find Social Security numbers or mine whatever data came their way for profit, national security, etc. We don't know.

So what the National Archives did was violated their own policy, which is derived from NIST standards and OMB regulations, and lost control of millions of veterans' files and records, and now, in the most recent case, thousands of Federal employees. Those are the simple facts.

Mr. MCHENRY. Thank you, Mr. Brachfeld. Now, there was originally veterans' data on that. What process did you go through—is that currently encrypted or did you delete information from that file?

Mr. BRACHFELD. This—this drive did not—I'm very careful, I am careful about what I do. This drive, I have the proper certifications, before I would leave the building with this, that it was wiped. And I have the technology that was used to wipe the drive. I have it certified that it has no information on it at this point. It is clear and again——

Mr. MCHENRY. Mr. Brill, could your company retrieve data off of that "wiped" hard drive?

Mr. BRILL. Sir, if the drive is wiped properly and completely, the answer is generally you cannot. Here is the problem. Either there's a big difference between "I believe I wiped the drive" and "I wiped the drive." We find, for example, that organizations sometimes discover that a disgruntled employee may have run a wiping program to get rid of data that would incriminate them. But not all wiping programs are created equally effectively. And some of them work very, very well and some of them work not well at all. That's why it's important not just to say "wipe the drive" but as I think the Inspector General has suggested, that it be wiped in a forensically acceptable way and possibly tested afterwards to make sure that when we say there's no data that, in fact, there is no data.

Mr. MCHENRY. Thank you for your testimony. I certainly appreciate it. And I don't think this is necessarily about contractors is Mr. Brachfeld's point; it is about secure chain of possession of sensitive information.

And, Mr. Chairman, I think this is a larger cultural issue with archives in terms of employee satisfaction and following basic pro-

cedures. And I certainly appreciate your leadership in making sure that we have good oversight of this to make sure we correct this.

Mr. CLAY. Thank you, Mr. McHenry, for your line of questioning. Mr. Cuellar is recognized for 5 minutes.

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

Ms. Thomas, let me ask you, looking at the big picture, looking at this in hindsight, what do you think the weaknesses are in this IT security? And also as the colleague just mentioned, when you look at not only in your area, but in the food chain or the custody down the line.

Just tell me overall, what do you think the weaknesses are?

Ms. THOMAS. I think one of the things that is happening is that, as Mr. Brill has sort of alluded to, technology is moving at such a fast pace that things—processes and procedures that were acceptable 6 months ago may not be acceptable today.

I know that when I moved to Virginia 30 years ago, my driver's license number was my Social Security number. I think our Social Security numbers were used on a lot of documentation. You were asked to, when you wrote a check; write your driver's license on it. That was your Social Security number.

When all of the information—not all the information but a good deal of the information became electronic and much easier to manipulate and use in nefarious ways and all the data was in a more concentrated small device, like Paul has mentioned, it's becoming more and more of a challenge to deal with that and to protect that information.

So our procedures, our policies, have to catch up to the reality of today and continuously change as technology changes.

Mr. CUELLAR. You said that we got to get our policies to try—looking at the word "try"—to catch up, are you caught up?

Ms. THOMAS. I think we are at the moment, but as Mr. Brill has said, technology tomorrow, I don't know.

Mr. CUELLAR. But you should have something in place that lets you keep up——

Ms. THOMAS. And that is certainly what the administration is doing, that's what OMB is doing, NIST is doing, and we are following those procedures.

Mr. CUELLAR. Let's talk about the internal audit that you conducted on your IT security. When was that performed and by whom?

Ms. THOMAS. We had a contractor, SAIC, come in and review all of our IT security.

Mr. CUELLAR. When was that?

Ms. THOMAS. It was this past year.

Mr. CUELLAR. What was the conclusion?

Ms. THOMAS. Well, they came up with a series of recommendations, I think I said 29 recommendations—at least 29—all of which we are working to implement. Most of them have been by now, and we're working on all of them.

Mr. CUELLAR. Out of 29, how many have been implemented?

Ms. THOMAS. I would have to provide that for the record. I don't know how many.

[The information referred to follows:]

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

November 10, 2009

The Honorable William Lacy Clay
Chairman, House Committee on Government Reform,
Subcommittee on Information Policy, Census and the National Archives
B-349C Rayburn House Office Building
Washington, DC 20515

Dear Chairman Clay:

I am writing to clarify and supplement the record for the Committee concerning the question and discussion about the "audit"/review of NARA's IT security program at the oversight hearing on November 5, 2009. I apologize for not having been able to answer the question as clearly and comprehensively as I would have liked to. I hope this letter helps to clarify the issue.

In the fourth quarter of FY 2007, NARA's Office of Information Services (NH) contracted with SAIC to conduct an assessment of the IT security program using the Program Review for Information Security Management Assistance (PRISMA) methodology developed by the National Institute for Standards and Technology (NIST).[1] The Inspector General was correct in pointing out that the assessment was not a government audit as defined in *Government Auditing Standards*, issued by the Comptroller General of the United States. I was using the term "audit" in an informal manner, and apologize for creating a misunderstanding with the Committee and the Inspector General. The PRISMA methodology is based on the Software Engineering Institute's Capability Maturity Model, a methodology which was incorporated in the CIO Council's *Federal Information Technology Security Assessment Framework* of 2000.

NIST describes the review process as "a proven and successful scalable process and approach to evaluating an organization's information security program" which, when employed, "identifies concise security program corrective actions, which, if taken, can improve the overall security program." The review conducted at NARA indicated that the IT security program was functioning at a level of "satisfactory" in all areas tested – but warned that the program was overly dependent on the personnel implementing it and was immature with respect to key processes required. As a result, NH self-declared an IT Material Weakness in FY 2007.

The report provided 29 broad recommendations. We took these recommendations and put them into a Plan of Action and Milestones (POA&M) and created a work breakdown structure and schedule for each action. We tracked these items against that detailed plan and have accumulated documentation supporting the status report for each of the items in the POA&M. On the basis of the cumulative effect of these actions to establish or improve key processes, management concluded that the

[1] I mistakenly said at the hearing that this review occurred "this past year," when, in fact, it was in 2007.

remaining weaknesses in the IT Security Program did not constitute an externally reportable material weakness, and removed that weakness from the latest Performance Accountability Report. However, we continue to closely monitor the IT Security Program within the agency.

We have established new processes or improvements in response to 27 of the 29 recommendations. However, since many of the items represent a baseline which needs to be continually evaluated over time, POA&M items would not be "closed," as one might see in response to a compliance audit. The recommendations are a means to establish continuous improvement within the IT Security Program.

For example, "Expand Information Assurance Annual Training" is one of the recommendations. NARA's program was found to be compliant with the minimum requirements of the IT Security Architecture, and the guidance provided by NIST Special Publication 800-16, *Information Technology Security Training Requirements*. Nonetheless the assessment found that this training was not being assimilated adequately throughout the organization. In response to this finding, we have formalized our procedures for identifying and taking advantage of training opportunities, enhanced our ability to communicate awareness to NARA employees and contractors, and strengthened our internal training requirements for persons with elevated security responsibilities. This is an on-going activity which must be built into the IT Security Program and it is the strength of the process, not the individual actions which is the target of measurement.

