Testimony of

The Computer Report

March 4, 2004

REPORT ON
THE INVESTIGATION INTO IMPROPER ACCESS TO THE SENATE JUDICIARY COMMITTEE'S COMPUTER SYSTEM

Prepared by:
Sergeant at Arms
U.S. Senate

TABLE OF CONTENTS

I. The Scope and Methodology of the Investigation

A. Events Preceding the Investigation

On Friday, November 14, 2003, a Wall Street Journal editorial set forth excerpts of five documents that the Journal described as Democratic "staff strategy memos." The following day the Washington Times reported that it had obtained 14 internal Democratic staff memoranda. The article specifically states the 14 documents "did not come from a Senate staffer." (The two articles are attached to this report as Attachment "A.") On Tuesday, November 18, 2003, 28 pages of material represented to be "the Democrat [sic] memos on judicial nominations," including those referenced in the Wall Street Journal and Washington Times articles over the weekend, were posted on the Coalition for a Fair Judiciary's website at www.fairjudiciary.com. (The 19 relevant documents from the website are attached to this report at Attachment "B.")

On Saturday, November 15, 2003, the Deputy Sergeant at Arms was first notified by Senator Kennedy's Chief Counsel for the Subcommittee on Immigration, Border Security and Citizenship, Mr. _____, that there was a potential security problem with the Judiciary Committee computer system. At the request of Mr. _____, the Deputy Sergeant at Arms arranged for a member of the Assistant Sergeant at Arms - Chief Information Officer's staff to meet Mr. _____ at his office to provide him technical assistance in assessing the situation.

Later that weekend, in consultation with the Deputy Sergeant at Arms, the Majority and Minority Staff Directors for the Committee agreed to place the Committee's server backup tapes in the custody of the United States Capitol Police (USCP) for preservation. The Committee's System Administrator gathered the backup tapes and just after midnight on Sunday, November 16, 2003, the USCP took into custody a box containing 20 tapes, two access cards that allow users to remotely access the network, and an envelope containing 3 pieces of paper with what appeared system administrator passwords noted. At this time, the door to the Committee's computer room, SD 222, was sealed with police tape.

B. The Beginning of the Investigation

The Sergeant at Arms initiated this investigation after receiving requests to do so from Senate Judiciary Committee Chairman Hatch and Senators Leahy, Kennedy, and Durbin of the Committee. Specifically, a letter dated November 17, 2003, from Senator Durbin asked that the Sergeant at Arms, as the Senate's "chief law enforcement officer and also the principal administrative manager for most support services in the Senate, including oversight of computer systems" investigate the "circumstances surrounding the theft of these documents and their distribution" beyond members of his staff. (Attachment "C.") A subsequent letter that same date from Senators Leahy, Kennedy, and Durbin asked the Sergeant at Arms to have an independent computer forensics and security expert help identify who retrieved and released the Democratic documents, assess weaknesses in the Committee's computer network, and make recommendations to help prevent unauthorized access from occurring in the future. (Attachment "D.") On November 20, 2003, a letter from Chairman Hatch authorized the investigation into whether there was any unauthorized access to the Committee documents referenced in the Wall Street Journal and Washington Times. Chairman Hatch also specifically requested: (1) the continued safekeeping of daily backup tapes; (2) a description of the accounts on the system and of the privileges these accounts and security groups have - or had - to network resources from January 1, 2001, to the present; (3) the retrieval of the old hard drives of the servers that were recently replaced; and, (4) replacement of the hard drives of the current servers and establishment of separate local area networks for majority and minority staffs. Chairman Hatch also indicated that he had directed his staff to interview all majority staff, "to determine whether they have any knowledge of actual or potential transgressions related to these documents." (Attachment "E.") The Sergeant at Arms, having consulted with Majority Leader Frist and Democratic Leader Daschle and receiving their approval, immediately commenced an investigation. The USCP continued to take custody of the Committee's daily backup tapes for safekeeping. Additionally, SAA staff determined that the "old hard drives" of the servers were still being used and could not be taken into custody without shutting down the Committee's computer system.

On Friday, November 21, 2003, staff for Chairman Hatch who had been conducting interviews of all majority staff on the Committee advised the Sergeant at Arms that a clerk in the Nominations Unit - Mr. _____ - had admitted to them that day that he had accessed Democratic files over the Committee's computer system. Mr. _____'s desktop computer was immediately taken into custody. Mr. _____'s desktop computer in the office of Majority Leader Frist was also taken into custody for analysis.

Also on November 21, 2003, Chairman Hatch gave the SAA permission to take the Committee's servers' hard drives. SAA staff conducted a site survey to ascertain the physical and logical layout of the Committee's servers and over the weekend of November 22-23, 2003, the four Committee servers were disconnected, their hard drives removed and preserved, and the Committee's data was restored to new hard drives.

On December 3, 2003, the file server from the Majority Leader's office was imaged and the copy secured for forensic

analysis. A backup tape of that office's e-mail server from November 17, 2003, was provided to investigators, but proved to be blank. Subsequently, the System Administrator provided backup tapes from September 29, 2003, and January 12, 2004. These tapes were readable and analyzed by the forensic experts.

C. Investigative Resources

The request for the Sergeant at Arms to conduct this investigation was, as best can be determined, unprecedented. To ensure a thorough investigation, the Sergeant at Arms supplemented his staff's resources with an independent computer forensics firm and additional investigators.

The services of a qualified, outside computer forensics company were obtained pursuant to an existing contract the SAA had in place for Information Technology Support. The Statement of Work for the analysis asked for: (1) a matrix of access permissions assigned to security groups, and individual accounts and the network resources to which they had access, as can best be reconstructed, back to January 2001; (2) an audit of all available and reconstructed logs to look for anomalies in login failures, account logins compared to machine names, file access, and copying, with special emphasis on the documents identified as being from the Judiciary Committee computer system; and, (3) an analysis of probable methods by which these files could have been obtained by other than permitted users. Each of the company's employees who worked on this analysis was required to sign a non-disclosure certification. The work of the forensics analysis and recovery team was overseen by the SAA's lead investigator, the Assistant Sergeant at Arms for Police Operations.

