U.S. House of Representatives
Committee on Oversight and Government Reform
Darrell Issa, Ranking Member

An Agency on the Brink: How the Theft of Sensitive Property Exposed a Culture of Complacency at the National Archives

Staff Report
U.S. House of Representatives
111th Congress
Committee on Oversight and Government Reform

April 6, 2010

TABLE OF CONTENTS

EXECUTIVE SUMMARY

After learning in March 2009 that a hard drive containing Clinton-era personally-identifying and national security information was missing from a National Archives facility in College Park, Maryland, Inspector General Paul Brachfeld commenced a criminal investigation. Because of the nature of the contents of the drive, the Office of the Inspector General (OIG) immediately enlisted the Federal Bureau of Investigation and U.S. Secret Service to investigate the apparent theft.[1] Subsequent investigation revealed the missing drive contained the Social Security numbers of Clinton White House personnel, contact information (including addresses) for various Clinton administration officials, Secret Service and White House operating procedures, event logs, social gathering logs, political records and other highly-sensitive information. Many of the affected personnel now work in the Obama White House.

While OIG investigated the apparent theft of the hard drive, the Committee worked to uncover how and why the National Archives and Records Administration (NARA) allowed a potentially catastrophic loss such as this one. Through interviews, briefings, hearings, and a tour of the College Park facility, the Committee learned that a lack of internal controls at NARA created a climate in which a loss of valuable hardware and/or sensitive information was effectively inevitable.

Inspector General (IG) Brachfeld recently filed a final report of criminal investigation. The IG's report concluded that the drive was likely stolen. Any thief was unlikely to have encountered any meaningful obstacles while removing the drive from NARA. The drive was left in its original packaging on a shelf above a workstation accessible to hundreds of badge holders, janitorial staff, public tours, and other NARA staff who used the supposedly secure area as a shortcut to the bathroom.

The IG's investigation focused on the activities of a NARA employee who used the missing drive to evaluate whether its contents were an accurate back-up of original Clinton-era White House tapes. The employee in question failed a polygraph test and failed to disclose travel to Cuba under questioning from the Secret Service.

The IG's report confirmed the Committee's concerns about the climate at NARA. NARA is plagued by employees who fail to recognize sensitive and classified materials, unsecure workspaces, a lack of internal controls, and low employee morale. These conditions combine to create a dangerous environment in which a disgruntled employee could easily steal valuable hardware or sensitive materials to sell on the street, or worse, to a hostile foreign government or terrorist network.

---

[1] H. Oversight and Gov't Reform Comm. Interview of NARA IG Paul Brachfeld, May 19, 2009 [hereinafter Brachfeld Interview].

THE LOSS OF THE CLINTON HARD DRIVE

The Electronic Records and Special Media Records Services Division (NWME) of the National Archives and Records Administration (NARA) operates a processing room in Suite 5300 of an agency facility in College Park, Maryland ("Archives II"). In that processing room, NWME Information Technology Specialist [NAME REDACTED] was using a two-terabyte Western Digital External Hard Drive ("My Book") to quality-check information transferred from original 4-8 mm tapes containing Clinton White House material. A new My Book retails for approximately $229.99.[2]

[NAME REDACTED] was working with two hard drives labeled "Master #2" and "Back-Up #2" (collectively, "the hard drives"). The boxes containing the hard drives were also labeled. The missing hard drive is Back-Up #2. [NAME REDACTED] began working with the hard drives in October 2008. She was tasked with verifying that the contents of Master #2 and Back-Up #2 were identical. The massive amount of information stored on the hard drives required [NAME REDACTED] to work on this project for several months.