The PRISMA methodology has been proven to establish precisely these types of measurable, repeatable and robust processes, and it is our goal to embed IT Security into the culture of our organization.

We undertook this effort to look at the IT Security Program as a whole because we felt that audits such as those conducted by the Inspector General under the guidelines established by the Comptroller General of the United States tend to identify symptoms of underlying program problems, but frequently do not get to the core requirement of continuous improvement and change at the organizational level. Thus, we considered this review to complement the work of the OIG, and not as a second opinion.

NARA has well established procedures for responding to internal and external audits, and those procedures specify the roles and responsibilities of the parties engaged in conducting and responding to such audits. The PRISMA review was conducted as an internal management action designed to enhance organizational performance, and was not intended to result in findings that would be managed through NARA's audit resolution process. For that reason, the IG was not involved in the assessment itself, the formulation of the recommendations of the assessors, or the approval of the mitigation strategies which were subsequently carried out as part of the plan of action and milestones.

We understand that the "results" oriented approach of the PRISMA methodology does not align neatly to the compliance-based approach of formal audit resolution procedures, and we are aware that the difference between these approaches might lead the IG to conclusions which may differ from those of management. This disagreement notwithstanding, the Inspector General's staff has been apprised of the review and the mitigation plans developed for the POA&M throughout the process and has provided useful input to the procedures which have been put in place since 2007.

Below is a current assessment of our completion of actions:

The PRISMA assessment identified 29 recommendations to strengthen NARA's IT Security program in early fiscal year 2008. When we documented the recommendations as a detailed Plan of Action and Milestones (POA&M) we further divided the first two recommendations into four separate actions, thus creating 31 items to be tracked by the POA&M.

The two recommendations and their associated actions were decomposed in the following manner:

1. Recommendation 3.1-1(a) - Centralize all IT security policy...
    - Action 1 - Add and document NHI Staff
    - Action 2 - Document roles and responsibilities

2. Recommendation 3.1-1(b) - Establish oversight / compliance and address POA&Ms in timely manner...
    - Action 1 - System owners sign off on C&A
    - Action 2 - TRG meeting held every 5th week to review POA&Ms

Attached please find the IT Material Weakness POA&M spreadsheet and Material Weakness summary which identifies mitigation strategies for each of the 31 discreet POA&M items. We would be happy to provide the Subcommittee with all related documentation if that would be helpful.

Based on the work products associated with the POA&M, we believe that of the 29 original PRISMA recommendations 27 have been either completed or the recommended processes have been established and the process is operational and ongoing.

The remaining two recommendations are still being worked:

> a) Finalize NH Strategic Plan (this no. 25 in the tracking document). A draft strategic plan has been published and has been circulated for review to NARA senior management. The plan is projected to be complete in the first quarter FY10.
>
> b) Conduct periodic incident response testing exercises (this is no. 31 in the tracking document.) A contract has been established with an independent third party to review NARA's incident response procedures, develop a plan to train and exercise those procedures, and conduct simulation exercises appropriate to the threat facing the agency's IT systems. This is projected to take two years, and the initial report of the evaluator is expected during the first quarter FY 10.

Once again, I apologize for not having been able to provide you this level of detail at the hearing, and thus causing confusion and uncertainty. I also greatly regret that we do not see eye-to-eye with the Inspector General about the usefulness and current status of this review process, which only serves to supplement the important work that his office performs. We will continue to view the OIG as a partner in future reviews.

Please feel free to contact me if you have additional questions.

Sincerely,

Adrienne C. Thomas

ADRIENNE C. THOMAS
Acting Archivist of the United States

cc: The Honorable Patrick McHenry, Ranking Member

Enc. (2)

IT Material Weakness
POA&M Summary Artifacts – August 31, 2009

Audit #	Weakness / Issue	Resolution	*Documentation*
1) PRISMA – Issue 3.1-1	Formalize NHI Organization	Staff added and documented roles and responsibilities	*1 – NHI Organization.ppt*
2) PRISMA – Issue 3.1-1	Document more specific roles and responsibilities for System Owner and Information System Security Officer (ISSO).	Documented System Owner and ISSO roles and responsibilities. Formal sign-off on appointment letters outlining duties and responsibilities.	*2a – Designated SO-ISSO.082109 htd* *2b – AAD – ISSO* *2c – ACMD io – ISSO* *2d – AERIC – SO* *2e – APS Title 13 – SO* ***(54 SO and ISSO Signed Letters)***
3) PRISMA – Issue 3.1-1	Establish oversight / compliance function.	System Owner and Office Head C&A formal approval	*3a – 43 RCPBS Accreditation Letter* *3b – 17 OFAS Accreditation Letter*
4) PRISMA – Issue 3.1-1	Establish oversight / compliance function (continued).	NH Technical Review Group (NH TRG) weekly meetings established – POA&M / Material Weakness, Product Plan / Deliverable Review, and Project Status Reports	*4a – NH TRG Weekly Meeting FY08* *4b – NH TRG Weekly Meeting FY09* *4c-* *NH_Technical_Review_Group_062309_Meeting_Notes_Draft* ***(79 NH TRG Meetings held and documented in FY08 & FY09)***
5) PRISMA – Issue 3.1-1	Develop and distribute procedures for removing system access.	Developed and formalized NARA 279	*NARA 279*
6) PRISMA – Issue 3.1-1	Establish procedures are being implemented effectively.	NH Technical Review Group (NH TRG) Weekly Meetings.	*See Documentation for Action Item 4*
7) PRISMA – Issue 3.1-2	Review relationships with business / system owners to enforce roles and responsibilities and delegate appropriate security activities.	Signed System Owner Appointment Letter w/duties and responsibilities & IT Security Methodologies	*See Documentation for Action Item 2 and IT Security Methodologies* ***(17 IT Security Methodologies documented to align to NIST Control Families)***
8) PRISMA –	Review and formalize	Document more specific	*See Documentation for Action Items 2 and 4*

