**Testimony of Adrienne Thomas**
**Acting Archivist of the United States**
**Before the**
**House Committee on Oversight and Government Reform,**
**Subcommittee on Information Policy, Census, and the National Archives**
**July 30, 2009**

## Introduction

Chairman Clay, Ranking Member McHenry and members of the Subcommittee, I am Adrienne Thomas, Acting Archivist of the United States and I appreciate being given this opportunity to appear before you to discuss a recent security incident which is a serious breach of the trust placed in the National Archives to protect our nation's records. As you know Mr. Chairman, we have kept your staff apprised of this issue, and we were very pleased that a group of staff were able to come to our College Park facility two weeks ago to get a first-hand briefing and tour of the location of this incident.

The National Archives and Records Administration (NARA) learned in late March 2009 that an external computer hard drive containing copies of Clinton Administration Executive Office of the President (EOP) Presidential and Federal records was missing from a NARA electronic records processing room. The Office of the Inspector General continues to investigate who was responsible for the disappearance of the hard drive. As the Acting Archivist, but also as someone who has devoted my entire 39 year career to the National Archives, I am deeply angered that a NARA employee or contractor may have intentionally removed this item, and I am disappointed that our procedures as implemented were not sufficient to forestall this incident.

In the testimony below, I will describe the circumstances and events surrounding the loss of a hard drive for which we were responsible and I will describe the steps we have taken to ensure that such a loss does not occur again. Since this hard drive contained personally identifiable information (PII), with me today is NARA's General Counsel and Senior Agency Official for Privacy, Gary M. Stern, who can respond to any questions you have about our efforts to inform individuals about the potential compromise of their personal information. In the event that you have specific questions which I cannot answer in regard to the operations and security of the NARA work area where this incident occurred, seated behind me is Sharon Thibodeau, Deputy Assistant Archivist for Records Services, who is prepared to provide these details.

The role of the National Archives and Records Administration is to serve as the nation's record keeper and to make those records as broadly accessible as possible, while balancing such access with the need to protect national security, personal privacy, and other sensitive information. We accession approximately 3 percent of all federal records—those deemed most important, with the greatest long-term value – and all Presidential records.

These records remain important long after they are no longer needed for the original purpose they were created. Americans come to our facilities all around the country to examine them—to trace their family roots, to verify Federal military or civilian service, to prepare for legal proceedings, to hold the agencies and their officials accountable for carrying out their role in serving the American people, and to enable historians to write another chapter of the history of our country.

Over the past 75 years, most of those records have come to us on paper. Today, these records total almost 9 billion pieces of paper archived in our facilities nationwide. They include acts of Congress, documents of individual departments and agencies, papers of Presidents, material from cases decided by the federal courts, and the personnel records of 56 million veterans of our armed forces. Besides text documents, we also have maps of land and sea, 14 million photographs of all kinds, and large audio and visual holdings.

Although our first accession of electronic records dates to 1969, the volume and complexity of electronic records has increased dramatically. Over the past decade, we have been getting new kinds of records from all across the Federal government: electronic text documents, e-mails, snapshots of web pages, digital images, spreadsheets, presentations, audio and video data files, databases, satellite imagery, geographic information systems, and more. The future will bring records created on Personal Digital Assistants and Internet features such as Blogs and Facebook pages of Federal agencies.

These new kinds of records present new challenges for us. They are coming to us on an increasing variety of hardware and storage devices—often physically smaller and more complex but able to hold more information. For example, in its first year of operation 75 years ago, the National Archives took in the equivalent of 8 million documents—58,794 cubic feet of records. Today, those 8 million documents would fit on a single portable electronic storage device. The concentration of so much data on a piece of equipment the size of a novel presents significant challenges that the original archivists in 1934 could not imagine. We must be even more vigilant in ensuring that our security protection measures are in place and being implemented by today's Archives staff.

Meeting these challenges is of paramount concern to the National Archives, but they are challenges we must take on with vigor because of the ever expanding opportunities to provide the American people – regardless of where they live – with access to the records that document our democracy, our rights and the story of our nation. But as with any endeavor that relies on the work of human beings, we will, despite our best efforts and best intentions, occasionally make mistakes along the way. While only a small portion of our holdings are truly sensitive, any error in our management of these sensitive records is unacceptable and we will learn from our mistakes to become better at what we do by encouraging an environment of continuous improvement.

Now I will describe a loss of data from which we must learn much, so that it does not happen again.

