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.