Issue 3.1-2	relationships with other security operations.	roles and responsibilities via System Owner and ISSO designation letters. NH TRG to include reviews of POA&Ms and RFC / RFW which includes NHT (includes Operational Security).	
9) PRISMA – Issue 3.1-2	Review and repair relationships with OIG.	Quarterly OIG and NHI Status Meetings	*Meeting on Contingency Plans - Attachments and Conference #.doc*
10) PRISMA – Issue 3.1-2	Document more specific roles and responsibilities for Authorizing and Certifying Officials.	Signed System Owner Appointment Letter w/duties and responsibilities	*See Documentation for Action Item 2*
11) PRISMA – Issue 3.2-1	Conduct comprehensive security planning process including System Security Plans	Roles and responsibilities outlined in System Owner Appointment Letter w/duties and responsibilities	*See Documentation for Action Item 2*
12) PRISMA – Issue 3.2-1	Establish / enforce security planning roles and responsibilities with program managers and system / information owners	NH TRG Weekly Meetings (Business Case Reviews w/Product Owners), ARB Monthly Meetings, BIA / CP Meetings.	*See Documentation for Action Items 2 and 4* *9 - Meeting on Contingency Plans - Attachments and Conference #.doc* ***(22 ARB Meetings held and documented in FY08 & FY09)***
13) PRISMA – Issue 3.2-1	Assess SSPs and provide a gap analysis of deficiencies.	NHI / SAIC Weekly Meeting – add agenda item for SSP review.	*13a – NHI Weekly Meeting FY08* *13b – NHI Weekly Meeting FY09* *13c - NHI.Weekly.Meeting.Summary.090807* ***(64 NHI / SAIC Weekly Meetings held and documented in FY08 & FY09)***

14) PRISMA – Issue 3.3-1	Expand Information Assurance Annual Training.	FY2009 Training - BIA II Meeting, CP Test Strategy Meetings, Annual IA Awareness Day, IA Annual Training, FOSA Conference, and AO Conference.	*14a – NARA Notice 2009 – 192.html* *14b – NARA Notice 2009 – 232.html* *14c – NARA Notice 2009 – 261.html*
15) PRISMA – Issue 3.3-1	Policies and procedures do not address the totality of functional, security areas, roles-based, training requirements, and complete, program, implementation practices.	Update Information Assurance Training and Awareness Methodology to define roles (e.g., users with significant responsibilities).	*15 - Security Training and Awareness Methodology.pdf*
16) PRISMA – Issue 3.3-1	Incorporate role-based, Security Awareness, Training and Education (SATE) participation as part of personnel reviews.	Update Awareness and Training Methodology.	*See Documentation for Action Item 15.*
17) PRISMA – Issue 3.4-1	Recommend Directive 801 process updates to include Security costs and implications.	Updated and delivered April 3, 2008. Completed with inclusion in 04/08 801 update that requests security costs on abbreviated and full product plans.	*17 - 801 – Supp-decide.doc*
18) PRISMA – Issue 3.4-1	Revise SDLC control gates to ensure policies are implemented effectively throughout the lifecycle	Addressed via NH Technical Review Group (NH TRG) weekly meetings - Product Plan / Deliverable Review, and Project Status Reports.	*See Documentation for Action Item 4*

19) PRISMA – Issue 3.4-2	Provide more clarity to security budget and fiscal planning at the system and program levels.	Updated and delivered April 3, 2008. Completed with inclusion in 04/08 801 update that requests security costs on abbreviated and full product plans.	*See Documentation for Action Item 17*
20) PRISMA – Issue 3.4-2	Institute appropriate practices and mechanisms to provide more clarity to security budget and fiscal planning at the system and program levels.	Updated and delivered April 3, 2008. Completed with inclusion in 04/08 801 update that requests security costs on abbreviated and full product plans.	*See Documentation for Action Item 17*
21) PRISMA – Issue 3.5-1	Develop procedures for determining whether additional security requirements are necessary when design constraints or design selection preferences exist during system design	NH TRG – Product Plan / Deliverable Review Meeting Notes. Procedure covered in EA Methodology (Directive 812) – EA Review Criteria.	*See Documentation for Action Item 4*
22) PRISMA – Issue 3.5-1	Develop proposed update to Directive 805 for protection of information and data.	Delivered draft NARA 805 update to Security Guidelines on April 3, 2008. To be incorporated in next update of NARA 805.	*22 - Redline_System.Development.Guidelines _040208.update*
23) PRISMA – Issue 3.5-1	Develop policy and procedures that fully require system, security documentation update and control to include the system security plan and IT Contingency Plan	Updated CP Methodology, CP Template, and CP Process that was reviewed with all System Owners.	*23 - NARA IT Security Methodology for Contingency Planning.pdf*
24) PRISMA – Issue 3.5-1	Review NARA's SDLC control gates for effectiveness,	Delivered draft NARA 805 updates to Security	*See Documentation for Action Items 17 and 22*

	enforcement, and integration with security and CPIC.	Guidelines on April 3, 2008 & NARA 801 update, and Roles and Responsibilities.	
25) PRISMA – Issue 3.5-2	Enact an initiative to collect IT requirements and needs for all agency programs	Draft NH Strategic Plan developed with input from all NH Divisions.	*25 - NARA NH Strategic Plan Draft v5 7.21.09.doc*
26) PRISMA – Issue 3.5-2	Update / develop guidance to NH for areas to consider during procurement (e.g., IPv6, Security, etc.).	NH Memorandum on areas to consider during IT acquisitions including Security	*26 – Contracting clauses for IT acquisitions.doc*
27) PRISMA – Issue 3.6-1	Incomplete contingency and disaster planning procedures	Updated Contingency Planning Methodology (3Q09).	*See Documentation for Action Item 23*
28) PRISMA – Issue 3.6-1	Reassess the contingency and disaster recovery plans under the updated policy and procedures including formal approval and signature	Develop Contingency Plan Template and review and update w/System Owner, Continue to test annually,	*28 - C&A Tracking Spreadsheet.doc*
29) PRISMA – Issue 3.6-2	NARA's information systems may be impacted due to incomplete policy, procedures, and corresponding incident identification, reporting, and response, security control implementation.	Signed System Owner Appointment Letter w/duties and responsibilities	*See Documentation for Action Item 2*
30) PRISMA – Issue 3.6-2	Update and issue as final IT Security Incident Handling Guide.	Delivered update on 9/25/08.	*30 - Updated Computer Security Incident Handling Guide v1.31 final.doc*
31) PRISMA – Issue 3.6-2	*Conduct period test of IT Security Incident Response using IT Security Incident Handling Guide.*	*NHI started work on acquisition of independent incident response capabilities assessment services.*	*Three year contract expected to be awarded by 8/31/09*