In addition to the forensics analysis of the Judiciary Committee servers, available backup tapes, and the desktops of relevant staff members, this investigation consisted primarily of interviews of those individuals who had access to the Judiciary Committee server. Over 160 interviews were conducted of current and former Judiciary Committee staff members and other individuals who were identified during interviews as possibly having information relating to the investigation. Employees of the SAA technology staffs were also interviewed. Four agents from the United States Secret Service were detailed to the SAA to assist in this investigation. They reported to the SAA lead investigator.

All of those interviewed were asked a standard set of questions as well as individualized questions based on the investigation to date, or as follow up to their answers to the standard questions. Interviewees were allowed to have counsel during the interviews; six individuals chose to have attorneys present.

It would not have been possible to conduct this investigation without the cooperation of the majority and minority Members of the Judiciary Committee and their staffs. Since the inception of the investigation, Chairman Hatch and Senator Leahy have encouraged their staffs to cooperate with the SAA. Staff Directors Mr. _____ and Mr. _____ have been invaluable in providing information and helping with the logistics of locating former employees and arranging interviews. The original copy of the final version of this report and the work product of this investigation will be kept by the Sergeant at Arms. Copies of this report have been made and distributed to the Chairman and Ranking Minority Member of the Committee.

II. Overview of Findings

Investigators interviewed over 160 individuals, primarily those who had access to the Judiciary Committee computer system. In addition, five servers, four workstations and multiple e-mail backup tapes from the Judiciary Committee and Majority Leader Frist's office were analyzed by forensic experts. Individuals who were interviewed did so voluntarily and were advised that this was an administrative, fact-finding inquiry. This report presents the findings of the investigation.

The report begins by outlining the structure of the Judiciary Committee's computer network then addresses whether the Democratic documents disclosed in the press were from the Committee's computer system. It then outlines the admissions of two former Committee staff members who accessed Democratic files, including the scope of that access, and sets forth the forensic verification of how they were able to access other users' files over an extended period of time. The report also examines the statements of other individuals who were identified as knowing that access to Democratic documents was available, addresses a possible source of the disclosures to the press, analyzes other possible means of access to the computer system, and finally, makes recommendations for the future.

Investigators were provided critical information early in the investigation (Friday, November 21, 2003) when staff for Chairman Hatch who had been conducting interviews of majority staff on the Committee advised the Sergeant at Arms that a clerk in the Nominations Unit had admitted to them that day that he had accessed Democratic files over the Committee's computer system. His desktop computer was immediately taken into custody by the SAA.

The forensic review confirmed that 18 of the documents at issue resided on the Nominations Unit clerk's desktop. The documents in question were found within a large, password protected compressed file with either the exact name, or a close approximation. The documents at issue were also found on the Judiciary Committee server in the authors' folders, or the folders of other Democratic staff members to whom the author sent the document.

The Nomination Unit clerk was interviewed on November 23, 2003, as part of this investigation and subsequently re-interviewed twice, with counsel present, later in the investigation. His version of events remained consistent each

time he was interviewed and the investigation verified much of what he told investigators. He and his counsel remained cooperative throughout the investigation.

The clerk first became aware that he could access the files of Democratic staff some time in October or November of 2001. He made this discovery after watching the Committee's Systems Administrator perform some work on his computer. An admittedly curious person, the clerk attempted to duplicate what the System Administrator had done. In so doing, he was able to observe all of the network's other users' home directories. He then clicked on different folders to see which ones he could access; he was able to access some folders, but not others. The folders that he could access, he stated, belonged to both Republican and Democratic staff.

The Nominations Unit clerk reported that he had access to the home directories of other users shortly after beginning his employment in the fall of 2001 until the spring of 2003. Initially he printed approximately 100-200 pages of documents pertaining to Judge Pickering's nomination and gave them to one of his supervisors. Two days later that supervisor and another admonished him not to use the Democratic documents and those that he had given his supervisor were shredded.

Mr. _____joined the staff of the Judiciary Committee in December 2001. A short time after Mr. _____ was hired, the clerk showed him how he could access Democratic files. The clerk who initially discovered how to access the files told investigators that he was not sure what to look for in the files, so Mr. _____ would guide him as to what information was helpful. Mr. _____ would often suggest which directories he should concentrate on and would sometimes tell him that there was something new in a particular folder and ask the clerk to print it for him. Mr. _____ admitted accessing the computer files of Democratic staff himself on one or two occasions.

The Nominations Unit clerk explained that he frequently searched the folders of some Democratic staff on an almost daily basis while working on the nomination of Judge Priscilla Owen. In fact, over the course of accessing other users' files for approximately 18 months, the clerk downloaded thousands of documents. Forensics analysis of a compressed zip folder from his workstation where he kept these documents identified 4,670 files, the majority of which appeared to be from folders belonging to Democratic staff. During the approximately 18 months the clerk accessed other users' files, he stated that he had four or five different computers assigned to him and that regardless of the hardware he used he was able to access this information.

In January 2003, Mr. _____ left the Judiciary Committee and took a position in the office of Majority Leader Frist. The Nominations Unit clerk and Mr. _____ both admitted that the clerk continued to provide Democratic - and also Republican - documents to Mr. _____ after he left the Judiciary Committee. Forensic analysis of the e-mail traffic between the two confirms this. In March or April 2003, the clerk was re-assigned to another Unit in the Judiciary Committee. About the same time (April 2003) the Committee's server was upgraded and the clerk believed that prevented him from being able to access other users' files on the server.

