February 21, 2008

By Email

Honorable Henry A. Waxman
Chairman
U.S. House of Representatives
Committee on Oversight and Government Reform
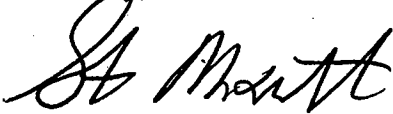2157 Rayburn House Office Building
Washington, D.C. 20515-6143

Dear Mr. Chairman:

I am writing you in response to your request for answers to specific questions relevant to the Committee's investigation relating to whether the Executive Office of the President has complied with federal laws requiring the preservation of preservation and federal records.

I have provided my responses to your questions to Mr. Emmet Flood, Special Counsel to the President and to M. Elizabeth Medaglia, Office of Administration General Counsel. In recent weeks they have expressed to me their concerns about potential disclosures of deliberative discussions involving the participation of Office of the Chief Information Officer management, Office of Administration General Counsel, White House Counsel's Office and White House management. To address these concerns, I have provided my responses to them for their review. They have committed to me that they will review and identify any responses or other specific information that they wish to be redacted from my response prior to submission to the Committee. Any items they choose to redact should be addressed to them.

I realize that there are many complex issues related to this topic. If you or your staff have any additional questions, please feel free to contact me via email at ██████████████████████, or via telephone anytime at ████████. Thank you for your time and attention in this matter.

Sincerely,

Steven McDevitt

General Background

1. During what time period did you work at the White House?

I was employed in the Office of the Chief Information Officer (OCIO) in the Office of Administration (OA) in the Executive Office of the President (EOP) from September 2002 through October 2006.

2. What position or positions did you hold at the White House? To whom did you report?

From September 2002 through July 2003, I was an Information Technology Specialist – Project Manager (GS-2210-14) in the Concepts, Requirements and Systems Engineering Directorate (CR&SE) in the OCIO. During this period I reported to Mr. Layton Clay, the Director of CR&SE.

In July 2003, the OCIO was reorganized and the Architecture and Engineering (A&E) Directorate was created. I was promoted to the position of Director of the A&E as a Supervisor Information Technology Specialist (GS-2210-15).

From July, 2003 through January 2005, I reported to Mr. Carlos Solari, the Chief Information Officer (CIO).

From January 2005 through May 2006, I reported to Mr. John Straub, the Director of the Office of Administration and acting CIO.

From May 2006 through the end of my tenure in the OCIO, I reported to Ms. Theresa Payton.

3. What were your primary job responsibilities? If they changed over time, please describe your responsibilities over time.

As an Information Technology Specialist – Project Manager (GS-2210-14), from September 2002 through July 2003, I was responsible for managing various systems development and systems implementation projects. During this period, the majority of my efforts were focused on the implementation of a new records management system for the White House Office of Records Management. The primary purpose of this system was to manage the paper records and document of the President and his staff.

During this time, I was also assign to begin the process of implementing an electronic records management system to manage the email and other electronic communications records throughout the EOP.

When I was promoted to the new position of Director of A&E my areas of responsibility increased significantly. The primary responsibilities of A&E includes:

- Systems Engineering and Integration – Responsible for the development and implementation of numerous custom developed applications and the implementation of commercial-off-the-shelf (COTS) based solutions.

- Business Applications Support – Provided day-to-day management and support for a wide variety of applications that supported the mission of the components of the EOP. There were approximately sixty-five applications that support the critical business needs of the EOP.

- Website Management and Support – The primary focus of this support was for whitehouse.gov. This included a team of web content management staff, web designers and technology specialists. Support for other websites was also provided. Including omb.gov, results.gov, wmd.gov and other White House related sites.

- Enterprise Architecture – A&E was responsible for the development and maintenance of the Enterprise Architecture (EA) of the EOP.

4. Did you have any staff who reported to you? If so, please describe the size and role of your staff.

As Director of A&E, I had between 8 and 13 staff reporting to me. The staff was a mix of project manager, technical specialists, enterprise architect and web specialists. All were Information Technology Specialists or Supervisory Information Technology Specialists (GS-2210) grades 9 through 15.

5. There were various contractors that worked with staff in the Office of the Chief Information Officer. Which contractors did you work with, and what was their role?