IT MATERIAL WEAKNESS POA&M - August 25, 2009

Audit #	Recommendation # / Description	Control Family	Weakness / Priority	POC	Resources	Scheduled	Milestones with Completion	Changes to Milestones	VOE	Status
1) PRISMA – Issue 3.1-1	Recommendation 3.1-1(a): Centralize all IT security policies and clearly relate associated IT policies to be followed easily by all personnel (e.g., developers, system administrators, security officers, users) who develop, install, maintain, monitor, and use NARA's IT resources.	Planning	IT security-related policies are not effective ... / Med-Low	Leo Scanlon	CIO and NHI	FY08 / FY09	Formalize NHI Organizational Structure - 2Q08	New Org. Structure documented via org. chart and responsibilities	Organization Chart and Responsibilities	Completed
2) PRISMA – Issue 3.1-1	Recommendation 3.1-1(a): Centralize all IT security policies and clearly relate associated IT policies to be followed easily by all personnel (e.g., developers, system administrators, security officers, users) who develop, install, maintain, monitor, and use NARA's IT resources.	Planning	IT security-related policies are not effective ... / Med-Low	Leo Scanlon	NHI, CIO, NHP, NPOL, Agency	FY08 / FY09	Document more specific roles and responsibilities via System Owner and Information System Security Officer (ISSO) designation letters - 2Q09	Signed System Owner Appointment Letter w/duties and responsibilities	Spreadsheet and Signed System Owner and ISSO letters	Process Established / Ongoing
3) PRISMA – Issue 3.1-1	Recommendation 3.1-1(b): Establish an oversight and compliance function either at the agency or system level to ensure that all IT security-related documentation is compliant with agency, Federal, and NIST guidelines, and all POA&M items are addressed and resolved in a timely manner.	Planning	IT security-related policies are not effective ... / Med-Low	Leo Scanlon	NHI, SAIC	FY08 / FY09	Pre-ST&E activities checklist and sys. owner sign-off - 2Q08	System Owner and Office Head C&A approval documentation	Signed C&A letters w/Office Head approval	Process Established / Ongoing
4) PRISMA – Issue 3.1-1	Recommendation 3.1-1(b): Establish an oversight and compliance function either at the agency or system level to ensure that all IT security-related documentation is compliant with agency, Federal, and NIST guidelines, and all POA&M items are addressed and resolved in a timely manner.	Planning	IT security-related policies are not effective ... / Med-Low	Leo Scanlon	NH TRG	FY08 / FY09	NH Technical Review Group (NH TRG) – POA&M / Material Weakness, Product Plan / Deliverable Review, and Project Status Report Meeting Notes - Ongoing Weekly	NH TRG Meetings	NH TRG FY08 & FY09 Meeting Dates and example notes	Process Established / Ongoing
5) PRISMA – Issue 3.1-1	Recommendation 3.1-1(c): Identify and develop procedures to comply with the security control areas (e.g., password configuration, changing, and distribution; controlling system access (approving, creating, suspending, and termination)). These procedures should be vetted to ensure they are effectively communicated.	Access Control	IT security-related policies are not effective ... / Med-Low	NA	NA, NPOL, Agency	FY08 / FY09	Develop and distribute procedures for removing system access. (CG 08-03) - 2Q08	NARA 279	NARA 279	Completed - 8/18/08
6) PRISMA – Issue 3.1-1	Recommendation 3.1-1(d): Establish mechanisms or measurements to ensure procedures are being implemented effectively (e.g., C&A, patch management, configuration management).	Configuration Management	IT security-related policies are not effective ... / Med-Low	Leo Scanlon	NHI, SAIC, NHT	FY08 / FY09	NH Technical Review Group (NH TRG) – POA&M / Material Weakness, Product Plan / Deliverable Review, and Project Status Report Meeting Notes - Ongoing Weekly	NH TRG Meetings	See VOE for Audit Item # 4	Process Established / Ongoing
7) PRISMA – Issue 3.1-2	Recommendation 3.1-2(a): Review relationships with business/system owners to enforce roles and responsibilities and delegate appropriate security activities.	Planning	Review, restructure, and formalize IT Security Office's relationships w/other security offices and business / system owners. / Med-Low	Leo Scanlon	NHI, NHP, NPOL, Agency	FY08 / FY09	Document more specific roles and responsibilities via System Owner and Information System Security Officer (ISSO) designation letters (2Q09) and IT Security Methodologies for each NIST control family via (2H08).	Signed System Owner Appointment Letter w/duties and responsibilities & IT Security Methodologies	See VOE for Audit Item # 2 & IT Security Methodologies (Screen Shot from NHI Webpage)	Process Established / Ongoing
8) PRISMA – Issue 3.1-2	Recommendation 3.1-2(b): Review and formalize relationships with other security operations. Consider restructuring communications and lines of authority to enable formal and repeatable integration between physical [paper and physical security] and logical environments.	Planning	Review, restructure, and formalize IT Security Office's relationships w/other security offices and business / system owners. / Med-Low	Leo Scanlon	NHI, NH, NHP, NPOL, Agency	FY08 / FY09	Document more specific roles and responsibilities via System Owner and Information System Security Officer (ISSO) designation letters - 2Q09. NH TRG to include reviews of POA&Ms and RFC / RFW which includes NHT (includes Operational Security).	1) Signed System Owner Appointment Letter w/duties and responsibilities, 2) NH TRG Weekly Meetings, and 3) Partnership with NAS.	See VOE for Audit Item #2 and #4	Process Established / Ongoing