Because she was printing out the contents of the hard drives to allow a side-by-side comparison, [NAME REDACTED] was generating a substantial amount of paperwork.[3] In January 2009, she was instructed to stop working on the project until a more efficient process could be developed.[4] When [NAME REDACTED] was not working with the hard drives, she stored them in their original boxes on a workstation shelf in Suite 5300.[5]

On March 24, 2009, [NAME REDACTED] was instructed by her supervisor to resume working on the hard drives.[6] When she pulled the boxes from the workstation shelf where they had been left for weeks, she discovered that Back-Up #2 was not in its box.[7] After searching for the drive, [NAME REDACTED] reported it missing to her supervisor on March 27, 2009.[8] NWME staff initiated another unsuccessful search for Back-Up #2 and on March 31, 2009, OIG was notified.[9]

---

[2] Western Digital website, available at http://store.westerndigital.com/store/wdus/en_US/DisplayCategoryProductListPage/parentCategoryID.13092300/categoryID.13092800 (last visited March 31, 2010).
[3] NARA OIG Memorandum of Interview with [NAME REDACTED], April 7, 2009 [hereinafter [NAME REDACTED] Interview].
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*

NARA OIG immediately commenced an investigation. Information describing Back-Up #2 was entered into the National Crime Information Center.[10] OIG quickly determined that the drive contained personally-identifying information (PII), classified documents, and sensitive U.S. Secret Service (USSS) data.[11] Because of the contents of the hard drive, NARA OIG notified the Federal Bureau of Investigation and USSS in April 2009.[12]

In late May 2009, USSS set up a hotline to receive information on the missing hard drive.[13] NARA announced a $50,000 reward for information leading to its recovery.[14]

NARA authorized sending as many as 175,000 letters to potentially-affected individuals notifying them of the breach and offering free credit monitoring through Experian.[15] The letters were written on National Archives letter head and signed by Adrienne C. Thomas, then-Acting Archivist of the United States.[16] However, the formatting of the letters and envelopes raised questions from some recipients about their authenticity.[17] NARA subsequently re-formatted the envelopes. Approximately 10 percent of recipients signed up for the offered credit monitoring services.[18] There is no evidence that any affected individuals have been victims of identity theft or other crimes associated with misappropriated Social Security numbers.[19]

OIG began conducting NWME staff interviews. [NAME REDACTED] testified that she did not believe there was a policy in place requiring her to return the hard drives to a secure area because they were copies and not originals.[20] [NAME REDACTED] typically logs items in and out of secure storage with pull-slips, but no one told her to use pull-slips for the hard drives.[21] Although [NAME REDACTED] knew the hard drives contained files from the Clinton White House, she did not believe they contained any sensitive or classified information.[22]

---

[10] NARA OIG Report of Investigation at 4.
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] Telephonic Interview of NARA Staff, March 8, 2010.
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] [NAME REDACTED] Interview.
[21] *Id.*
[22] *Id.*

No NWME staff could provide any substantive information about when the hard drives were last seen or went missing from the workstation in Suite 5300.[23] OIG investigators observed that several other My Book hard drives remained in Suite 5300.[24]

Because [NAME REDACTED] was the last person who worked with Back-Up #2, she was interviewed as a suspect.[25] [NAME REDACTED] testified that she did not know where the drive was or who took it.[26] She further testified that she "had nothing to do with this."[27] She said she does not bring hard drives out of NARA.[28] [NAME REDACTED] testified she had a My Book hard drive at home but it was purchased from Wal-Mart.[29]

In September 2009, [NAME REDACTED] submitted to a polygraph test. The test was administered by the U.S. Department of Defense OIG. [NAME REDACTED] answered "No" to each of the following questions: "Did you steal that disk? Did you steal that disk from that work area? Do you know where the disk is now?"[30] The polygraph showed [NAME REDACTED]was being deceptive when answering each of those questions.[31]

In a subsequent interview, [NAME REDACTED] continued to deny criminal involvement in the loss of the hard drive.[32] A consent search was conducted on the personal computer equipment at her residence.[33] The forensic examination revealed that the missing hard drive had not been connected to any of the four computers she presented to OIG investigators.[34] While OIG investigators were at [NAME REDACTED]'s home, her son removed a laptop computer from the residence.[35] The son refused to consent to allow OIG investigators to forensically image his computer.[36]