The contractors that supported the mission of A&E included:

- Boeing – Enterprise architecture support for the development and maintenance of the EOP EA.

- Booz Allen Hamilton – Was awarded the contract for the implementation of the White House Office of Records Management, records Management system (RMS). They were also awarded the contract for the initial requirements analysis and solution selection for the Electronic Communications Records Management System (ECRMS)

- Lockheed-Martin – Support the for IntranetQuorum system used by the Office of Correspondence.

- MZM – Provided support for the implementation systems related to the email infrastructure.

- Systems Management and Engineering Inc. – Enterprise architecture support for the development and maintenance of the EOP EA.

- TKC Communications – Provided systems engineering and technical assistance support on a wide variety of systems development and systems implementation projects.

- Unisys – Provided systems analysis and systems implementation support. These were specific tasks under the larger multi-year information technology support contract that provided enterprise-wide services to the EOP. Unisys was tasked with the implementation and integration of the ECRMS system.

E-mail Systems and Archiving

6. The Committee understands that, at some point in 2002, the White House began a migration of e-mail systems, switching from Lotus Notes to a Microsoft Exchange system. Do you know when the decision was made to make this migration? What was the rationale for the change? When did the migration begin and when was it completed?

There were multiple reasons for the desire to migrate from Notes to Exchange.

- Senior White House staff had a desire to migrate to Microsoft Outlook and Exchange because that is what they were used to on the campaign.

- The Outlook platform was widely used in commercial enterprises and provided better integration with the Microsoft Office suite of applications that was the standard within the EOP.

- Also, there were a number of features of Outlook that were not available in the Notes Mail environment.

The project to evaluate the migration to Outlook / Exchange began prior to the beginning of my employment with the EOP in 2002.

The migration for part of the Office of Administration occurred as early as September 2002. The reason I know this for certain is that when I began my employment, I was not provided a Notes Mail account, I was provided an Outlook/Exchange account.

7. Was there any particular order dictating how the migration proceeded? Was the migration done component by component or on a more individual basis?

With about two thousand people to migrate from Notes to Exchange, there was a formal process that was put in place to support the migration. As a general rule, the migration was done on a component by component basis with groups of individuals migrated at a time. The migration needed to be coordinated with the management of each component as it impacted email of each user.

I personally had no direct operational responsibility for this process. Detailed plans were created to support this migration. The OCIO should have detailed documentation on when each user or groups of users were migrated.

Those responsible for the planning and execution of the migration included Bruce O'Dell, the Deputy CIO during this period, Bart Hill, the Director of Information Systems & Technology and the OCIO email support team that provided operational support for the email systems.

8. With the Lotus Notes e-mail system, the White House used an archiving system known as ARMS to preserve e-mails sent and received by White House staff. Are you familiar with this system? Were you aware of any concerns about the adequacy of the ARMS program? If so, please describe those concerns.

I was not involved in the implementation of the ARMS system as it was implemented in 1994, prior to my employment with the EOP. My knowledge of the ARMS system was the result of the analysis that I performed in 2002 as part of the project to implement a long-term solution to support the email records management of the EOP.

The ARMS system is really a set of systems that were developed in 1994 to meet a court mandated need to preserve E-mail records. At the time these systems were implemented, no commercial-off-the-shelf (COTS) system to support email records management existed in the marketplace.

The ARMS system was implemented using the staff, contractors, resources and technologies that were present-at-hand within the EOP at that time. The system used simple operating system utilities for the data management, access, search and retrieval of data and the file system for the storage and access control of the data.

During the Clinton administration there were a number of significant problems with ARMS and the associated supporting systems. These problems or anomalies (Mail 2, Letter D and Multi-Host) resulted in situations where E-mail was not appropriately archived by ARMS. These issues were corrected and various project were completed to recover the email that was not archived. The GAO has produced reports documenting these issues and the resolution and corrective actions that were taken.

During my analysis of the ARMS system, a number of operational and non-functional risks and limitations were identified. These were documented in the Concept of Operations (CONOPS) document that I created in 2002. This document was reviewed by OCIO staff, OA Records Management, OA Counsel, the White House Office of Records Management and White House Counsel. This document was the basis for the project to implement a COTS solution to support the email records management of the EOP.