Audit #	Recommendation # / Description	Control Family	Weakness / Priority	POC	Resources	Scheduled	Milestones with Completion	Changes to Milestones	VOE	Status
9) PRISMA – Issue 3.1-2	Recommendation 3.1-2(c): Review and repair relationships with OIG. Successful organizations demonstrate a strong working relationship between OIG and CIO/SAISO offices.	Planning	Review, restructure, and formalize IT Security Office's relationships w/other security offices and business / system owners. / Med-Low	Leo Scanlon	NHI, OIG	FY08 / FY09	Quarterly OIG and NHI Status Meetings including notes and action items - Ongoing - Quarterly beginning 2Q08	Quarterly / Ongoing Meetings w/OIG	BIA II Kickoff Meeting notice (OIG invited)	Process Established / Ongoing
10) PRISMA – Issue 3.1-2	Recommendation 3.1-2(d): Review and update information system roles and responsibilities based on redefined security procedures and organizational relationships. Define roles and corresponding responsibilities for Authorizing and Certifying Officials.	Planning	Review, restructure, and formalize IT Security Office's relationships w/other security offices and business / system owners. / Med-Low	Leo Scanlon	NHI, NH, NHP, NPOL, Agency	FY08 / FY09	Document more specific roles and responsibilities via System Owner and Information System Security Officer (ISSO) designation letters - 2Q09	Signed System Owner Appointment Letter w/duties and responsibilities	See VOE for Audit Item #2	Process Established / Ongoing
11) PRISMA – Issue 3.2-1	Recommendation 3.2-1 (a): Review and update NARA's policy statement for security planning and develop methodical process [procedure] traceable to policy identifying NARA specific elements of who, what, when, and how and with identified control gates for all security controls identified in NIST 800-53/53A.	Planning	NARA's information systems are not benefiting from a comprehensive security planning process and documented SSPs. / Med-Low	Leo Scanlon	NHI, NH, NHP, NPOL, Agency	FY08 / FY09	Document more specific roles and responsibilities via System Owner and Information System Security Officer (ISSO) designation letters - 2Q09. NH TRG Meetings - Business Case / Deliverables Review.	Signed System Owner Appointment Letter w/duties and responsibilities	See VOE for Audit Item #2	Process Established / Ongoing
12) PRISMA – Issue 3.2-1	Recommendation 3.2-1 (b): Establish/enforce security planning roles and responsibilities with program managers and system/information owners.	Planning	NARA's information systems are not benefiting from a comprehensive security planning process and documented SSPs. / Med-Low	Leo Scanlon	NH TRG	FY08 / FY09	NH Technical Review Group (NH TRG) – POA&M / Material Weakness, Product Plan / Deliverable Review, and Project Status Report Meeting Notes - Ongoing Weekly	NH TRG Weekly Meetings (Business Case Reviews w/Product Owners), ARB Monthly Meetings, BIA / CP Meetings	See VOE for Audit Item # 4 and # 9 and ARB Meeting Dates / example notes.	Process Established / Ongoing
13) PRISMA – Issue 3.2-1	Recommendation 3.2-1 (c): Form a security planning assessment team to review each SSP and provide a gap analysis of deficiencies. Update accordingly.	Certification and Accreditation	NARA's information systems are not benefiting from a comprehensive security planning process and documented SSPs. / Med-Low	Leo Scanlon	NHI, System Owners	FY08 / FY09	NHI Team Meeting standing agenda item for SSP review – NHI Meeting Notes - Ongoing as SSPs are developed / updated.	NHI / SAIC Weekly Meetings	NHI / SAIC FY08 & FY09 Meeting Dates and example notes	Process Established / Ongoing
14) PRISMA – Issue 3.3-1	Recommendation 3.3-1(a): Develop or append policy and procedures to include forms of training (example: incident response) in addition to orientation Security Awareness, Training and Education (SATE) training and annual refresher training. Include any requirements for training when moving to a new position. Also, discuss certification training and qualifications of the proctor for training courses.	Planning	Policies and procedures do not address the totality of functional, security areas, roles-based, training requirements, and complete, program, implementation practices. / Med-Low	Leo Scanlon	NHI, NA, SAIC, agency	FY08 / FY09	Update IA New Employee Orientation (1Q08), hold C&A / SSP Brownbag (2Q08), conduct annual IA awareness day (2Q08), provide annual training (4Q08), and provide file encryption training (1Q08).	FY2009 Training - BIA II Meeting, CP Test Strategy Meetings, Annual IA Awareness Day, IA Annual Training, FOSA Conference, and AO Conference.	NARA Notice 2009-192, 1009-232 (IA Training and Reminder) and 2009-261	Process Established / Ongoing
15) PRISMA – Issue 3.3-1	Recommendation 3.3-1(b): Develop or append policy to include a requirement for users to have access to organizational policies and procedures. Also, it is recommended that all users be able to easily access any rules of behavior that may be applicable to them.	Planning	Policies and procedures do not address the totality of functional, security areas, roles-based, training requirements, and complete, program, implementation practices. / Med-Low	Leo Scanlon	NHI, SAIC, NCON	FY08 / FY09	Update Information Assurance Training and Awareness Methodology to define roles (e.g., users with significant responsibilities)		Training and Awareness Methodology.	Process Established / Ongoing
16) PRISMA – Issue 3.3-1	Recommendation 3.3-1(c): Incorporate role-based, SATE participation as part of personnel reviews.	Planning	Policies and procedures do not address the totality of functional, security areas, roles-based, training requirements, and complete, program, implementation practices. / Med-Low	Leo Scanlon	CIO, NHI, SAIC, NA	FY08 / FY09	Develop ISSO / FOSA Roles and Responsibilities - 3Q08	Update Awareness and Training Methodology.	See VOE for Audit # 15	Process Established / Ongoing

Audit #	Recommendation # / Description	Control Family	Weakness / Priority	POC	Resources	Scheduled	Milestones with Completion	Changes to Milestones	VOE	Status
17) PRISMA – Issue 3.4-1	Recommendation 3.4-1(a): Update, revise, and develop a comprehensive set of policies and procedures that also include security, as appropriate, and reference specific, security-related polices and procedures.	Planning	NARA budgeting, resource, and procurement-related policies and procedures lack sufficient security requirements and integration. / Med-Low	Leo Scanlon	NHI, SAIC, NHP, NPOL, Agency	FY08 / FY09	Recommend Directive 801 process updates to include Security costs and implications - 2Q08	Updated and delivered April 3, 2008. Completed with inclusion in 04/08 801 update that requests security costs on abbreviated and full product plans.	Interim Guidance 801-2, Review of Information Technology (IT) Investments - Product Plan template - see section 4.5	Process Established / Ongoing
18) PRISMA – Issue 3.4-1	Recommendation 3.4-1(b): Institute, align, or revise SDLC control gates to ensure policies are implemented effectively throughout the lifecycle.	Planning	NARA budgeting, resource, and procurement-related policies and procedures lack sufficient security requirements and integration. / Med-Low	Leo Scanlon	NHI, SAIC, NHP, NH TRG, NPOL, Agency	FY08 / FY09	Addressed via NH Technical Review Group (NH TRG) weekly meetings (3Q08). Product Plan / Deliverable Review, and Project Status Report Meeting Notes - Ongoing / Weekly	NH TRG Weekly Meetings	See VOE for Audit Item #4	Process Established / Ongoing
19) PRISMA – Issue 3.4-2	Recommendation 3.4-2(a): NARA should identify within their policies discrete line items for information security and establish them in programming and budget documentation along with the supporting procedures.	Planning	NARA should institute appropriate practices and mechanisms to provide more clarity to security budget and fiscal planning at the system and program levels. / Med-Low	Leo Scanlon	NHI, SAIC, NHP, NPOL, Agency	FY08 / FY09	Recommend Directive 801 Process updates to include Security costs and implications - 2Q08	Updated and delivered April 3, 2008. Completed with inclusion in 04/08 801 update that requests security costs on abbreviated and full product plans.	See VOE for Audit Item #17	Process Established / Ongoing
20) PRISMA – Issue 3.4-2	Recommendation 3.4-2(b): NARA should supply, as part of their procedures, sample, common, security areas and templates to enable normalization in future trend analyses.	Planning	NARA should institute appropriate practices and mechanisms to provide more clarity to security budget and fiscal planning at the system and program levels. / Med-Low	Leo Scanlon	NHI, SAIC, NHP, NPOL, Agency	FY08 / FY09	Recommend Directive 801 Process updates to include metrics and templates - 2Q08.	Updated and delivered April 3, 2008. Completed with inclusion in 04/08 801 update that requests security costs on abbreviated and full product plans.	See VOE for Audit Item #17	Process Established / Ongoing
21) PRISMA – Issue 3.5-1	Recommendation 3.5-1(a): Develop procedures for determining whether additional security requirements are necessary when design constraints or design selection preferences exist during system design	Planning	NARA's information security planning and expenditures may be incorrectly allocated due to a lack of integration of security planning and funding into the SDLC. / Med-Low	Leo Scanlon	NHI, NH TRG	FY08 / FY09	NH TRG – Product Plan / Deliverable Review Meeting Notes. Procedure covered in EA Methodology (Directive 812) – EA Review Criteria - Ongoing Weekly.	NH TRG Weekly Meetings	See VOE for Audit Item #4	Process Established / Ongoing
22) PRISMA – Issue 3.5-1	Recommendation 3.5-1(b): Specify in policy and procedures the security constraints to protect information and data during the system test phase, to include specific types of test data	Planning	NARA's information security planning and expenditures may be incorrectly allocated due to a lack of integration of security planning and funding into the SDLC. / Med-Low	Leo Scanlon	NHI, SAIC, NHP, NPOL, Agency	FY08 / FY09	Develop proposed update to Directive 805 for protection of information and data - 3Q08.	Delivered draft NARA 805 update to Security Guidelines on April 3, 2008.	Proposed revisions to NARA 805 submitted to NHP/NHPC for next update.	Completed
23) PRISMA – Issue 3.5-1	Recommendation 3.5-1(c): Develop policy and procedures that fully require system, security documentation update and control to include the system security plan and IT Contingency Plan	Contingency Planning	NARA's information security planning and expenditures may be incorrectly allocated due to a lack of integration of security planning and funding into the SDLC. / Med-Low	Leo Scanlon	NHI, SAIC, System Owners	FY08 / FY09	Develop Contingency Plan Template, review and update w/System Owner, and update SSP (if necessary) - 2H08	Updated CP Methodology, CP Template, and CP Process that was reviewed with all System Owners on 3/26/09	NARA IT Security Methodology for Contingency Planning	Process Established / Ongoing