While there was extensive analysis of servers and individual workstations in this investigation, the results were limited due to the absence of proactive security auditing on the Committee's computers. The fact that not all security events were audited significantly inhibited this investigation because permission changes could not be analyzed on any computer.

Because the Committee was not auditing permission changes, the forensic review was not able to provide a history of who had access to the files containing the Democratic documents at issue.

The forensic review of the Judiciary Committee servers that was conducted is consistent with the clerk's explanation of how he was able to access democratic files. The forensic analysis provided investigators with two "snapshots" of the network's permission settings - one from July 2003 (when a file copied from the older server in April was deleted) and one from November 2003 when the server was imaged for this investigation.

The forensic analysis indicated that a majority of the files and folders on the server were accessible to all users on the network. Any user on the network could read, create, modify, or delete any of the files or folders within these folders.

The investigation revealed that users whose network profiles were established prior to August 2001- when a new System Administrator was hired by the Committee - were generally established correctly and had strict permissions; those established after the date were "open." The investigators do not believe that the Committee's System Administrator acted maliciously, or that he himself inappropriately accessed any user's files. Rather, this significant security vulnerability appears to have been caused by the System Administrator's inexperience, and a lack of training and oversight. This System Administrator left the Committee in July 2003, but permissions remained "open." Forensic analysis of the Judiciary Committee server when this investigation began in November 2003 indicates that the system was even more open to all users on the network at that time.

Despite this significant lack of security, the investigation did not reveal any evidence that users continued to access other users' files after the Nominations Unit clerk stopped doing so in April 2003. Other than the Democratic documents in question, no one who was interviewed brought forth any other documents that they believed had been compromised from the computer system.

The investigation did not identify any individuals, other than the clerk and Mr. _____, who were accessing other users'

files on the Judiciary Committee computer network. While the clerk admitted to accessing and printing approximately 100-200 pages of documents and providing them to his supervisor in October or November of 2001, they did not know how he had obtained the documents or that he continued to access additional Democratic documents. Additionally, the supervisors did not bring the matter to the attention of the Staff Director. A forensic analysis of the hard drives of both supervisors was conducted and none of the Democratic documents at issue resided on either drive.

The Nominations Unit clerk identified other Judiciary Committee staff members within the Nominations Unit whom he believed knew Democratic computer files were accessible.

Investigators interviewed all of those individuals that were identified as having knowledge about access to Democratic files. Of those interviewed, only one - the Committee's former System Administrator who was working part-time on developing a database for the majority - knew that any users' folders were inappropriately open to others. This individual did not know the extent of the problem and thought the System Administrator was just "sloppy" with setting some users' permissions. He did not advise the System Administrator of his discovery.

In the interviews that were conducted, to date no other individuals on either the Republican or Democratic staffs admitted that they knew that access could be obtained to the other's files. There was speculation among those interviewed that if Mr. _____ learned how to get access to Democratic files, others on the Committee were probably doing the same thing. The Democratic staff working on judicial nominations clearly did not know there was a vulnerability. If they had, presumably they would have protected their files.

Members of the press and the Coalitions who had possession of the document at issue declined to be interviewed. Without their cooperation, the investigation faced a significant impediment to identifying the source of the disclosure. Several individuals who were interviewed, both Republicans and Democrats, implicated Mr. _____. While there is no definitive evidence pointing to Mr. _____ as the individual who gave the documents to the press, or a party outside of the Senate, there is circumstantial evidence implicating him.

When the Nomination Unit clerk, who considered Mr. _____ a friend, was asked how the Democratic documents were disclosed to the press, he identified Mr. _____ as the likely source. He described a conversation with Mr. _____ shortly after the documents were excerpted in the press where he understood Mr. _____ to acknowledge giving the documents to a third party who then gave them to the press.

The report does not make any recommendation for referral of individuals for Senate or legal ethics or criminal violations. It does set forth some of the options the Judiciary Committee may be considering. It also recommends immediate steps that the Committee should take to enhance its computer security and sets forth measures the SAA will be recommending to the Senate leadership to enhance the computer security network-wide.

III. The Judiciary Committee Computer Network

A. Organizational Background

The SAA provides Information Technology support to the entire Senate, including Committees. Office Automation support is accomplished via the current SAA contractor, Signal Solutions.

The SAA provides Senate offices with a variety of computer hardware and software, including networks, workstations, peripherals and all products associated with a computer system connected to a Local Area Network (LAN), including software such as Operating Systems (usually a variant of Windows NT) and other functional packages and office suites. Software setup and Operating System configuration is usually conducted by SAA staff following configuration specifications requested by the office's System Administrator.

Almost all Senate offices, including Committees, employ their own Systems Administrator. These individuals have a broad range of technical skills, ranging from the bare minimum to advanced technical understanding. The SAA provides training (through the Joint Office of Education and Training), guidance, and/or direct support to Systems Administrators when requested to do so.

B. History of the Judiciary Committee's Network and Systems Administrators

It was determined from interviews of SAA employees that the Judiciary Committee migrated from a mini-computer system to a Local Area Network prior to October 31st, 1991. The specific date is not known, nor is the name of the Systems Administrator at the time.

On August 14th, 1995, the Judiciary Committee computer software system was upgraded from Microsoft (MS) LAN Manager Version 1.1 to MS Windows NT Server 3.51. In December 1999, another upgrade was completed resulting in the software installation of MS Windows NT Server 4.0.