**Background**

The loss of the hard drive occurred while NARA was conducting preservation processing of electronic media that we had received from the Executive Office of the President (EOP) at the end of the Clinton Administration. In accordance with the Presidential Records Act, the EOP transferred the official electronic records of the Clinton Administration in 2001. While most records transferred from the EOP are received and processed by the staffs of the Presidential Libraries, records in electronic form have, since the Reagan Administration through the Clinton Administration, been transferred for preservation to NARA's Electronic and Special Media Records Services Division, which is located organizationally within the Office of Records Services in our facility in College Park, MD.

In addition to official electronic records from the Clinton Administration, NARA also received from the EOP over 60,000 electronic storage items consisting of backup tapes and work media, additional copies of files restored from the backup tapes, snapshots of employee working drives on various 4mm and 8mm tape formats, and actual hard drives from the Clinton EOP. The material from the EOP included units that fell under the requirements of either the Federal Records Act (FRA) or the Presidential Records Act (PRA) and included both classified and unclassified materials.

As part of NARA's responsibility to ensure that electronic materials are preserved until such time as their final disposition is determined, NARA identified a subset of approximately 2,500 tapes and four hard drives from the Clinton EOP, known as "reallocation tapes," for re-copying. Such re-copying is consistent with our regulatory requirement that electronic tape media at least 10 years old should be copied to new media to prevent deterioration. Essentially the reallocation tapes contained "snapshots" of the contents of the working drives of departing EOP employees, which were originally created and preserved to fulfill the requirements of pending litigation.

These tapes consisted of a wide variety of 4mm, 8mm, and QIC (quarter inch cartridge) tape formats, and most of the tapes could not be read by NARA tape drives. Therefore, NARA sought vendors that could read the tapes and copy them onto formats compatible with NARA's electronic records preservation systems starting in Fiscal Year 2005. Over the course of four years NARA had three different companies under four separate contracts conduct preservation copying on a portion of this media. In July 2005, NARA contracted with Arkival Technology Corp. Arkival Corp copied 437 tapes onto digital linear tape (DLT) media. In April 2006, Arkival Corp copied another seven tapes and four hard drives onto DLT media. Later in Fiscal Year 2006, Muller Media Conversions copied 277 tapes onto DLT media. In Fiscal Year 2007, Arkival copied 300 tapes onto two one-terabyte My Book hard drives, which, as the name implies, are about the physical size of a paperback book. Arkival subsequently made an additional set of back up copies of the hard drives for a total of four hard drives.

In Fiscal Year 2008, NARA contracted with RICOMM Systems, Inc, to copy 1,428 tapes. RICOMM to date has copied 881 tapes onto eight two-terabyte My Book hard drives. As

with the Arkival contract, RICOMM also made a backup copy of each of the 2 terabyte hard drives for a total of sixteen My Book hard drives. Two of these RICOMM-created My Book hard drives were delivered to NARA on September 18, 2008. They were labeled "Master #2" and "Backup #2." Records show that each of these drives contained copies of data from 113 of the Clinton Administration "reallocation tapes" designated for preservation copying. The missing hard drive about which we are testifying today is the hard drive that was labeled "Backup #2."

**Incident**

On the day of their delivery to NARA, the RICOMM-created hard drives Master #2 and Backup #2 were taken to a work station within suite 5300 of the NARA facility in College Park, MD. An Information Technology Specialist, GS-13, Team Leader verified the paperwork received from the contractor and confirmed that we received the correct hard drives.

Suite 5300, which Oversight Committee staff visited two weeks ago, contains offices, work cubicles arranged in an open configuration, and separate, enclosed unclassified, classified, and Census electronic records processing rooms. There are three doors opening into the suite, two front doors and a back door, each of which is controlled by an electronic card key system. All of the controlled doors to suite 5300 are within NARA's general perimeter security system. At the time of receipt of Master #2 and Backup #2, approximately 85 individuals (NARA employees and contractors) had badges that activated the card key system controlling the doors to suite 5300. Although separately enclosed, the unclassified electronic records processing room had no additional security. Individuals with badge access to suite 5300 also had access to the electronic records processing room. In fact, one of the three doors into the suite, the back door, opens directly into the electronic records processing area

At the time of receipt of Master #2 and Backup #2, the back door to suite 5300, the one opening directly into the unclassified electronic records processing room, was sometimes held open to allow for better ventilation in that room. This occured because the large number of electronic devices operating in the room could elevate its temperature to problematic levels. Staff members were instructed never to open the door for ventilation purposes unless an authorized staff member was always present in the area. I will describe the security enhancements that have been made since the loss of the hard drive later in this testimony.