Audit #	Recommendation # / Description	Control Family	Weakness / Priority	POC	Resources	Scheduled	Milestones with Completion	Changes to Milestones	VOE	Status
24) PRISMA – Issue 3.5-1	Recommendation 3.5-1(d): Review NARA's SDLC control gates for effectiveness, enforcement, and integration with security and CPIC. Document control gates in terms of objectives, inputs, outputs, feedback loops [metrics for performance monitoring], approvals, and enforcement.	Planning	NARA's information security planning and expenditures may be incorrectly allocated due to a lack of integration of security planning and funding into the SDLC. / Med-Low	Leo Scanlon	NHI, SAIC, NHP, NPOL, Agency	FY08 / FY09	Develop proposed updates to 801 (2Q08) and 805 (3Q08).	Delivered draft NARA 805 update to Security Guidelines on April 3, 2008, NARA 801 update, and Roles and Responsibilities.	See VOE for Audit Item #17 and #22	Completed
25) PRISMA – Issue 3.5-2	Recommendation 3.5-2(a): Enact an initiative to collect IT requirements and needs for all agency programs through a data call or tiger team. This may be more effective from the EA office with security supporting the effort.	Planning	NARA's SDLC should be communicated and enforced for all development activities despite size, funding, or location (Note: some flexibility may be needed). / Med-Low	Leo Scanlon	All NH	FY09	Develop NH Strategic Plan.	Draft NH Strategic Plan developed with input from all NH Divisions.	Draft NH Strategic Plan	Draft circulating for comment
26) PRISMA – Issue 3.5-2	Recommendation 3.5-2(b): Update policy and procedures to address security in contract solicitation documents to include updating security controls as new threats/vulnerabilities are identified and as new technologies are used.	System and Services Acquisition	NARA's SDLC should be communicated and enforced for all development activities despite size, funding, or location (Note: some flexibility may be needed). / Med-Low	Leo Scanlon	NHI, CIO, NAA, SAIC	FY08 / FY09	Update / develop guidance to NH for areas to consider during procurement (e.g., IPv6, Security, etc.).	NH Guidance on areas to consider including Security	NH Memomadum on Contracting clauses for IT acquisitions	Process Established / Ongoing
27) PRISMA – Issue 3.6-1	Recommendation 3.6-1(a): Update policy to include comprehensive and formal "shall" statements. Develop complimentary security procedures to implement the security control and describe the performance parameters of how, when, who, and what needs to be performed.	Planning	NARA's business operations and IT assets are at risk due to incomplete contingency and disaster planning procedures rooted in an all-inclusive policy. Currently, contingency and disaster planning policy and procedures are incomplete in some areas. / Med-Low	Leo Scanlon	NHI, SAIC, NHP, NPOL, Agency	FY08 / FY09	Updated Contingency Planning Methodology (3Q09).		See VOE for Audit Item #23	Process Established / Ongoing
28) PRISMA – Issue 3.6-1	Recommendation 3.6-1(b): Reassess the contingency and disaster recovery plans under the updated policy and procedures including formal approval and signature, version control, full notification steps including interconnected systems, plan storage and dissemination, personnel relocation support, periodic testing, etc.	Contingency Planning	NARA's business operations and IT assets are at risk due to incomplete contingency and disaster planning procedures rooted in an all-inclusive policy. Currently, contingency and disaster planning policy and procedures are incomplete in some areas. / Med-Low	Leo Scanlon	NHI, SAIC, System Owners	FY08 / FY09	Develop Contingency Plan Template and review and update w/System Owner, Continue to test annually - 2H08.		See BIA / CP Tracking Spreadsheet	Process Established / Ongoing
29) PRISMA – Issue 3.6-2	Recommendation 3.6-2(a): Update policy to include comprehensive and formal "shall" statements. Develop complimentary, security procedures to implement the security control and describe the performance parameters of how, when, who, and what needs to be performed.	Planning	NARA's information systems may be impacted due to incomplete policy, procedures, and corresponding incident identification, reporting, and response, security control implementation. / Med-Low	Leo Scanlon	NHI, SAIC, NHP, NPOL, Agency	FY08 / FY09	Update 804.8 with more specific roles, responsibilities, and relationships - 4Q08.	Signed System Owner Appointment Letter w/duties and responsibilities	See VOE for Audit Item #2	Process Established / Ongoing
30) PRISMA – Issue 3.6-2	Recommendation 3.6-2(b): NARA IT Security Incident Handling Guide, v3.0 should be reviewed, approved, and marked as final.	Incident Response	NARA's information systems may be impacted due to incomplete policy, procedures, and corresponding incident identification, reporting, and response, security control implementation. / Med-Low	Leo Scanlon	NHI, SAIC	FY08 / FY09	Update and issue as final IT Security Incident Handling Guide - 2Q08.	Delivered update on 9/25/08. Completed.	Updated Computer Security Incident Handling Guide	Completed
31) PRISMA – Issue 3.6-2	Recommendation 3.6-2(c): Periodically test incident response plan and capability through exercises and penetration test activities. Modify incident response plan and training based on results and feedback.	Incident Response	NARA's information systems may be impacted due to incomplete policy, procedures, and corresponding incident identification, reporting, and response, security control implementation. / Med-Low	Leo Scanlon	NHI, CIRT Team	FY08 / FY09	Conduct period test of IT Security Incident Response using IT Security Incident Handling Guide and update procedures based on new contractor input - 1H10	NH started work on acquisition of independent incident response capabilities assessment services.	Three year contract expected to be awarded by 8/31/09	Est. Award on 8/31/09

Mr. CUELLAR. You don't know right now how many have been implemented?

Ms. THOMAS. I do not know. I know it's more than 50 percent, probably more like three-quarters.