In July 1999, Mr. _____ left the Judiciary Committee after serving as its Systems Administrator. According to SAA staff, Mr. _____ was very independent and rarely used their customer support. In August 1999, an SAA team installed new Y2K-compliant workstations within the Committee. This caused a number of network issues to surface as a result of the System Administrator's nonstandard configurations on the servers and customized, non-standard, individual logon script files. In late 1999, the Judiciary Committee requested assistance from the SAA to bring its computer network back to a standard configuration and into Y2K compliance. An SAA contractor assisted the

Committee for approximately 2 months during the transition to a new Systems Administrator, Mr. _____.
SAA Service Center tickets which track service requests to the Help Desk show that in December 1999 Mr. _____ requested specific assistance from the SAA Help Desk with regard to the Judiciary computer server upgrade. According to these records, Mr. _____ "successfully changed and synchronized server passwords for proper security measures."
On June 21, 2001, Mr. _____ resigned as the Committee's System Administrator and Mr. _____, the System Administrator for Senator Leahy's personal office, performed those duties "unofficially" for the Committee until Mr. _____ was hired on July 17, 2001. This position was first job after obtaining his college degree.
The Committee received new computer hardware ordered by Mr. _____ on February 20, 2003. (Service Center ticket 92377). The service ticket's notes indicate that Mr. _____ declined to schedule a pre-installation meeting with SAA staff and declined the SAA's offer to configure the system. He requested that the equipment be delivered in the original boxes and indicated that he would handle the installation himself. After this installation Mr. _____ called the SAA Help Desk on April 18, 2003, with questions about how to copy files from one server to another. He was advised of the proper procedures and, according to the Help Desk report, was able to copy the files successfully. Three days later Mr. _____ called the Help Desk regarding problems associated with the new Windows 2000 server he had built to use as a file server. He reported encountering login problems on workstations when users attempted to connect to the server and contacted the SAA Help Desk for assistance. The SAA provided technical assistance and on April 30, 2003, Mr. _____ advised the Help Desk staff that he was not having any further difficulties.
On May 29, 2003, Mr. _____ assumed the System Administrator position for the Committee. He remains in this position today. Mr. _____ left the Committee on July 21, 2003. A timeline reflecting the tenure of the Committee's recent System Administrators is attached at "G."
Like some other Senate offices, the Judiciary Committee has historically been staffed with Systems Administrators who preferred to perform most computer-related tasks themselves. This has been true even if they had only minimal technical experience before becoming the Committee's System Administrator. There is no minimum level of proficiency required to obtain a System Administrator position, and there was a considerable variance in the proficiency levels of the Committee's different system administrators. Notably, the records of the Senate Joint Office of Education and Training reflect that Mr. _____ only attended two technical training classes during his tenure, neither relating to the NT Administration.
C. The Architecture of the Judiciary Committee Network
The Judiciary Committee Computer network, when it was imaged at the beginning of this investigation, consisted of a Primary Domain Controller (PDC) Server known as "JUDAK," a Backup Domain Controller (BDC), a Print Server known as "JUDPT," and a File Server which is referred to as "JUDFS01". Collectively, these servers are simply known as the Judiciary Committee File and Print Servers. The network configuration also included an e-mail server that was not taken into custody because backup tapes were available. A diagram of the Judiciary Committee Local Area Network as of November 2003 is attached as "H."
The "JUDAK" server was the primary domain controller (PDC) for the Committee. The server ran the Windows NT 4.0 Operating System and controlled all servers, computer workstations, users, printers, scanners and other computer hardware on the network. PDCs are considered critical infrastructure machines and act as the central management point for the entire network and all its users.
The print server "JUDPT" was the central managing point for all printers and computers that printed. This connected all servers and workstations to all printers and managed the printing of all documents.
The file server "JUDFS01" acted as the central file repository point for all users on the network. The file server allowed users to save and retrieve their files and folders from a central location. This central location offered a large amount of hard drive space (over 200 gigabytes) for data storage by the over 140 user accounts. Administrators generally backup the entire file server periodically as a single entity providing for the recovery of lost data.
The Committee's servers were configured in a way that a Local drive/partition contains the Server Operating System and related utilities, this is known as the server "C:" drive. There also exists a server "E:" drive. This particular local drive/partition contains data files, such as user home directories and shared directories. The System Administrator is responsible for security settings or permissions on the various folders on this drive or partition to allow (or not allow) them to be "shared" with users on the network. The practice in the Judiciary Committee is to "share" certain files among staff working for the same Senator. Users access the folders by mapping them to a drive letter (e.g., H: or S:) that they use just like a drive on their individual workstations.
Specific to each user's desk workstation is a Local "C:" drive that contains the workstation Operating System, applications, and data files. Additionally, the "H:" drive (as
stated above) is also seen and is "mapped" to a user's home directory on the file/print server. An "S:" drive is also "mapped" to the shared folder on the file/print server.
Each user should have exclusive access to his or her own directory. As the name implies, more than one user

typically has access to any shared folders on the server. Access to home directories and shared folders is controlled by permissions set by the system administrator.
The diagram below reflects the Committee's server and desktop configurations.

A detailed explanation of each drive is attached at "I."

IV. The Documents Disclosed to the Press Resided on the Judiciary Committee Computer Network

The Democratic staff documents excerpted in the press and published on the internet appeared initially to have been taken from the Judiciary Committee's computer system. Specifically, one of the authors of a memorandum to Senator Kennedy advised investigators that the document posted on the public website was not the final version of the memorandum printed and disseminated. Likewise, the author of the document that does not have a heading (the first page posted on the website with an "02" in the upper right corner) indicated that it was typed as an outline of thoughts, not intended to be read by anyone else and, therefore, never printed.
The forensic review confirmed that 18 of the documents at issue resided on the Judiciary Committee server. The one document that was not found was identified to investigators as written by Mr. _____, Counsel for Senator Biden, and was posted on the website with "p.20" in the upper right corner. The forensic review searched all files and folders - even those that had been deleted - on all of the servers and workstations taken into custody. Printed copies and, in some cases filenames, of the Democratic staff documents that were provided to the forensic consultants. Additionally, unique mathematical computations for each file were created by the forensic experts and used to search for the documents. All of the found documents resided on desktop. The documents in question were found within a large, password protected compressed file with either the exact name of the original document, or a close approximation. The documents were also found on the Judiciary Committee server in the authors' home directories, or the home directories of other Democratic staff members to whom the author sent the document. A list of the folders where the documents were found is attached at "J" (Memos in Question Analysis).
The forensic analysis revealed no matches for the documents in question on any of the other computer analyzed.
V. A Judiciary Committee Staff Member Accessed the Computer Files of the Documents' Authors