To reduce or eliminate these risks, the ECRMS CONOPS outlined the need to implement a system that utilized current commercially trusted technologies to support the email records management needs of the EOP.

It is also important to note that by 2002 there were a number of COTS products that provided effective email records management solution that were designed to support seamless integration with the Microsoft Exchange platform.

9. What was your role in planning how e-mails would be archived and preserved in the new system? Who else was involved with this and what were their roles?

My role was to lead the effort to perform the analysis, selection a solution and implement the solution to support the effective records management of EOP emails. This project is referred to in various documents and presentations as ECRMS. For a period of time, the project had the name EARS. These two names refer to the same project.

In 2002, there were two other projects that This project began in late 2002 when it was recognized that the first two attempts to use the ARMS system to support the Microsoft Exchange environment could not be the long term solution to support the records management of EOP emails.

Prior to the initiation of the ECRMS project there were two attempts to continue to use the ARMS solution.

The first project was an attempt to modify Windows XP and Microsoft Outlook interface to support integration with ARMS. There were numerous technical issues that prevented this approach from being successful. The OCIO should have documentation on this project.

The second project was an attempt to use an email integration solution to manage and archive email messages using the ARMS environment. The approach was to use Legato EmailXtender solution to provide a mechanism for all Outlook / Exchange E-mails to be managed in ARMS. The project was abandoned as the poor performance of the solution prevented it from supporting day-to-day email message volume requirements.

I believe that Mr. Howard Sparks was responsible for both of these projects.

10. How were e-mails sent to and from Microsoft Exchange accounts archived and preserved? Please describe the various steps involved and the individuals responsible for each step, including the process through which e-mails stored in journals were saved in .pst files.

I was not directly involved in the management decision to proceed with the implementation of Outlook / Exchange. I also did not have any operational responsibility for the archiving of email in either the Notes or Exchange environments.

The initial email retention process involved a manual process of copying messages from the Exchange journals to .pst files for storage and retention. This process was to be performed on a regular basis.

At some point, this process was partially automated using a utility designed for this purpose. The Mail Attender utility was used to automatically copy email message from the journals to the .pst files on a regular basis.

The details regarding the standard operating procedures should be obtained from the IS&T Directorate within the OCIO.

11. As the migration took place, did you have any concerns about how e-mails were being archived and preserved under Microsoft Exchange? What were those concerns? Did you express them to anyone? When did you do this and with whom did you share your concerns?

There was a great deal of concern about proceeding with the migration to Outlook / Exchange without having an adequate email records management solution in place. By early 2003, an entire year had been spent trying to identify a solution that would support the email records management requirements of the EOP. There were four types of risk that were discussed on a number of occasions within the management ranks of the OCIO and OA. This risks included:

- Incomplete Data – The process by which email was being collected and retained was primitive and the risk that data would be lost was high. In addition to this being a manual process, the risk was compounded by the fact that there was no mechanism to reconcile the messages that were retained in the .pst files and the messages that had been processed by the Exchange system. The potential impact: The system does not contain all required data.

- Data Reconciliation – The use of .pst files for warehousing email records does not provide a mechanism to reconcile against what was originally retained by the system. This is there is no way to guarantee that all records are retained in their complete and unmodified state. The potential impact: It cannot be demonstrated that the data in the system is complete.

- Public Perception – Given the issues that occurred during the prior administration, it should warrant extra caution on the part of the EOP before making any changes to the email retention process. Additional system problems would create a public perception that the EOP was unwilling or unable retain records that were required under current law. The potential impact: Increase scrutiny of the EOP and significant additional expense to correct any problems that might occur.

- User Accountability – The approach of simply storing email message in .pst files provides no mechanism or audit trail that tracks changes to data files or the activities performed by users or system administrators. The integrity of the data could be called into question because it was not possible to ensure the inappropriate action, either intentional or unintentional, could not occur. Or, if they did occur, the actions would be logged and the user who performed those actions could be identified. The potential impact: No verification that data retained has not been modified or what activities have been performed by system users or administrators.