On September 23, after NARA staff verified receipt of the drives, they were placed in the unclassified electronic records processing room in Suite 5300 where staff would then verify that the contractor had completed the work. The IT Specialist Team Leader created a map of the Master #2 hard drive that describes the directory structure of the disk. The hard drives were placed on a shelf in the unclassified electronic records processing room of Suite 5300, and on October 30, 2008, the work of processing the records on the hard drive was assigned to a GS-11 Information Technology Specialist. The IT Specialist was instructed to compare the actual file structure of the disk to the map

that the IT Specialist Team Leader had produced, print out the first five pages of each file on the disk, and compile the printouts in folders without examining the contents of the printouts. Work was performed only on the Master #2, not the Backup #2 (which would later be missing from the processing room).

Normally electronic media in the custody of NARA are housed in storage areas called stacks which have limited access. Standard operating procedures call for staff members to check out media from the storage area, process the records in the appropriate electronic records processing room and return the records to the storage area at the end of the day. In addition, when the contents of the media are determined to have sensitivities, such as personally identifiable information, NARA stores the records in areas with an additional level of security. In the case of the missing hard drive, the hard drives were not returned to the storage area at the end of the day. The staff member performing the preservation copying of the hard drive had no knowledge of the contents of the media and thus did not know that it contained personally identifiable information. That was only determined later when the hard drive disappeared and the content of Master #2 was examined. Nevertheless, the hard drive had characteristics that made it vulnerable to theft, such as a high storage capacity (two terabytes) and portability. When not being processed, both hard drives should have been placed in a storage area with an additional level of security.

Work on Master #2 stopped on January 30, 2009. Because of the voluminous amount of paper generated as a result of printing out the first five pages of each file, the IT Specialist Team Leader halted the project in order to investigate an automated way to validate the hard drive directory structure. On February 5, 2009, the IT Specialist working on the project placed the Master #2 into its box located near the work station. The IT Specialist noted that Backup #2 was also securely housed in a box adjacent to Master #2.[1] The two boxes which should have contained the two hard drives remained on a shelf located above the electronic records processing work station in the unclassified electronic records processing room until March 24, 2009. During this time period, no one reported opening the boxes and viewing their contents.

We should also note at this time that NARA backs up its electronic records processing system data onto high density, portable hard drives. One brand NARA uses is the one-terabyte version of the Western Digital My Book line of hard drives, which is similar in appearance to the two-terabyte version that is missing. Because the hard drives had no distinctive marking as containing record materials, staff members not familiar with the EOP preservation project might erroneously have thought that the hard drives containing the EOP material were media used for system backups, and therefore assumed that they were properly stored in the processing room. We do not offer this as an excuse for the improper handling of the hard drive, but simply as an explanation for why it may have taken a long period of time before staff discovered the hard drive missing. It also demonstrates a potential challenge in our inventory procedures that we must consider as we move forward from this incident.

[1] The Office of the Inspector General has informed us that when they interviewed the staff member, the staff member could not be 100% certain that Backup #2 was in the box on February 5.

With the new software procured and tested, on March 24, 2009, the IT Specialist originally assigned to work on Master #2 and Backup #2 returned to work on these media and discovered that the box that had contained the hard drive labeled as Backup #2 was empty. The adjacent box was found to contain the hard drive labeled Master #2. The IT Specialist informed the IT Specialist Team Leader and the IT Specialist Team Leader informed the Supervisor that a loss had occurred. The IT Specialist Team Leader and Supervisor immediately began a search for the missing hard drive, Backup #2. They checked all of the workstations and rooms within Suite 5300 and the stack area normally used to house electronic media. They also checked other work spaces occupied by the division. They did not find hard drive Backup #2.

On March 27, 2009, they informed the Director of the Electronic and Special Media Records Services Division (NWME) of the apparent loss. The Director commenced a division-wide search which did not produce results. Staff thoroughly searched the processing rooms and the stack areas where original and back-up media are stored. Staff working in the unclassified processing room was also questioned about their knowledge of the hard drive. On March 31, 2009, the Supervisor submitted a report of the loss to the NWME Division Director. On April 1, 2009, the Division Director informed NARA security and other staff members within the Office of Records Services, Washington, DC including the Assistant Archivist who manages the Office. On April 2, 2009, I, NARA's Inspector General, and NARA's General Counsel were informed of the loss.

**Response and Investigation**

While NARA employees searched for hard drive Backup #2, staff also began to review hard drive Master #2 in order to determine whether it (and its missing counterpart, Backup #2) contained any sensitive information, such as personally identifiable information. After performing a number of key word searches of hard drive Master #2, NARA discovered that there were numerous files containing personal names and social security numbers. The hard drive contained the contents of the working drives of EOP staff members and, as such, represented a snapshot of the administrative work conducted by the staff of the EOP. The administrative work included managing personnel actions, payroll, White House visits, and other administrative matters. In addition, NARA also found a small number of files that contain markings indicating that they may contain information that was classified at the time of creation. While transfer information from the EOP indicated that the hard drives did not contain classified data, we believe the presence of what may be classified information occurred when EOP employees accidentally or improperly stored classified information on their unclassified computers. The OIG has the lead responsibility for facilitating the declassification review process to determine if any of these files contain information that should remain classified.