A. Mr. _____ Initial Access

As noted earlier in this report, counsel for Senator Hatch who were conducting interviews the week of November 17th brought to the attention of the Sergeant at Arms that Mr. _____, a nominations clerk for the Senate Judiciary Committee, had acknowledged accessing Democratic files on the Judiciary Committee's computer system. Mr. _____ was interviewed on November 24, 2003, as part of this investigation and subsequently re-interviewed, with counsel present, later in the investigation. His version of events remained consistent each time he was interviewed and the investigation verified much of what he told investigators. Importantly, prior to the initial media reports referencing the Democratic documents at issue, Mr. _____ had already been accepted to graduate school in accounting in Texas and was planning on leaving employment with the Judiciary Committee. He was put on administrative leave the day of his admission to Senator Hatch's counsel and left for Texas on January 7, 2004.
Mr. _____ began working for the majority in the Nominations Unit of the Judiciary Committee on September 19, 2001. He was interviewed and hired by Mr. _____, the Republican Staff Director for the Committee at that time. Mr. _____'s responsibilities involved the handling and processing of nominations paperwork. Later he was given additional responsibilities, including researching for the Committee's attorneys and speaking with the Department of Justice's Legislative Affairs and Legal Policy representatives. He stated that he worked for Ms. _____ and Mr. _____.
According to Mr. _____, he became aware that he could access the files of Democratic staff some time in October or November of 2001. He made this discovery after watching the Committee's Systems Administrator, Mr. _____, perform some work on his computer. An admittedly curious person, Mr. _____ attempted to duplicate what the System Administrator had done after Mr. _____ left his workspace. According to Mr. _____, he accessed "My Network Places/Entire Network/Judak." In so doing, he was able to observe all of the users' home directories. He then clicked on different folders to see which ones he could access; he was able to access some folders, but not others. The folders that he could access, he stated, belonged to both Republican and Democratic staff.
Mr. _____ reported that he had access to other users' home directories shortly after beginning his employment in the fall of 2001 until the spring of 2003. Mr. _____ recalled that the nomination of Judge Charles Pickering to a seat on

the Fifth Circuit was the "hot topic" within the Judiciary Committee in the fall of 2001. As a result, he began navigating the server and searching for information about Judge Pickering. He printed approximately 100-200 pages of documents pertaining to Judge Pickering's nomination and gave them to Ms. _____ in an attempt to get on good terms with her. According to Mr. _____, Ms. _____ appeared pleased with the information and thanked him. He reported that two days later Mr._____ and Ms. _____ admonished him not to use the Democratic documents and Ms. _____ shredded the materials he had given her.

B. Mr. _____'s Possession of Democratic Documents

In December of 2001 Mr. _____ joined the Judiciary Committee as a counsel for the Nominations Unit. Mr. _____ stated that a short time after Mr. _____ was hired, he showed Mr. _____ how to access Democratic staff files and explained that Mr._____ and Ms. _____ had instructed him not to use Democratic materials. Mr. _____'s response, according to Mr. _____, was that everyone knew about the open access and that he did not have to follow the directions given by Mr. _____ and Ms. _____. Furthermore, Mr. _____ recalled that Mr. _____ told him that Senator Hatch wanted the staff to use any means necessary to support President Bush's nominees.

According to Mr. _____, he was not sure what to look for in the files, so Mr. _____ would guide him as to what information was helpful. Mr. _____ explained that Mr. _____ would often suggest which directories he should concentrate on and would sometimes tell him that there was something new in a particular folder and request that Mr. _____ print it out for him. When Mr. _____ printed out documents, he would either hand them to Mr. _____ or leave them in Mr. _____'s top desk drawer. He recalled specifically leaving documents in the desk drawer without a handle.

In his second interview, Mr. _____ explained that Mr. _____ was his supervisor, (a relationship not corroborated by anyone else, including Mr. _____), and when asked by Mr. _____ to look for specific Democratic information he believed he was being directed to do so by his supervisor. Mr. _____ believed that Mr. _____'s instructions superseded those he had been given earlier by Ms. _____ and Mr. _____. Mr. _____ also stated that Mr. _____ told him there was nothing wrong, or illegal with accessing the Democratic files.

In January 2003, Mr. _____ left the Judiciary Committee and took a position in the office of Majority Leader Frist. He continued to have access to the Judiciary Committee server until at least February 12, 2003, when he e-mailed himself (from his Judiciary Committee account to his account on the Frist server) more than 45 documents over three days. Mr. _____ and Mr. _____ both admitted that Mr. _____ continued to provide Democratic - and also Republican - documents to Mr. _____ after he left the Judiciary Committee. E-mail traffic between Mr. _____ and Mr. _____ confirms this. For example, on February 24, 2003, Mr. _____ replied to an e-mail from Mr. _____ with the subject matter "please send asap" by attaching over 30 documents to Mr. _____. And, a March 3, 2003 e-mail from Mr. _____ to Mr. _____ with the subject "lots of chatter" attaches ten documents, the majority of which appear to be written by Democratic staff.