Additionally, during interviews with the USSS, [NAME REDACTED] initially failed to disclose that she visited Cuba in 2006 in response to questions about international travel.[37] She was unable to recall if she reported travel to Cuba on her recently-completed background clearance form (form SF-86).[38]

---

[23] NARA OIG Report of Investigation at 4.
[24] *Id.* at 5.
[25] DOD OIG Psychophysiological Detection of Deception Examination Summary [hereinafter Polygraph Summary].
[26] NARA OIG Report of Investigation at 5.
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] Polygraph Summary.
[31] *Id.*
[32] *Id.*
[33] NARA OIG Report of Investigation at 5.
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] [NAME REDACTED]Interview.
[38] *Id.*

COMMITTEE ACTION

On May 19, 2009, NARA Inspector General (IG) Paul Brachfeld notified Committee staff that an investigation of the missing hard drive was underway.[39] Mr. Brachfeld informed the Committee that his office was conducting a criminal investigation with the assistance of the Department of Justice and the USSS.[40] At the time, investigators were unable to determine if the loss was the result of theft or negligence.[41] Mr. Brachfeld described the loss of Back-Up #2 as "the greatest loss ever and troubling and amazing."[42]

During the May 19, 2009 briefing, Mr. Brachfeld described a potentially catastrophic lack of internal controls at NARA. According to the IG, even NARA's secure storage spaces for sensitive information are susceptible to breach.[43] Mr. Brachfeld explained that at least 100 "badge-holders" had access to the area where Back-Up #2 was left unsecured. In addition to those individuals who were officially authorized to access sensitive material, Mr. Brachfeld stated that janitors, visitors, interns and others passed through the area workspace in Suite 5300. Even though a badge is required to access the workspace, Mr. Brachfeld explained that the door to Suite 5300 was propped open for ventilation. Because the doors were often open, NARA employees used Suite 5300 as a shortcut to the restroom.

On May 19, 2009, Mr. Brachfeld further described to Committee staff how then-Acting Archivist Adrienne Thomas wrote off the loss of $6 million worth of computer equipment (driver, laptops, etc.).[44] Mr. Brachfeld's characterization of NARA's tendency to ignore security protocols gave rise to concern that the agency was suffering from the absence of a permanent Archivist.

On May 21, 2009, the Subcommittee on Information Policy, Census, and the National Archives held a hearing entitled "Stakeholders' Views on [NARA]." Given the alarming nature of the concerns raised during Mr. Brachfeld's briefing, Acting Archivist Adrienne Thomas was invited to testify at the hearing. Subcommittee Ranking Member Patrick McHenry intended to ask Ms. Thomas important questions about the loss of the hard drive, including what measures were taken in the immediate wake of the loss to determine exactly what was missing and to prevent further losses.[45]

Ms. Thomas declined to appear as a witness. She informed Committee staff that she would be in St. Louis on May 21, 2009 for the dedication of a new NARA facility.

---

[39] Brachfeld Interview.
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] Opening Statement of Ranking Member Patrick McHenry, Subcommittee on Information Policy, Census, and the National Archives Hearing, "Stakeholders' Views on NARA," May 21, 2009 [hereinafter McHenry Opening Statement].

On the morning of May 21, Ms. Thomas was observed attending a speech by President Obama at the National Archives Building in Washington, D.C., less than one mile from the Committee's hearing room.[46]

Ms. Thomas's failure to appear meant that not a single NARA official testified at the May 21, 2009 hearing. Because the NARA Inspector General described an agency in dire need of strong leadership and because Ms. Thomas failed to appear at the Subcommittee's hearing and misled Committee staff as to the reasons why, Ranking Member McHenry called for the President to expedite his decision to name a permanent Archivist of the United States.[47]

On July 17, 2009, Committee staff toured NARA's College Park facility and observed the area from which the drive was removed. NARA staff explained that the drive was being stored in its original packaging, which made the value of the hardware obvious. NARA staff also confirmed that the workspace where the drive was being stored is insecure – accessible to personnel without clearance and typically left with the doors open.