In early 2003, prior to the large scale rollout of Exchange, these concerns we often discussed within the management ranks of the OCIO and OA. People involved in these discussion include Tim Campen (OA Director), Carlos Solari (CIO), Bruce O'Dell (Deputy CIO), Bart Hill (IS&T Director), Jaime Borrego (Information Assurance (IA) Director) and myself.

The reason for my involvement in these discussions was that I was leading the effort to identify and implement the long-term email records management solution.

12. Under this Exchange system, were you aware of any avenues through which e-mail archiving could have been circumvented? If so, please describe those avenues as well as any steps you or others took to prevent the loss of e-mails.

Only those email messages sent and received using the EOP Outlook / Exchange and EOP Lotus Notes environments would be included in the EOP email retention process. Other avenues of electronic messaging included:

- Email message sent and received using non-EOP mobile devices (cell phones and PDA's) would not be retained within the EOP records.

- The use of non-EOP mobile devices to access other email service providers such as Hotmail, Gmail or Yahoo. These messages would not be retained with the EOP records.

- Peer-to-Peer Messaging, such as PIN-to-PIN Blackberry messages would not be retained within the set of EOP records.

- Use of non-EOP email sites from EOP computers, such as those hosted by political or other organizations. These records would not be retained within the set of EOP records.

The EOP Information Assurance Policy addressed each of these issues. Current OCIO employees should be able to address these questions.

13. During your time at the White House, was there every any system put in place to audit or verify that e-mails were archived and preserved correctly? If so, when was this system put in place? Who was in charge of this audit and verification?

After the implementation of Microsoft Exchange in 2002 and 2003, and after the migration of users from Notes to Exchange began, there was no automatic audit system that was implemented to ensure that emails were archived and preserved.

It was also discovered in October of 2005 that there was no manual periodic accounting or reporting process.

After the issue of potential missing email was identified in October 2005, one of the corrective actions was to implement a standardized formal daily procedure to ensure that the daily process to copy email messages from the Exchange journals to .pst files occurred without error and was completed as defined by the standard operating procedure.

At the time, this process was conducted on a daily basis by staff that independent of the email operational support team. The results of this process would provide the basis of an audit trail that could be used to validate the number, size and number of messages retained in the inventory of .pst files.

14. Who had access to the servers that held the archived Exchange e-mails? Did these servers have any extra security protections? Would these files ever be opened or modified — for example in a search for records? Who would have had access? Were there any protections to prevent them from being modified or deleted — either intentionally or accidentally?

I had not operational responsibility for the email retention process and I do not know the answers to these questions.

Staff from the IS&T Directorate had operational responsibility for the EOP email systems and the email retention processes.

In mid-2005, prior to the discovery of the potential email issues, a critical security issue was identified and corrected. During this period it was discovered that the file servers and the file directories used to store the retained email .pst files were accessible by everyone on the EOP network.

15. Was there any policy that prevented White House staff from accessing external e-mail accounts on their official White House computers? Was this policy applied universally?

In 2002 and 2003 the EOP Information Assurance Policy was drafted, reviewed and approved. The policy was approved by each component within the EOP.

The purpose of the policy was to address the wide array of information security and information assurance requirements of the EOP.

Relating to email, this policy specifically prohibited the following:

- Use of non-EOP email environments was prohibited because it would not provide a means for supporting records management requirements.

- Use of encrypted email was prohibited because there was no facility to manage records retention of encrypted email.

- Use of peer-to-peer messaging was prohibited.

- The use of instance messaging environments was prohibited.

Questions and information requests on the applications of this policy should be addressed by current OCIO staff.

Potential Losses of E-mails

16. The Committee understands that, at some point in the fall of 2005, concerns arose at the White House that some e-mails may not have been properly archived. According to an e-mail exchange between you and Susan Crippen at the White House, it appears that those concerns may have first been raised on October 11, 2005. What precipitated these discussions about message storage issues? What was your role in these discussions, and who else was involved?

Actually, I believe that I and some members of the OCIO management team suspected there were issues and we discussed these issues within the OCIO management meetings a week or so prior October 11, 2005.