C. The Scope of Access

Mr. _____ explained that he frequently searched the folders of Mr. _____ (Sen. Kennedy), Mr. _____ (Sen. Durbin), Mr. _____ (Sen. Feinstein), Ms. _____ (Sen. Leahy), Mr. _____ (Sen. Biden), Mr. _____ (Sen. Feingold), and Ms. _____ (Sen. Leahy). He acknowledged that most of the documents he accessed were from the files of Ms. _____ and Mr. _____. He admitted accessing these files on an almost daily basis while working on the nomination of Texas Supreme Court Judge Priscilla Owens to the District Court. He stated he accessed the files much less frequently after October 2002 when his mother was murdered. Mr. _____ provided investigators with a two-page printout of a computer screen with Judiciary Committee staff folders and indicated which folders he could access and those he could not. (Attachment "K.")

According to Mr. _____, when he learned of the vulnerability of the computer server he took steps to safeguard his own files. He did this by contacting a friend outside the Senate, whom he thought to be very good in computer security issues. This individual guided Mr. _____ through the necessary steps at his desktop. An interview with this individual confirmed that Mr. _____ advised him that others could read his files and asked for assistance in preventing this access. Mr. _____'s friend helped him "right click on properties" and establish permissions on his files. Mr. _____ stated that he also secured the files of Mr. _____ and Mr. _____, another member of the Nominations Unit, from their workstations.

In March or April 2003, about the same time Mr. _____ left the Nominations Unit and moved to the Civil Division, the server was upgraded and Mr. _____ believes that prevented him from being able to access other users' files on the server. During the approximately 18 months Mr. _____ accessed other users' files, he stated that he had four or five different computers assigned to him and that regardless of the hardware he used he was able to access this information.

The investigation revealed that over the course of accessing other users' files for approximately 18 months, Mr. _____ downloaded thousands of documents. He stated that he created a password protected "zip folder" on his desktop computer once he realized there was going to be an investigation and moved the relevant documents to that

folder. He provided investigators with the password for the folder. The forensics analysis revealed that the compressed zip folder contained 4, 670 files, the majority of which appeared to be from folders belonging to Democratic staff. Over 2,000 of these files appear to belong to one individual, a former counsel for Senator Durbin. Mr. _____ told investigators that the only copy of these documents that he possessed other than those found on his workstation was given to his attorneys. Mr. _____'s counsel provided investigators with two discs which included the contents of Mr. _____'s H: drive, including the zipped files. The attorneys also provided investigators with approximately 500 pages of documents including Democratic documents, Republican talking points and issue papers on judicial nominations, and press and website reports about judicial nominees and this investigation. They represented this to be the complete results of Mr. _____'s production to them of any documents he had in his possession relating to this investigation. Mr. _____ confirmed that he had given everything over to his counsel.

VI. Forensic Verification and Analysis

A. Limitation of Analysis

While there was extensive forensic analysis of servers and individual workstations in this investigation, the results were limited due to the absence of proactive security auditing. Each server and workstation contains three main logs; an application log which tracks programs and what they are doing on the network, a system log which tracks any remarkable system, operating system events, and a security log which tracks successful and failed access attempts to system resources. System Administrators can use the security log to apply both reactive and proactive measures to potential and actual security incidents. The security log can audit successful and failed log ons and log offs, file accesses, user rights, security policy changes and computer restarts.

Prior to the Committee's server upgrade in April 2003, only failed log-on and log-offs were audited. As a result, the forensic review was unable to determine whether any users changed their user rights, attempted to access files to which they did not have access to, or the exact date and time of each log on and log off.

The fact that not all security events were audited significantly inhibited this investigation because permission changes could not be analyzed on any computer. When a user account is created, the System Administrator assigns that user access to certain privileges and resources on the network. If the system is not properly configured, users may be able to change their level of access and privileges. Because the System Administrators were not auditing permission changes, the forensic review was unable to produce a history of who had access to the files containing the Democratic documents at issue. This trend of not fully logging security events began before the the Committee's server upgrade in April of 2003. When the Committee migrated from Windows NT to Windows 2000 in April 2003, the same log settings were preserved and, as a result, the logging continued to be inadequate for a comprehensive security audit.

B. Open Permissions

The forensic review of the Judiciary Committee servers is consistent with Mr. _____'s explanation of how he was able to access files that were owned by Democrat staff of the Committee. The files on the Committee's server (JUDAK) were copied to the new server (JUDIC-FS01) on April 18, 2003 and deleted in July 2003. Forensic experts were able to recover most of these deleted files and analyze file permissions as they were set at the time of deletion.

The forensic analysis indicated that a majority of the files and folders on the server were accessible to all users on the network. Specifically, in 84 out of 144 of the home directories analyzed, the permission assignment was "open," indicating that the "EVERYONE" group had full control. This means that any user on the network could read, create, modify, or delete any of the files or folders within these folders. The remaining folders had a "strict" permission assignment, which meant that a specific user(s) were assigned to the folder, typically the owner of the home directory and the System Administrator. The folder permission analysis is attached to this report at "L".

The folder permission analysis verified Mr. _____'s statements that he was able to access the home directories, or H: drives, of Ms. _____, Mr. _____, Ms. _____, Mr. _____, Ms. _____, and Mr. _____. These files were among those open to everyone on the Judiciary Committee server. Additionally, the forensic review confirmed that access was restricted to the files belonging to Mr. _____, Mr. _____, and Mr. _____ . This finding is consistent with Mr. _____'s report that he took steps to protect these users' files.

The Windows 2000 operating System is built on Windows NT technology and has similar security. As a result, the open permission settings that existed before the Judiciary Committee's server upgrade in April 2003 were inherited by the new server unless the System Administrator took specific steps to change them. Nevertheless, the conversion to the Windows 2000 Operating System left Mr. _____ unable to navigate access to other users' files. Part of the explanation for this is that the Windows 2000 server has a setting (unlike the previously used Windows NT) that does not show the list of all users' folders. As a result, while the Democratic files Mr. _____ had been accessing were still technically open, the path to get to them had changed and it appeared to him that access was no longer available.