On July 28, 2009, two days before a follow-up hearing on the state of the National Archives, President Obama announced David Ferriero as his choice to permanently replace Ms. Thomas. During the July 30, 2009 Subcommittee hearing entitled "[NARA] Organizational Issues," Ms. Thomas and Mr. Brachfeld testified. In response to questions, Mr. Brachfeld reiterated his concerns about a lack of internal controls at NARA. He was unable to answer specific questions about the investigation because it was ongoing. Ms. Thomas assured Members of the Subcommittee that steps were being taken to prevent additional losses and to correct the culture of complacency at NARA.

During hearings in October, November and December 2009, Members of the Subcommittee continued to demand answers and updates from NARA personnel. Committee staff remained in contact with Mr. Brachfeld and received updates as the investigation developed.

PERSISTENT CONCERNS

Inspector General Brachfeld's Report of Investigation gives rise to serious ongoing concerns about the efficacy of NARA's security protocols. The experiences and observations of staff who toured Archives II on July 17, 2009 confirmed that those concerns are valid. Although the lack of internal controls at NARA pre-dates the tenure

---

[46] Distance calculated using Google Maps, available at http://maps.google.com/maps?f=d&source=s_d&saddr=700+pennsylvania+avenue+nw+washington+dc&daddr=50+Independence+Avenue+Southwest,+Washington,+DC+20515+(Rayburn+House+Office+Building)&hl=en&geocode=FR9zUQIdU7lo-ymzHCC3mre3iTFMQT0TMEU2SA%3BFYVgUQIdfOdo-ylpNdOvgLe3iTHd6N36QbcsdA&mra=ls&sll=38.889764,-77.016113&sspn=0.014547,0.033023&ie=UTF8&ll=38.889722,-77.016982&spn=0.007482,0.016512&z=17 (last visited April 1, 2010).

[47] McHenry Opening Statement

of former Acting Archivist Thomas,[48] the loss of Back-Up #2 during her watch appears to have been a tipping point. The following deficiencies contributed to the loss of Back-Up #2:

Lack of Recognition of Sensitive Material

In the case of Back-Up #2, a lack of recognition of the inherent sensitivity of the contents of the drive contributed to its loss.[49] Because [NAME REDACTED] was unaware that the drive contained sensitive information, she stored it in an unsecure location for months at a time. According to OIG:

> ...[N]o one appeared to know what information the drive contained. As a result, security of the drive had not been a priority, even though it was well-known that it contained information from the Clinton White House.[50]

Additionally, the lack of familiarity of NWME personnel with the drive's contents negatively impacted OIG's ability to conduct a fruitful investigation.[51]

Unsecure Workspace Environment

According to OIG, "there was an inherent lack of internal controls necessary to secure sensitive information in NWME."[52] The OIG's investigation revealed that 85 badge holders had access to the main entrance of the processing room in Suite 5300. An additional 34 badge holders (primarily custodial staff0 had access through a back door. Additionally, the OIG was informed that tour groups of up to 25 people were taken through the workspace in Suite 5300.[53]

The back door was occasionally propped open to facilitate the flow of air-conditioning.[54] The back door opened to an all-access hallway.[55]

Lack of Internal Controls

OIG investigators were told by staff that "it would be very easy to leave the processing room with a 2 terabyte hard drive."[56] Suite 5300 and the processing room are

---

[48] *See, e.g.,* H. Oversight and Gov't Reform Comm. Minority Staff Report, "Sandy Berger's Theft of Classified Documents: Unanswered Questions," Jan. 9, 2007.
[49] NARA OIG Report of Investigation at 5.
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] Brachfeld Interview.
[55] NARA OIG Report of Investigation at 5.
[56] *Id.* at 6.