It was reported by the email support team to the OCIO management team that there were some issues related to the processing of the Exchange journals and creation of .pst files for each EOP component. At the time it appeared that because of server / application reconfiguration errors that occurred in August 2005, all EOP email for most of August and September were retained as OA email. It did not appear that any email was missing or not retained, but rather it appeared that all EOP email was retained in a single set of OA .pst files and not the .pst files associated with each component. It was also reported that they email support team attempted to take corrective action to correct the issues, but where unable to fix the problem and separate out the email into their respective components.

This precipitated a series of discussion within OCIO management and staff about how the .pst files were managed and inventoried. It became clear that these files were not being effectively managed.

Some of the issues that became known include:

- The EOP email retention .pst files were scattered across various servers on the EOP network.

- There was no complete inventory of all .pst files

- The processing of the Exchange journals to create the .pst files did not always complete during the normal processing cycle.

- There was no separation of duties or audit controls in place to ensure that the processing of these was being performed on a consistent basis.

- There was no well documented process

- There was no consistently applied naming convention for the component .pst files.

- There was no daily review to ensure that all processing was completed correctly. This point was emphasized by the fact that over a month had gone by before it was discovered that there was a problem in August and September 2005.

17. The White House informed Committee staff that these message storage issues may have been first discovered during a search for documents that found several weeks of e-mails for certain White House components had been stored in the wrong files. Does this match your recollection? What was the circumstance of this search, what was found to have been misfiled, and how was the issue resolved?

Yes this does match my recollection. During my tenure in the OCIO, I was never directly responsible for performing email searches. I do not know about the circumstance of this particular search.

I do not believe that these misfiled email messages were ever separated out back to their associated components. The current OCIO staff should be able to answer this question.

18. At some point, the White House appears to have expanded its search for misfiled e-mails. At this point, the Committee staff understands that you undertook an analysis of e-mails preserved from the Microsoft Exchange environment breaking down the analysis by each of 12 components of the White House. When and why did this process begin? Who worked with you on the process? How did you conduct the analysis?

The process originated when it became apparent in October 2005 that OCIO staff and contractors were not effectively managing the .pst files used to retain the email records for the EOP. This set of issues was brought to the fore by the .pst file management problems that occurred in August and September of that year.

The initial set of actions was simply to organize and inventory the .pst files used for EOP email records retention and to put in place a formal process to manage these files. The primary issue was the .pst files were scattered across various servers on the EOP network. To the best of my recollection, these series of events included:

- Performed a search all servers on the EOP network for all .pst files to identify and locate all .pst files in the EOP environment

- Collect a data set that contains all relevant information about these files (Name, location, size, creation date, etc.)

- Create a secure and organized server environment in which these files could be stored.

- Copy all .pst files to this new secure and organized location

- Verify and validate that all actions to copy these files completed successfully.

- Create an inventory of all .pst files and verify all the information.

These activities were performed by a team of OCIO staff and contractors. Each step of the process was discussed and documented. The team met on a daily basis to plan activities and to report on actions that had been completed.

In addition to this .pst file analysis, the team also began the development formal daily verification process that would support the effective management of these files and the process that created them.

While this process was taking place, I began to notice a few anomalies with these files. These included:

- .pst files that contained no data. The file size was zero bytes.

- Inconsistent naming of files that made it difficult to determine the associated component and date to which the file was associated.

- Obvious gaps in the date ranges represented in filenames of the file. As an example, one file may have been named "OA May 1-5" and another file "OA May 8-10" but there appears to be no file that represented May 6 and 7. This is just an illustrative example.

- There was a wide disparity of frequency of how often .pst files were created for each component.

- There was a wide disparity in size of files that represented similar periods of time.

Because of these issues and because there was no way to effectively determine what data was retained in each file, the team took on the task of performing an additional level of analysis.

If my recollection is correct, at that time there were over 5,000 .pst files with an average size of approximately 2 Gigabytes. Since each of these files contained messages one or more days and since it was not possible to determine what days were included in any given file, we needed to determine a method to perform this analysis. Prior to this effort, Microsoft had provided the EOP with a custom software application for performing searches on .pst files. This tool was commonly referred to as the "FindIt" tool.

Microsoft was contacted and was tasked to modify the FindIt tool so that it included the additional functionality of providing a message count for each day represented in a given .pst file. This process was performed on each .pst file in the inventory and the data was aggregated into a single data set. This is the data set that provided the basis for the analysis.