Mr. CUELLAR. You can see how that can be a problem. If you do an internal audit to see what your weaknesses are and we haven't implemented, how long would it take you to implement 100 percent of the recommendations, of 29 recommendations?

Ms. THOMAS. I know that the CIO is working on implementing all of the recommendations, and I am going to say that within the next 6 months. And I may have to correct that after I talk to the CIO. I'm sorry.

Mr. CUELLAR. So if we are going to try to keep up with the changes that you mentioned, have your policy keep up, we have to wait another 6 months to implement those?

Ms. THOMAS. These are identified weaknesses which we are trying to correct in all instances. Some are more serious than others. Those are the ones that we have tackled first.

Mr. CUELLAR. Well, let me ask you, Mr. Brachfeld, was this in fact an audit, and who performed it?

Mr. BRACHFELD. It technically cannot be considered an audit. It was performed by SAIC under what is called a Program Review for Information Service Management Assistance. It's called PRISMA. So it's not technically allowed to be called an audit. It was not an audit. It does not—in fact; SAIC in their PRISMA report, specifically states that it's not an audit.

Mr. CUELLAR. What would you classify that?

Mr. BRACHFELD. It's a review that was done for management, in addition to the audit work that we do. Where we have determined that IT Security is a material weakness, management opted to get a second opinion, so to speak, and contracted for SAIC to do that work. They came out with a finding of 29; I believe it was, weaknesses that they identified.

Mr. CUELLAR. Now you have reviewed those, that matter. Do you know how many of the 29 recommendations NARA has implemented?

Mr. BRACHFELD. My IT auditors, whom I have a tremendous amount of faith in and who have been right throughout in terms of their analysis, determined that 27 of the 29 have not been adopted to date. We believe that only two have been closed out and completed to our satisfaction.

Mr. CUELLAR. Mr. Chairman, can I just follow on up on that? Twenty-seven out of the 29 have not been implemented?

Mr. BRACHFELD. That was reported on September, I believe, 9th or 20th. It was reported just this past month to management. We put together a matrix defining why we believe 27 to 29 had not been corrected. We requested a meeting in September to discuss this. And it is now November 5th, and our request for a meeting has not been addressed.

Mr. CUELLAR. And the question, Mr. Chairman, was—I believe Ms. Thomas' testimony was that more than half or three-quarters of it had been implemented, and Mr. Brachfeld is saying that, according to his folks, that only two have been implemented and the meeting has not been set up, and I find that a little disturbing.

Mr. CLAY. Sounds like there is some discrepancy. Thank you.

Now, Ms. Thomas, you assured the subcommittee in July that in regard to the theft or loss of the Clinton administration hard drive, you would act with swift and appropriate disciplinary action. Have you made your determinations as to the causes of the theft or loss, and what specific actions have you taken?

Ms. THOMAS. The determination of what, how the hard drive went missing, was stolen, is an investigatory responsibility of the Inspector General. So we are waiting for the investigation to be complete. We have, however, determined that there were certainly internal control weaknesses that allowed whatever happened to happen, and we have made substantial changes in the way the controls of the equipment—who can have access to it—and we are ready to take disciplinary action against those people who were not following existing policy. But we are waiting for the end of the investigation.

Mr. CLAY. You could take action now in your agency?

Ms. THOMAS. We have been requested not to by the Inspector General. Yes, but we could take action now, were it not for that standing request.

Mr. CLAY. Mr. Brachfeld, is it complete?

Mr. BRACHFELD. The investigation—your question is, is your investigation complete? No. We are actively investigating it. We have new information which I cannot discuss publicly at this open hearing, but we do have progress in our investigation. And as the nature of the investigation is extremely sensitive, the acting Archivist is correct. We respectfully requested that they hold off, because we don't want to do anything at this point that could damage our investigation.

So in that case, that is correct. We have respectfully requested that disciplinary action be held back pending the furtherance of our investigation or in support of our investigation.

Mr. CLAY. Thank you for that response.

Mr. Powner, can you estimate the cost of integrating increments one and two down the line? I mean, you stated that it was a project at $550 million?

Mr. POWNER. Right, $550 million life cycle cost. We have spent about half of that to date. We do not have clear integration costs going forward.

Here is the problem, not only with the integration costs going forward, but when you look at the outyear increments, 3, 4 and 5, how are we going to allocate the remaining money? There is a serious question with the remaining money to be spent, including those integration costs, whether we are going to get a full operational capability by 2012.

If you look at the track record to date, I think the answer is likely no. And so what we want to see is real clear plans for the next three increments and exactly what's going to be delivered so we can measure to that.

This is similar in cost, Mr. Chairman—we were here a year ago talking about FTCA. That was a $500 million contract at one time, a system at one time that doubled quickly. We want to avoid a situation like that.

Mr. CLAY. Has there been a—I guess we will call it a cavalier attitude with taxpayers' money in this instance?

Mr. POWNER. I wouldn't say that. But I would say that the management discipline that we would like to see from the government is clearly not where we want it to be. And I will give you an example where we look at these contractor reports and we see contractor reports where they're spending money, receiving funds, but not getting the work done. There's a program management technique that is OMB-endorsed, called earned value management. We look at those reports and scrub them.

And what we need here is we need the program office to pay close attention to those reports so that we are overseeing the contractor and the government is in charge, not the contractor.

Mr. CLAY. Would you supply this committee with a summary report of the spending to this date and what problems you see are on the horizon as far as the spending is concerned with this program?

Mr. POWNER. Yes, we can do that, Mr. Chairman.

Mr. CLAY. Thank you so much. And I notice that you may have wanted to get in on the discussion earlier on whether there are industry standards that NARA could use that would have helped this situation. Did you have a comment?

Mr. POWNER. Well, the one comment on the multiple classifications, GAO has done a lot of work on sensitive but unclassified data. This is dated; but 2 to 3 years ago, there were over 70 classifications of sensitive but unclassified data. And I think the quick answer to the Congressman's question is consolidating those many classifications is a clear work in progress and it's incomplete.

Mr. CLAY. Thank you for that response.

Mr. Brill, any comment on industry standards?

Mr. BRILL. I think if there is anything to be said about industry standards, there's recognition that the more complex you make any program, the more likely you are to have problems. If you can keep things simple, if you can classify things in a limited number of buckets, and you have some clear rules about what to do in each case, then it is much more likely that you're going to have a very high degree of success in that program.

We see all the time—you know, my work is kind of divided in two, sir. In some cases, we are brought in, in advance, to try and avoid problems. But in a lot of cases, we're the firemen. We're the guys who get the call when something terrible happens, and I think it would be fair to tell you that when that happens, we can end up, in most cases, classifying the incident into one of two major buckets. One is "It happened." The other is, "It happened, but it shouldn't have happened." It was an avoidable problem that, if rules had been followed—if, for example, something as simple as a patch from a vendor had been applied to a computer, wouldn't have happened. If a firewall was properly configured, wouldn't have happened.

If we can manage those, if we can avoid the avoidable incidents by simplification, by good management, by good followup, by good audits, that is key.

