TESTIMONY OF ADRIENNE THOMAS

ACTING ARCHIVIST OF THE UNITED STATES

BEFORE THE SUBCOMMITTEE ON

INFORMATION POLICY, CENSUS AND NATIONAL ARCHIVES

OF THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

ON

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

NOVEMBER 5, 2009

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 document instances of accessing data in a PII system, as required by the Privacy Act, 5 U.S.C. § 552a(c)(2).
- 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.