It took a couple week to perform the analysis on the thousands of .pst files. When the data was tabulated it became clear that a problem existed because there were days for which no email was retained. Extensive testing was performed at that time to ensure that the tools and the tabulation processed was performed correctly. An independent verification and validation was also perform by a different set of contractors to ensure that this analysis process was completed correctly and that the data was correctly analyzed and the accurately represented.

In addition to there being hundreds of days for which specific components had no email retained, there were a number of days for which it was clear that the number of emails retained was lower than expected.

There was a formal analysis to determine if the number of days for which the number of retained EOP emails was lower than what one would expect based on the email volume trends. The analysis determined that there was a clean pattern of email volumes. This analysis accounted for

working days and non-working days (weekends and federal holidays). A multi-week moving average model was employed in various version of the analysis to account for normal fluctuations of normal email volume. Depending on the assumptions made in the analysis, the team identified hundreds of days for which the volume of email was inexplicably low.

Those who worked on this team are listed in response to question 19.

19. The White House provided the Committee with a 23 page color chart titled, "EOP Exchange Environment — All Components," with the subtitle, "Summary — Messages per Day." It lists the total days with zero messages and low messages for 12 components of the White House, as well as the actual message count for each of these components for the period from January 1, 2003 to August 10, 2005. The copy provided to the Committee is dated Feb. 6, 2006, at 4:13 p.m. Were you involved in the creation of this chart? If so, what was your role? Who else was involved in the development and production of the chart?

I was responsible for leading the team that created this chart. The chart to which you refer was the result of many weeks of analysis that involved over a dozen people. I was responsible for designing the chart and had a leading role in the definition and execution of the analysis.

To the best of my recollection, those involved in this effort, in addition to myself, included:

EOP Employees - Jaime Borrego (Acting IS&T Director), William Reynolds (Deputy Director, Information Assurance), Vic Bernson (OA General Counsel), Keith Roberts (Deputy OA Counsel), Howard Sparks (IS&T), Sue Crippen (IS&T), Bryan Reese (IS&T), Stephen Warshauer (IS&T), Keith Regatts (A&E), Aimee Felker (Director OA Records Management), Shaffers Rawlings (EOP Records Management)

Contractors - ███████ (Unisys), ███████████ (Unisys), ████████ (SRA) and various contractors whose names I cannot recall from Microsoft and SRA.

20. Was this the final version of the chart? If not, when was the last version of the chart created?

I reviewed the chart provided to the Committee and I am not able to determine if the version provided is the final version. There were many version of this analysis. Each version was identified with a unique version number. Different version of the analysis included different assumption about date ranges and thresholds.

I do not recall the exact number of versions of this analysis, but I believe it was between 12 and 20. What can be said is that what was provided to the Committee is just the analysis summary report, not the complete analysis.

The complete analysis was approximately 250 pages in length. It included the complete background data and trend analysis.

21. Please describe the steps you and others took to perform the analysis required for the production of this chart. What types of files did you search? Where did you look for these files? Did you face any challenges related to files being misnamed, too large, corrupted, or having other such problems?

In addition to the response to question 18.

During the process to organize and inventory the .pst files, there were a small number of files that appeared to be corrupted. Additional analysis was performed on these files. I do not recall the specific outcome of these analysis, but the data in there files were not for the periods for which data was missing.

22. Each of the 12 components has a different start date on the chart and a different end date. Can you explain why this is?

Each component has a different start date because components were migrated from Notes to Exchange over a several month period.

The OCIO should have detailed list of users and the schedule of when users and components were migrated.

23. Was this chart the only result of your analysis of messages from the EOP Exchange environment? If not, did you produce any other briefing materials or documents that explained your methodology or findings? What were those documents?

There were numerous documents, PowerPoint presentations and other memoranda that described the analysis that was performed, the actions taken to correct the process and the recommendations to improve the processing of .pst files. The team documented the details of each action taken to clean up and correct the identified issues.

There must be thousands of email messages between the team members that describe the actions of the team, the completion of specific tasks, analysis of issues and to provide status to OCIO management, OA Counsel and OA management.