C. Pattern of Open Permissions

Our investigation revealed that some user home directories were set to "open" permissions and other home directories were set to "strict" permission. This appears to be a result of the Judiciary Committee Network having two System Administrators during the time frame in question. One System Administrator had very strict account policies in place and the other did not. An analysis of the creation date and permissions of various user accounts was performed and supports this. (Attached at "M" is a chart H: Drive Permissions Analysis Including Start/Creation Dates).

Users accounts created prior to August 2001 were generally created with "strict" permissions; those established after that date were "open." Of the 126 users whose folders were available for forensic analysis, there were only nine exceptions to this general pattern. Four of these exceptions were Nominations Unit staff whose files Mr. _____ admitted protecting. Of the remaining five exceptions, only two had strict permissions that should have, according to the pattern, been open -Ms. _____, counsel for Senator Kyl since August 2003 (formerly counsel for Senator Sessions from August 2002 - August 2003) and counsel for Senator Brownback. Judiciary Committee leave records indicate that Mr. _____ was on leave when Ms. _____ and Mr. _____ began their employment with the Committee. It is likely that their user profiles were established by Mr. _____ in Mr. _____'s absence. They both were interviewed and denied any knowledge of being able to access other user files, or of the Democratic documents in question.

The Committee's recent System Administrators were interviewed on multiple occasions. Mr. _____ was the Committee's System Administrator from December 1999 to June 21, 2001. At that time Mr. _____, the System Administrator from Senator Leahy's personal office took over the duties unofficially until Mr. _____ began on July 17, 2001. Mr. _____ remained in the position until Mr. _____ assumed the duties on May 29, 2003.

Investigators interviewed Mr. _____ in person early in the investigation and had subsequent telephone and e-mail conversations with him. After explaining to investigators how he set up a user profile, Mr. _____ called to correct his response and subsequently sent an e-mail on February 18, 2003, which stated, in part:

In the final step of the process, [sic] I said I would go into the newly created user folder, enable the share, and restrict permission to full access by the particular user. I want to clarify that this was only done under the system I put in place in Spring 2003.

In conversations I've had with Mr. _____ since we spoke, it has come to light that I was not instructed to set such user permissions on each folder under the old system. This was an oversight in teaching me how to set up the accounts. My assumption was that these permissions were restricted by some other means, and as I was taking over an already functioning system, I did not think to double check this area of security.

This statement explains why permissions were open for users who came to work for the Judiciary Committee after July 2001. The investigators do not believe that Mr. _____ acted maliciously, or that he himself inappropriately accessed any user's files. Rather, this significant security vulnerability appears to have been caused by Mr. _____'s inexperience, and a lack of training and oversight.

Despite Mr. _____'s assertions that he properly set permissions after April 2003, forensic analysis of the Judiciary Committee server when this investigation began in November 2003 indicates that the system was even more open to all users on the network at that time. Two-thirds of the folders analyzed were created on April 18, 2003, when they were copied from the old server (JUDAK) to the new server. The majority of the folders on the new server (JUDIC-FS01) have no permissions set. Access to these files would require a user to manually map to another user's drive (as opposed to clicking on folders as Mr. _____ did).

Because the servers in the Judiciary Committee Network remained open from August 2001 through November 2003 it is plausible to assume that additional users may have escalated their privileges, and therefore would have been able to view files belonging to other users. Despite this significant lack of security, the investigation did not reveal any evidence that users continued to access other users' files after Mr. _____ stopped doing so in April 2003. Other than the Democratic documents in question, no one who was interviewed brought forth any documents that had been improperly acquired from the computer systems in question. The next section of this report will address the knowledge of the individuals identified by Mr. _____ as having knowledge of the ability to access Democratic files.

VII. Other Individuals Identified as Having Knowledge

A. Ms. _____ and Mr. _____ in the Fall of 2001

As previously discussed in this report, Mr. _____ admitted to accessing and printing approximately 100-200 pages of documents and providing them to Ms. _____ and Mr. _____ in October, or November of 2001. Ms. _____ and Mr. _____ confirmed that Mr. _____ brought them a stack of documents that appeared to be written by Democratic staff. Ms. _____ stated that she did not know how Mr. _____ had received these documents, but that her impression at that time was that they came from a computer that Mr. _____ inherited from a former Democratic staffer. She remembers recognizing that one of the documents was an internal Democratic memorandum at which point she decided not to do

anything with them and placed them in her top desk drawer. The next day she shredded the documents and told Mr. _____ to shred every copy he made and admonished him that it was not appropriate to read them - "this is not the way they do things here."

Mr. _____'s account of receiving the documents is very similar to that of Ms. _____. Mr. _____ recounts that it was late in the day when Mr. _____ presented a manila folder of documents that appeared to be written by Democratic staff. Mr. _____ did not know that Mr. _____ had access to the files. He stated that later in the evening as he thought about the documents, he concluded that it was wrong to have or use them. The next day he told Ms. _____, "I don't think it's right, we need to get rid of them." They then asked Mr. _____ into Ms. _____'s office and told him to destroy any hard copies that he had and advised him to delete the files if they were on his computer.

Ms. _____ and Mr. _____ both stated that they thought they had resolved the problem and did not feel it was necessary to bring the matter to the attention of their supervisor, Staff Director, Mr. _____. Mr. _____ is no longer a Senate employee, but was interviewed for this investigation. He denies having access to Democratic files or knowing that anyone else had access. The investigation also revealed that is unlikely that Mr. _____ shared with Mr. _____ the fact that he could access Democratic files. Interviews revealed that the two gentlemen did not have a close or friendly working relationship.

The forensics analysis of both Ms. _____'s and Mr. _____'s Judiciary Committee hard drives was conducted. This analysis revealed that none of the Democratic documents at issue resided on either drive. Furthermore, the analysis determined that neither Ms. _____, nor Mr. _____ altered the manner in which they saved their documents, which they might have done if they understood that Mr. _____ and others could access files through the Judiciary Committee server.

