EXHIBIT 1

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CITIZENS FOR RESPONSIBILITY)
AND ETHICS IN WASHINGTON,)
)
Plaintiff,)
)
v.) Civil Action No: 07-cv-01707
)
EXECUTIVE OFFICE OF THE)
PRESIDENT, et al.,)
)
Defendants.)
)
NATIONAL SECURITY ARCHIVE,)
)
Plaintiff,)
)
v.) Civil Action No: 1:07-cv-01577
(HHK/JMF)
)
EXECUTIVE OFFICE OF THE)
PRESIDENT, et al.,)
)
Defendants.)
)

THIRD DECLARATION OF THERESA PAYTON

I, Theresa Payton, declare as follows:

1. My name is Theresa Payton and I currently hold the position of Chief Information Officer (CIO) in the Office of Administration (OA), Executive Office of the President (EOP). In this capacity, I am responsible for providing strategic and operational leadership within the Office of the Chief Information Officer (OCIO). I have held the position of CIO in OA since May 2006.

2. I submit this Third Declaration in response to the Magistrate Judge John M. Facciola's Memorandum Order and First Report and Recommendation ("First

Report") dated April 24, 2008 and in connection with Defendants' Responses to and Request for Reconsideration of the First Report. The statements contained herein are based on my personal knowledge and upon information made available to me by members of my staff in the performance of my official duties.

3. The Office of the Chief Information Officer (OCIO) provides around-the-clock technological support for all EOP components. OCIO provides both Federal and Presidential components with services such as production support, application development and support, intranet and office automation, email, disaster recovery services, support for continuity of Operations (COOP), Enterprise Architecture, Information Assurance, Federal Records Management, and technology assistance to the White House Office of Records management. As part of this support, OCIO manages the email accounts for the sensitive but unclassified network at the EOP for over 3000 customers. In addition to these responsibilities, we are currently preparing the people, process and technology for the Presidential transition to the next administration.

Responding to the Court's Questions

A. ***Question 1: "How many current EOP employees were employed at any time between March 2003 and October 2005?"***

4. Based on information from OA's Human Resources Division, I understand that there are 583 individuals who presently work at EOP FRA components who also worked in an FRA component sometime between March 2003 and October 2005.

B. ***Question 2: "How many hard drives are in the possession or custody of EOP that were in use between March 2003 and October 2005?"***

5. As part of its core administrative responsibilities, OA delivers workstations, which include hard drives and CPUs, to the components. To my

knowledge, OA has not historically tracked hard drive information regarding assignments to individuals using a workstation within each component. Like security specialists elsewhere, between March 2003 and October 2005, OA did not have an established asset management process, which would have included activities such as tracking hard drive assignments within each EOP component.[1] OA does not know what hard drives these 583 individuals used during that timeframe or if the hard drives are still in existence. Accordingly, OA is unable to directly respond to the court's request for the number of hard drives that were in use between March 2003 and October 2005.

6. However, the closest proxy available to approximate the information requested by the Court is that OA has been able to identify 545 workstations, not hard drives, that may have been in use at the EOP between March 2003 and October 2005. OA used a research process to identify these workstations by which OA has manually reviewed manufacturer dates for workstation models and manually reviewed the network through a query process for older workstation models.[2] The results of this review were then cross-referenced to the EOP workstation serial number and then compared to a vendor report, generating a list of potential workstations that may have been in use at the EOP between March 2003 and October 2005. The limitations of this process should be noted, however. Of the 545 workstations, we are presently aware that 527 are in the possession of components that have technology staff and budget that allow them to move and configure assets to meet their component's mission. Therefore, OCIO would not

[1] Until recently, security specialists did not have access to rigorous standards and policies covering IT asset management. IT Asset management principles merge traditional financial practices with security concerns, such as the tracking and inventory of computer hard drives. *See, e.g.*, ISO/IEC 27002, *Information Technology-Security Techniques-Code of practice for Information Security Management* at Section 7 (*Asset Management*) (2005, amended 2007) (This new international ISO standard for Security Management includes extensive policies and guidelines governing the management of IT assets, ranging from inventory and classification to use, labeling, tracking, and handling).