not connected to an alarm system.[57] Additionally, there is no protocol in place to prevent staff or visitors from bringing briefcases, backpacks, or bags into the processing room.[58]

[NAME REDACTED] testified that she was not aware of any policy requiring her to return the hard drives to a secure storage area.[59] Although she frequently uses "pull-slips" to log items in and out of secured storage, she was not instructed to do so in the case of the hard drives.[60] The hard drives were not marked classified.[61] Because the hard drives were copies and not originals, [NAME REDACTED] assumed that they did not need to be secured.[62]

Staff who participated in the July 17, 2009 tour of Archives II were left with the impression that a motivated criminal would be able to remove sensitive materials from the National Archives with little to no resistance from the security measures in place.

Low Morale

NWME supervisors were aware of and condoned the practice of propping the Suite 5300 door open for ventilation purposes.[63] NWME staff were aware that this was a dangerous practice but did not take it up with supervisors for fear that management would have "gone ballistic" in response to being questioned.[64]

NWME staff confirmed during interviews with OIG investigators that the perceived security problems described above did in fact exist.[65] NWME staff further explained that morale is dangerously low and employees are "kept in the dark" and "pitted" against one another to create an "atmosphere of mistrust."[66]

In 2009, NARA ranked 29th out of 30 large agencies surveyed for employee satisfaction and commitment.[67] The anecdotal evidence gathered by OIG, confirmed by the results of the 2009 survey, raises the alarming prospect of disgruntled employees taking advantage of the lax security atmosphere at NARA facilities to steal valuable hardware. Even more alarming is the possibility that such employees might attempt to steal sensitive and classified materials to sell to foreign governments or terrorist organizations.

---

[57] *Id.*
[58] *Id.*
[59] *Id.* at 3.
[60] *Id.*
[61] [NAME REDACTED] Interview.
[62] *Id.*
[63] NARA OIG Report of Investigation at 3.
[64] *Id.*
[65] *Id.* at 4.
[66] *Id.*
[67] Partnership for Public Service and American University's Institute for the Study of Public Policy Implementation Survey, "The Best Places to Work in the Federal Government in 2009," available at http://data.bestplacestowork.org/bptw/overall/large (last visited April 1, 2010).

VI. CONCLUSION

The apparent theft of Back-Up #2 from Archives II revealed an agency in dire need of vigilant oversight from the Committee. During each hearing of the Subcommittee on Information Policy, Census, and the National Archives, Members should continue to question NARA personnel to determine whether specific measures are being taken to improve security and employee satisfaction.

More importantly, Archivist David Ferriero must make the promulgation and implementation of internal security protocols a top agency priority. He must also address the agency's low morale. The holdings of the National Archives are too valuable and, in many cases, too sensitive to be in the possession of unhappy employees operating without clear and enforceable security controls.

In addition to low morale and a lack of internal controls, NARA suffers from a lack of accountability. Former Acting Archivist Adrienne Thomas's decision to make herself unavailable to answer important questions from Congress at a critical point in the Committee's investigation is emblematic of a culture of complacency at NARA.

About the Committee

The Committee on Oversight and Government Reform is the main investigative committee in the U.S. House of Representatives. It has authority to investigate the subjects within the Committee's legislative jurisdiction as well as "any matter" within the jurisdiction of the other standing House Committees. The Committee's mandate is to investigate and expose waste, fraud and abuse.

Contacting the Committee

For press inquiries or additional information regarding this report:

Frederick R. Hill
Director of Communications
(202) 225-0037

For general inquires or to report waste, fraud or abuse:

Phone: (202) 225-5074
Fax: (202) 225-3974
http://republicans.oversight.house.gov

Committee on Oversight and Government Reform
Ranking Member, Darrell Issa (CA-49)
B350A Rayburn House Office Building
Washington, DC 20515
Phone: (202) 225-5074 • Fax: (202) 225-3974