Testimony of

Computer Report #2

March 4, 2004

C. Other Judiciary Committee Staff

In the interviews that were conducted, 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 is 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.

Other than the supposed "demonstration" by Mr. _____, neither Mr. _____, nor Mr. _____ identified anyone who they thought knew about accessing Democratic files. It is believable that they would not have told others. Notably, excerpts from e-mails between the two men set forth later in this report indicate their desire to keep secret the fact they had access to these documents. Mr. _____ was thought of by his peers as having "a mole" on the other side and would smile when he was asked how he knew what appeared to be insider Democratic information.

There was speculation, by Republican staff that were interviewed, that the Democrats had been reading their memoranda. Each time this was mentioned, the investigators asked the person being interviewed to identify documents that he/she thought had been compromised and none was ever identified.

Unfortunately, forensic analysis cannot determine which users accessed specific files and/or folders. As explained earlier in this report, the audit logs that would show this were not turned on in the Judiciary Committee system. While the system has this type of tracking capability, in the Senate it is typically used only as an incident response and it is standard procedure to leave the logs off during normal operation. For this same reason, forensics cannot tell us whether a user was successful or unsuccessful in attempting to access something he/she was not authorized to access.

VIII. A Possible Source of the Disclosure to the Press

During the investigation several individuals acknowledged having seen hard copies of the Democratic documents. Investigators spoke with anyone that was identified as having a copy of the documents to ascertain how they came into their possession. Most individuals who had hard copies had downloaded them from the Coalition for a Fair Judiciary website. The one exception to this was Mr. _____, counsel for Senator Kyl, who told investigators that he received the documents from Mr. _____ of the Wall Street Journal on November 14, 2003.

Counsel for the Wall Street Journal declined to make Mr. _____, or Ms. _____, available for interviews. Mr. _____, the author of the Washington Times article on November 15, 2003, stated that he received the documents in hard copy, but not from a staff person on the Hill. He declined to name his source.

Ms. _____, President of the Coalition for a Fair Judiciary, whose website initially posted the documents, also declined to be interviewed citing the Sergeant at Arms' lack of "jurisdiction" over her, or the Coalition. Mr. _____, Executive Director for the Committee for Justice, who Mr. _____ believed to be the middle-man between Mr. _____ and the press, declined to be interviewed after investigators refused to give him a list of questions in advance. He also returned investigators' call to interview Mr. _____, Chairman of the Committee for Justice, reporting that Mr. _____ declined to be interviewed.

Without the press, or Coalitions being willing to reveal their source of the Democratic documents, the investigation faced a significant impediment to identifying the source of the disclosure. Additionally, because this was a fact-finding, administration investigation, law enforcement tools such as grand jury subpoenas to compel testimony and offers of prosecutorial immunity were not available to investigators. However, several individuals who were interviewed, both Republican and Democratic, 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 a substantial amount of circumstantial evidence implicating him. Additionally, Mr. _____'s statements contradicted forensic evidence on two occasions and at other times were inconsistent with the recollection of other, reliable individuals.

Mr. _____ has admitted to accessing Democratic files on his computer. Initially he told investigators that Mr. _____ has tried to demonstrate this to him, but he was unsuccessful because he was not very computer savvy. Later, he admitted to accessing the files from his workstation on two occasions. In his press statement the day he resigned, Mr. _____ stated, "Although I came to learn how to access two or three of these files easily enough, I did so few times