[2] This query process was explained in the declaration provided on March 21, 2008.

ordinarily know if hard drives had been reconfigured, removed or transferred to another workstation over time.

7. Additionally, the normal maintenance and software upgrades significantly increase the likelihood that OA would need to pursue a rigorous forensics process to provide meaningful information from these 545 workstations. Our preliminary estimate based on initial market research indicates that the cost of performing this process for all 545 workstations would be extremely costly in the aggregate.[3] This estimate does not include additional direct and indirect costs such as OA staff, integration services, oversight, quality assurance, and delivering the output to the court. These financial and staff burdens are extraordinary.

8. For example, if required to undertake some or all of the tasks implicated by the Court's First Report, numerous OCIO employees, including the OCIO leadership team, would be diverted from essential tasks of providing service to the EOP components, including planning for the Presidential transition. In some cases, leadership resources have spent 100 percent of their time dedicated to this inquiry rather than attending to other operational priorities.

C. *Question 3: "[W]hether all back-up tapes created between March 2003 and October 2003 have been preserved – and, to the extent they have not, [] state the specific dates within that period for which no back-up tapes exist."*

9. Upon review of the Court's First Report, OCIO took steps to respond to the inquiry on the number of disaster recovery back-up tapes created between March 1 and September 30, 2003. Given the method in which the back-up system provides information about the tapes, OCIO is not able to determine the specific creation date of

[3] A leading U.S. computer forensics producer suggested that costs would not only include forensic services per unit but also specialized software and services commitments. The producer provides to a wide range of Federal departments and agencies and has published formal pricing on the GSA schedule.

the tape (eg., first use) but can determine a date the tape was "written to" as it was used during this targeted timeframe.

10. According to the disaster recovery back-up tape system, there are 438 disaster recovery back-up tapes that were written to between March 1 and September 30, 2003. The tapes – now totaling approximately 60,000 in number, and growing each month – have been preserved in a controlled-access tape vault since tape recycling stopped on October 1, 2003.

11. Due to the disaster recovery back-up tape process, each of the 438 tapes is likely to contain data written to it on multiple days. The data written to it may also cover multiple days that were present on the EOP network when the backup was made. (For example, a file from 2001 present on a backed up server in the EOP network in 2003, would be found on a 2003 disaster recovery back-up tape). At this juncture, based on our due diligence, and according to the disaster recovery back-up tape system, the earliest date on which data was written on any of the 438 tapes is May 23, 2003; the latest date that data was written was September 29, 2003.

12. Even without determining what specific information may be on those 438 tapes, a full set of disaster recovery backup tapes created in October 2003, for instance, should contain email information present on the EOP network, including Exchange servers, at the time of the backup, whatever their creation date. Such a backup should also include email messages residing in a user's inbox, sent folder, trash box, folders saved in the mailbox, as well as email information in the journals and .pst file stores. The disaster recovery backup system in use by EOP is not designed to capture just that email information created during the 24 hours preceding a backup, or since the last full set of

backup tapes were created, but should capture emails sent or received in March 2003, for example, still residing on the EOP network in October 2003.

13. The burden associated with providing the court more detailed information regarding the content on the 438 tapes is extraordinary. This burden includes financial resources to fund additional equipment, make copies of the tapes, procure software, deliver integration services, and support staff. Significant senior management oversight will be needed to procure qualified resources to perform the work, retain the integrity of the tapes, manage the overall process and report back findings to the court upon completion. The burden also requires OA personnel that would need to be diverted from core mission and Presidential transition planning activities.

14. Finally, the Court's proposals in the First Report would divert OA from its comprehensive, measured, process-driven, and cost-effective approach to address Federal Records Act compliance within the EOP for FRA components.[4] We expect OA's approach to be more accurate, and if any restoral process is ever required, the information gained from the approach will identify and focus the efforts on a targeted universe of tapes for restoral. We believe this approach balances the extraordinary financial and human resource burdens with a comprehensive plan to address these matters.

I declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, the foregoing to be true and correct.