There will always be incidents. Human beings will always make mistakes. Machines are not infallible. So, rather than sometimes

throwing up our hands and saying things happen, let's classify it simply. Let's stop the things that we can reasonably prevent through what I consider a commercially reasonable set of controls, have plans in place for what we are going to do if something happens in spite of our best efforts, and recognize, as everybody has said here, that the environment changes.

The first computer that I used at the Pentagon back in 1968 had 2,000 positions of memory, 2K. The systems in my office now are measured not in kilobytes but in petabytes. And one petabyte is 1 million gigabytes. The vast amounts of data mean that we have to treat it in a systematic fashion. Those who figure out how to do that, how to build the security into the network, build it into the systems, tend to have fewer mistakes. And the mistakes that occur don't fall into that tragic category of "We could have prevented this."

Mr. CLAY. Thank you so much. The gentlewoman from California is recognized for 5 minutes, Ms. Watson.

Ms. WATSON. Thank you so much, Mr. Chairman. And I came in late and probably a lot of this has been already discussed.

But what would each one of you recommend after the investigation into the breaches, into the delays and so on, what would you recommend as we move forward? Because this valuable information that is stored in the Archives, if there are breaches or if the machinery in some way collapses, what kind of backup systems do we need to have? What do we need to build into our base equipment so, as you said, Mr. Brill, these things should not have happened? Can any of you look forward and tell us what you would like to see?

Mr. BRACHFELD. I guess I'll tackle it. It's my nature; what can I do.

There are two different issues here in terms of the breaches and the events that transpired. I think that if you look at NARA today, we have policies and procedures that are defined because they have been derived from NIST and OMB. So we have that piece of the equation.

The question, as we move forward now, is ensuring through training and oversight that there's compliance with those requirements and, as appropriate, punishment. Because those regulations which are on our books, which are in our requirements, say that if people violate the security provisions, appropriate administrative and potentially criminal action and criminal charges——

Ms. WATSON. Who should do the oversight?

Mr. BRACHFELD. I'm not a program official. I do audits investigations. The agency is in charge with oversight of programs, ensuring that their programs are implemented and successful. So the agency needs to do that piece of the puzzle. I'm there to provide whatever guidance and support I can in that regard. And should somebody or an entity fail to live up to their requirements, I'm there to do investigations. And if it turns criminal, I'm there to do the criminal investigations—and my staff.

Ms. WATSON. Who determines there should be an investigation? Whose responsibility would that be?

Mr. BRACHFELD. That's my decision. If I'm alerted to—it happens all the time. We get hotline calls. We get people coming to us. We

get formal referrals. Once my office becomes aware of an event or events, we make a decision. My Assistant Inspector General for audits and Assistant Inspector General for investigations, we work the issue. We make determinations.

If we believe it's a potential for criminal, we work through the Department of Justice, as we are required by law to do. If we believe it's administrative, we take a different track. Or if we believe that nothing inappropriate happened and it's not my responsibility in that regard, we may just do a referral. But it weighs on my shoulders and we address that.

Ms. WATSON. Mr. Brill, you were mentioning that we should have standards. What should we do in order to avoid these kinds of, well, breaches? I don't know what you would do. But what would you suggest?

Mr. BRILL. It's as good a word as any, I suspect. You know, it's an interesting thing. I have been sitting here thinking about something and it's this. Back in about 1975, I was an Army Reserve officer. I served Active and Reserve for 38 years. And I was assigned to the Office of the Secretary of Defense as a mobilization designee. And we started looking, even back then, at information security.

And I remember a meeting that I had with the then-Deputy Assistant Secretary of Defense for Audits, and I had just successfully compromised a data center that I had been requested to test out.

And what I said to him was this. How can you, how can you go before Congress and have to say that the standards that you're using maybe would not be acceptable in a major corporation? I work with corporations primarily, not governments. But what I found is there is an evolution. The standards that have come out, the internal controls, as the Inspector General has said, following things like Sarbanes-Oxley, following the changes in governance, in the corporate world, have changed things.

The changes that occurred in 2006 when the Federal Rules of Civil Procedure were modified as a result of the work of the Sedona Conference to recognize the importance of digital records in the civil litigation process—there's been a sea change. People are realizing that the key to this is good management. It's no different than it was 100 years ago.

When we had paper records, we could preserve them, but that didn't mean they were going to be readable unless we preserved them properly and we protected them properly.

Digital records are no different. The techniques vary, but the principles are the same. And isn't it always the same, ma'am, that responsibility has to be taken, somebody has to be the person that you can to talk to about it, and that there are standards, whether we use the ISO standards, whether we use the good work that's been done at NIST, whether we use the standards of other organizations?

I don't really care what standards there are, but if we have a standard and we all agree to it, then an agency knows what to do. You know what you can ask them. The auditors know that it's a fair game, that you're testing on the basis of rules.

So I think what I'm seeing is that, just as corporations have recognized that the way that they handled automated records in the past is no longer acceptable, if you did what you did a few years

ago you're likely to find a judge holding that you've committed spoliation, and that there could be penalties for that.

Just as I said to the guy at the Defense Department years ago, I think that if we are lucky as citizens, there's a two-way street between the private sector and the public sector in terms of exchanging knowledge, research that's done, best practices. And to the extent that can be done, I think there's great value to be had.

Let's see what some of the best-run companies are doing. Let's see why the standards are changing. Let's see what's being done. I think the real key in getting that information is perhaps the simplest thing that anyone can do. And I can express it in one word: Ask.

Ms. WATSON. Thank you, Mr. Chairman. I yield back.

Mr. CLAY. Thank you, Ms. Watson.

Just as a final question, Ms. Thomas, at a hearing last month, we heard about your advisory committee on the electronic records archives. NARA believes that the advisory committee has been valuable in providing outside expert advice in the development of ERA. Its members represent expertise in an extremely wide range of areas. However, as far as we can tell, the committee does not include one expert or even anyone with direct experience in the area of information technology security.

Why isn't this important field represented on your advisory committee?

Ms. THOMAS. I don't know whether there is any specific person whose profession is information security. I think all of the members who have responsibility for systems certainly have responsibility for information security, security over those systems and therefore come to the committee with a wealth of experience in how they deal with their own systems.

Mr. CLAY. Well, do they bring a knowledge of information security like, for instance, your fellow panelist, Mr. Brill?

Ms. THOMAS. I think Mr. Brill is unique.

Mr. CLAY. I do too. But there has to be, just to have someone——

Mr. MCHENRY. I think that is a compliment, Mr. Brill.

Ms. THOMAS. It is. It is.

Mr. CLAY. To have someone else represent that aspect of information technology would be probably helpful to the advisory committee.

Ms. THOMAS. I think you're probably right, Mr. Chairman, and we can certainly look at the membership and if we are deficient in that, having that kind of person—maybe Mr. Brill would even like to join ECERA.

Mr. CLAY. We will let you and Mr. Brill discuss that. If there are no other questions, the hearing is adjourned. Thank you.

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