Investigators found Ms. _____ and Mr. _____ to be credible and cooperative in this investigation. In fact, on February 23, 2004, Ms. _____ called investigators after she discovered one of the Democratic documents at issue in her possession when she was unpacking her files at a new job. She told investigators she had received the document from Mr. _____, counsel for Majority Whip McConnell, in February or March of 2003. She does not remember the exact conversation, but she had the impression the document came from Mr. _____. When Mr. _____ was re-interviewed he indicated Mr. _____ may have shown him an "opposition document" early in the year, but denied any recollection of the giving the specific document to Ms. _____; although, he acknowledged that it was possible he did so.

B. Nominations Unit Staff

Mr. _____ was questioned by investigators about whether he was aware of anyone else who knew that Democratic files were accessible. He initially stated that, "Everybody knew," but when questioned further he named only several Judiciary Committee staff within the Nominations Unit, specifically, Ms. _____,Mr. _____, Mr. _____, and Mr. _____. Mr. _____ indicated that he was also able to access these files from Ms. _____'s computer. Mr. _____ stated that the other individuals he named had knowledge of being able to access Democratic files because Mr. _____, a former System Administrator for the Committee who was re-hired in November 2001 to develop a database for the majority, demonstrated how access could be obtained. The investigators interviewed all of those individuals that were identified by Mr. _____ as having knowledge about access to Democratic files.

Ms. _____ was employed by the Judiciary Committee in July 1998 as a legislative correspondent and later its nominations clerk. After a break in service she returned to the Committee from August 2001 through September 2003, first as the Nominations Unit investigator and later as a counsel in the Unit. In her first interview, Ms. _____ recalled overhearing a conversation between Ms. _____, Mr. _____, and Mr. _____, in which she heard Mr. _____ say that he could access Democratic files. She believed this was possible because he had inherited a computer previously used by Democratic staff. She further stated that if Mr. _____ had shown colleagues how to access files, it was only because he was shocked or startled that it was possible; he was not showing them so that they could access the files.

When Ms._____ was re-interviewed she was asked again about the "demonstration" Mr. _____ told investigators that Mr. _____ had conducted and her knowledge of Mr. _____'s ability to access Democratic files. Ms._____ recollection of events is not clear. She initially stated during the second interview that Mr. _____ told her directly that he could access other individual's files on the server and at one point had shown her how he could do it, using his own workstation. She later indicated that it could have been that Mr. _____ showed her on her own computer. Ms._____ also stated that she does not have specific recollection of a demonstration by System Administrator. She stated that it is possible that it happened and that she does not remember it because she did not think it was significant at that time. Overall, Ms._____ was not helpful in determining whether others within the Nominations Unit knew that access was available to Democratic files. She acknowledged that events "could have happened" the way Mr. _____ described them to investigators, but had no specific recollection. Mr. _____, conversely, is certain that Ms. _____knew how to access Democratic files, but had no specific knowledge that she had ever done so.

When Mr. _____ was the Committee's System Administrator from December 1999 to June 2001 he stated that he

was meticulous about security permission. Investigators interviewed Mr. _____ three times. While he was nervous and guarded with investigators initially he eventually was forthcoming and essentially confirmed Mr. _____'s recollection of events. He denied accessing Democratic files and had never seen the documents at issue.
When Mr. _____ returned to the Committee in November 2001 to create a database he remembers discovering that Mr. _____, then the Committee's System Administrator, was being "sloppy with permissions." Mr. _____ denies ever giving a "demonstration" as Mr. _____ reported, but does recall that when he was working on Ms. _____'s computer (she did not have an H: drive and was helping her fix that problem) he was able to view folders belonging to other Judiciary Committee staff. He remembers trying to open "a couple" folders and that they were only "Hatch stuff." He recalls that Ms. _____, Mr. _____, and Mr. were present at the time and that he may have said something like, "I can't believe he left it open." This discovery occurred while he was working on Ms. _____'s computer. When asked whether he thought Ms. _____ might have been able to remember the steps he had taken to access other users' folders he stated, "If _____ could remember steps, I'd give you a hundred dollars. She is the most technologically illiterate person I know."
Mr. _____ does not recall ever notifying Mr. _____ of the fact that he was able to access folders that should have been closed. During this investigation Mr. _____, still a Senate employee, sent an e-mail to Senator Hatch's counsel responding to a Boston Globe report that a Republican "computer technician informed his Democratic counterpart of the glitch, but Democrats did nothing to fix the problem" by stating:
... my firmest recollection is that I did not have a conversation with Mr. _____ about what, at the time, I could only have deemed him as being sloppy with some permission and not some problem that of which others would take advantage. What I can remember is leaving him a message to call me about a concern and he didn't return my call.

The only individual interviewed who alleged that Mr. _____ told the Committee's System Administrator about open access to user files was Mr. _____. He claimed to have learned about this from Mr. _____. However, Mr. _____ denied telling Mr. _____ this and stated he did not know whether Mr. _____ was apprised of the situation.
Mr. _____, a law clerk for the Committee in the summer of 2002 and currently Investigations Counsel, initially told investigators that he had never been shown how to access Democratic files. In a second interview focusing on the "demonstration" Mr. _____ said took place, Mr. _____ stated that he had no recollection of a "demonstration" by Mr. _____, but that it could have happened. Mr. _____ thought it was possible that he could have been present while Mr. _____ was showing something on the computer, and he may not have known what was going on. Mr. _____ denies accessing the files of Democratic staff.
Mr. _____, also a law clerk for the Committee in the summer of 2002 and no longer employed by the Senate, was interviewed telephonically and denied accessing Democratic files. He stated that he was not aware that the possibility of doing so existed; it was not common knowledge in the office. He also denied being present at a "demonstration" by Mr. _____.