[4] For details regarding OA's approach, please refer to the written testimony provided to the House Committee on Oversight and Government Reform February 26, 2008. A copy of this written testimony is attached.

Executed the 5 day of May, 2008

Theresa M Payton

THERESA PAYTON
Chief Information Officer
Office of Administration, Executive Office
of the President

Testimony of Theresa Payton

Chief Information Office, Office of Administration

Before the

House Committee on Oversight and Government Reform

February 26, 2008

Good morning Chairman Waxman, Ranking Member Davis, and members of the Committee on Oversight and Government Reform. I am Theresa Payton and I am the current Chief Information Officer (CIO) in the Office of Administration (OA) at the Executive Office of the President (EOP). I have been in this role since May 2006. I am glad to be here today to discuss the status of the White House efforts to preserve emails. I will summarize my remarks and ask that my full statement be included in the record.

Let me begin by saying that the Executive Office of the President is committed to maintaining a thorough and reliable archiving process for Presidential and Federal records. We believe that we have such a process currently in place. Work is underway to improve that process significantly and we fully expect such improvements to be implemented before the end of this Administration. We are also committed to having a robust and reliable system to quickly recover from any disasters that may affect the EOP network. We are confident that our disaster recovery system meets industry standards and has been responsibly managed. Before I discuss the EOP archiving process and disaster recovery system and address what I believe are the Committee's concerns regarding these activities, I would like to provide some background on my office and on the EOP email systems used by this Administration.

The Office of the Chief Information Officer (OCIO) provides around-the-clock technological support for all EOP components. OCIO provides components with services such as production support, application development and support, intranet and office automation, email, disaster recovery services, support for Continuity of Operations (COOP), Enterprise Architecture, Information Assurance, Federal Records Management, and technology assistance to the White House Office of Records Management. As part of this support, OCIO manages the email accounts for the sensitive but unclassified network at the EOP for over 3000 customers.

I have had numerous conversations with my staff and have reviewed OCIO documents pre-dating my arrival in May 2006. The portions of my written testimony relating to matters occurring before my arrival derive principally from those sources. It appears that the current Administration used Lotus Notes as its email platform at the beginning of the first term. By 2002, the decision was made to replace Lotus Notes with Microsoft Exchange. The transition from Notes mail to Exchange mail occurred over a two year period from 2002 through 2004.

From the start of the current Administration, the EOP has had a process for archiving email sent from or received by the EOP network. This archiving process has evolved over time as new technologies emerged and industry practices evolved. When Lotus Notes was the email platform, the archiving process relied on the ARMS system. ARMS was launched in 1994. At a general level, if a customer received email from outside of the EOP network (a non-EOP account), ARMS would archive the email during a scan of the customer's email account. If a customer sent or received email inside the EOP network using Lotus Notes, a copy of the email was sent to ARMS for archiving.

During the transition from Notes email to Exchange mail, the OCIO attempted to create a system to allow ARMS to serve the same archiving function for Exchange as it had for Lotus

Notes. This project, called EIS, was eventually abandoned due to various technical and system performance reasons. ARMS was a custom-designed application, and I understand that it was discovered that it just could not be effectively integrated with Microsoft Exchange—despite the best efforts of OCIO.

In place of ARMS, the OCIO developed an archiving process that used the journaling function inherent in Microsoft Exchange. Under that process, and in very general terms, whenever email is sent or received by an EOP Exchange customer, a copy of that email is automatically created and stored on a journal to which customers should not have access. Journaled emails are then archived on a separate server in what is referred to as a Personal Storage Table or "PST" file. This process today separates archived email by respective EOP component to facilitate preservation under the Federal Records Act or the Presidential Records Act.