In accordance with OMB requirements, NARA immediately reported the missing hard drive Backup #2 to the U.S. Computer Emergency Readiness Team of the Department of Homeland Security as a potential breach of personally identifiable information. NARA also notified staff of our House and Senate Oversight Committees, the White House Counsel's Office, and the representative of former President Clinton. In addition, NARA

convened our Breach Response Team in order to determine how to respond to the breach of the PII.

The Office of Inspector General immediately commenced an investigation to determine who was responsible for removing the hard drive, which remains ongoing. We have been advised by the OIG that there are currently no facts to determine whether the drive has been stolen or was misplaced, and no suspect has been identified.

NARA also immediately moved all previously copied hard drives with EOP content and original EOP tapes to classified storage. Further, NARA has offered a reward of up to $50,000 for information that leads to the recovery of hard drive Backup #2.

NARA has made a copy of Master #2 and is currently reviewing the data on it to compile a list of those individuals who may have had their personal information compromised. Through the services of a credit monitoring contractor, NARA has begun to send out letters to these individuals as they are identified. To date, approximately 15,750 letters have been mailed. The letters also have an enclosure that provides individuals with information regarding the breach and ways for those individuals to protect themselves. In addition, NARA is offering each individual one year of free credit monitoring services and fraud protection. Further, NARA has set up a Breach Response Call Center and a Breach Response email box, which are fielding inquiries from individuals requesting additional information. We have also posted information about this matter on our website, at www.archives.gov. Because of the extremely large volume of data on the drive – over 8.7 million individual files – we do not yet know the total number of individuals whose privacy has been affected. Breach notification letters will be sent to individuals as they are identified.

**Changes made as a result of the loss**

NARA has taken several steps to improve internal controls in the following areas: physical security of the electronic records processing workspace and treatment of electronic devices containing personally identifiable information.

First, NARA has completely separated access to the unclassified electronic records processing room from access to suite 5300. The entrance to suite 5300 that had opened directly into the processing room is no longer operational as a suite entrance. This door is being equipped with emergency exit hardware which will sound an alarm if a person opens it for any reason. (The ventilation concerns that had led to instances of opening this door have been addressed by installation of improved air handlers in the room.) Individuals who need access to the unclassified electronic records processing room are limited to entering the room from doors inside suite 5300. These processing room doors now have separate card key access systems and only individuals with badges programmed to open these doors may enter the room. Individuals without badge access to the processing room must be authorized by a NARA manager, sign a log prior to entry, and be escorted while in the room by an individual with badge access.

Second, we conducted an audit of all physical media, for example, magnetic tapes, CDs, hard drives, and similar portable devices containing PII and other sensitive information (including Presidential EOP media). Those devices identified as containing this type of information were moved to a separately secured storage area where only those employees who handle such materials have access. Access to this protected space, which is located within the secure stack storage area housing unclassified electronic records (which your staff also visited two weeks ago), is granted only to employees authorized access to sensitive records, including PII. The employees identify the material being withdrawn and log the movement of the material in and out of the storage area on a separate media log. A supervisor must ensure compliance by reviewing the sign-in logs and inspecting the processing and storage areas on a daily basis.

Finally, all NARA staff is required to take two courses on how to handle sensitive information: Personally Identifiable Information training and Information Assurance Awareness training. In addition, the staff of the Electronic and Special Media Records Services Division was trained on the new procedures described above and sensitized to returning records to proper storage areas when not in use.

**Conclusion**

As the Subcommittee knows, the investigation of this incident is ongoing under the direction of NARA's Office of Inspector General. Additionally, the United States Secret Service has assisted in providing forensic IT support to NARA's Office of the Inspector General. While I cannot comment on the investigation, I can assure you that the results of that investigation will be taken very seriously by me and swift and appropriate disciplinary actions will be taken if it is determined that any NARA employees were responsible for removing the hard drive or failed to adhere to proper records handling procedures.

NARA is a public trust, and the 3,000 women and men who work at NARA facilities across the country take their jobs, and that public trust, very seriously. In this year, in which NARA celebrates 75 years of service to the nation, I wish I was up here today to testify about all of the vital work we do every day to preserve and protect, while providing public access to, over 9 billion – and growing – pages of records. Given the seriousness with which we take this loss, however, I am thankful to you for giving me the opportunity to testify and I would be happy to answer any questions.