We are aware that the Committee has expressed concerns about allegations that EOP emails were not properly archived between 2003 and 2005. I am aware of a chart created by OCIO staff in late 2005 to early 2006 that identifies dates and EOP components for which email counts were thought to be low or non-existent during the 2003-2005 time period. Since that time, the OCIO staff came to have reservations about the tool used to collect the data in the chart. OCIO thus hired a contractor to perform a comprehensive re-inventory of existing archived messages by component and date. This re-inventory effort is nearly complete. OCIO has also begun an analysis of potential anomalies. Once both the re-inventory and analysis are complete, we will have a separate team do a quality assurance review to confirm the accuracy of the results. This process of re-inventory, analysis, and quality assurance is complex, labor intensive, and time-consuming. At this stage, OCIO does not know if any emails were not properly preserved in the archiving process. Once we complete our review, we will share the results with NARA. If there are any anomalies that cannot be resolved, we will work with NARA to discuss the details of a recovery effort and may seek additional help to ensure that the requirements of both the Presidential Records Act and the Federal Records Act are met during the transition of this Administration.

The EOP has continued to seek ways to improve the archiving process through new technology and updated procedures. For example, beginning in 2005, the OCIO undertook an internal review of record keeping procedures. OCIO made changes to and documented additional standard operating procedures as our internal review revealed areas where we could improve both the accuracy and performance of our archiving process.

After the transition to Microsoft Exchange, the EOP also considered implementing a hardware and software system called ECRMS (Electronic Communications Records Management System) in order to improve and expand the existing message archiving process already in place. However, in late 2006, after consulting staff in OCIO, I determined that ECRMS required additional investments and modifications if it was to fulfill the EOP's requirements for records management and archiving. While testing the process of loading email records into the ECRMS system, the team also found performance issues. For several reasons, including the need for additional modifications, the identified performance issues, and projected costs, the deployment of ECRMS was cancelled. Some of the hardware, software, and technical expertise gathered during the project were then used by OCIO for other projects.

The EOP is currently in the process of deploying Documentum™ and its platform extensions for records management, a DoD-approved system that meets NARA guidelines and will meet the EOP's requirements for records management and archiving. The Documentum™

system is widely used in the Federal Government and we expect will be less costly to implement than other systems considered, including ECRMS. We conducted a technology pilot in late 2007 to confirm that the technology will meet EOP requirements and we believe that the deployment of the Documentum™ system will meet the EOP's records management and archiving needs for the foreseeable future and will address many, if not all, of the alleged concerns raised about the current archiving process.

In addition to the archiving process to preserve emails, the EOP has had a disaster recovery system in place since the start of the Administration to backup our network for protection in the event of a catastrophe or system failure. The EOP Network has been and continues to be regularly backed up onto disaster recovery backup tapes as part of the EOP's disaster recovery system.

From April 2001 to October 2003, in accordance with industry standards and best practices, OCIO used a "Grandfather-Father-Son" approach to backups where three generations of full disaster recovery tapes were kept offsite. Under this approach, whenever a new generation of backups was created, the oldest set of tapes was available to be recycled.

We understand concerns have been raised that the recycling of backup tapes from 2001 to 2003 may have resulted in the loss of EOP emails. Let me be clear: whether or not disaster recovery tapes were recycled would not affect whether emails were preserved by the archiving process. The archiving process and disaster recovery system are separate functions with different purposes. The disaster recovery system is not the system designed to preserve and archive email communications. The disaster recovery tapes would, however, contain email information on the EOP system at the time of a backup, in addition to a backup copy of the email archives, as well as much other information. Therefore, in the event that an email was not preserved by the archiving process, it may, nonetheless, be available on the disaster recovery tapes.

In September or early October 2003, OA ceased its practice of recycling disaster recovery tapes. OA continues to preserve its disaster recovery tapes to the present day. Since October of 2003, the OCIO has stored its backup tapes in a secured vault that meets the storage guidelines provided by the tape manufacturer and NARA. Of course, the EOP also continues to preserve emails through its normal archiving process, as it has since the start of the Administration.

In closing, I would like to reiterate that the OCIO is committed to maintaining a thorough and reliable archiving process for Presidential and Federal email records. We fully intend to complete our analysis of the archiving process, address any and all identified anomalies, and deploy the Documentum™ system as the EOP's email archiving and records-keeping solution for the foreseeable future. We look forward to continuing our partnership with NARA to ensure the EOP's Presidential and Federal email records are properly preserved throughout this and any future Administration and transitioned to NARA as appropriate.

Thank you. I will be glad to answer your questions.