and initially to ascertain that Democrats could access Republican files as well."
When the Democratic documents first appeared on the Coalition for a Fair Judiciary website on November 18, 2003, the last document that was posted was an e-mail containing the directory path of Mr. _____ at the bottom. A forensic review helped determine this document was an e-mail from a web page that was viewed and printed by Mr. _____ with Internet Explorer. Mr. _____ could not offer an explanation for this, other than noting that the document was not a Democratic staff memorandum. When he was advised his directory path was on a document on the website, he called and asked that it be removed and a new version without his directory path was subsequently posted.
When Mr. _____ was asked how the Democratic documents were disclosed to the press, he identified Mr. _____ as the likely source. Mr. _____ stated that he met Mr. _____ in the Senate Chef (an eatery in the Dirksen building) early in the week of November 17, 2003, shortly after the story broke. Mr. _____ stated that he specifically asked Mr. _____ if he had leaked the documents to the press and that Mr. _____ said "No." Mr. _____ told investigators that he then asked Mr. _____ whether he gave them to Mr. _____ who gave them to the press. Mr. _____'s response, according to Mr. _____, was to nod his head affirmatively.
When investigators presented Mr. _____ with this information, he confirmed meeting Mr. _____ in the Senate Chef, but denied giving the documents to Mr. _____, or indicating to Mr. _____ that he did so.
Mr. _____ recalled having seen nine of the Democratic documents that were posted on the website before they were made public. He may have seen the others, but stated that he did not specifically recall them. He denied giving the documents to the press in his initial interview and when asked in his second interview whether he had ever given them to anyone else, he answered "no - not to my recollection." In his third interview, Mr. _____ continued to deny giving the documents to the press and had no specific recollection of giving them to anyone else, although he admitted he often shared "opposition information" with colleagues and could not say for sure whether he had given them to anyone else.
Also in his second interview, Mr. _____ told investigators that most of the documents Mr. _____ printed for him were useless and he would just throw them out. The ones he thought might be useful he kept in a folder that he later lost. He speculated this might have happened when he moved from the Judiciary Committee to the Majority Leader's offices. In his third interview he indicated he believes he lost the folder in the Majority Leader's office.
In Mr. _____'s interview with investigators on January 15, 2004, he admitted to receiving memoranda while in the Senate Majority Leader's office, but denied actively soliciting it. The e-mail traffic below directly contradicts Mr. _____'s statement to investigators:

From: _____, _____ (Frist)
Sent: Wednesday, April 09, 2003 3:27 pm
To: _____, _____ (Judiciary)
Subject: anything

On what Feinstein is doing re: Owen. Info on meeting she has had. Her Tps?[sic]

_____

From: _____, _____
Sent: Wednesday, April 09, 2003 3:40 PM
To: _____, _____ (Frist)
Subject: RE: anything

This all I could find (most of it from __).

Mr. _____ asserted to investigators that his conduct in accessing Democratic files was not unauthorized and that it was appropriate to make these documents public because they were left available to others by the Democrats. He does not believe that he has committed any wrongdoing. A review of the e-mail traffic between Mr. _____ and Mr. _____, however, indicates that they actively sought to keep what they were doing from others and acted covertly. For example, in the e-mail exchange between the two set forth below in March 2003 regarding a set of Republican documents referred to as the "Amex binder," Mr. _____ does instruct Mr. _____ to send documents to a third party.
From: _____, _____ (Frist)
Sent: Thursday, March 06, 2003 10:48 AM
To: _____, _____ (Judiciary)

Subject: Am Ex
Importance: High

_____,

Can I ask you to undertake a discreet mission. Mr. _____ should get a complete relpcate [sic]of the Ame Ex binder. He needs to get up to speed with outr [sic] best info as he build [sic] relationships with the press.

Let me know how soon...assuming you accept, Mr.Phelps.

_____
_____

From: _____, _____ (Judiciary)
Sent: Thursday, March 06, 2003 11:09 AM
To: _____, _____ (Frist)
Subject: Am Ex
Importance: High

_____,

Of course I would be happy to assist in this covert action. The question is: exactly how much should I provide? You know, we have loads on [sic] information.

_____

From: _____, _____ (Frist)
Sent: Saturday, March 08, 2003 3:50 PM
To: _____, _____ (Judiciary)
Subject: Am Ex
Importance: High

Whatever is in the binder and whatever gives him a sense of the facts in rebuttal to the recurring themes.

_____

From: _____, _____ (Judiciary)
Subject: Follow up on previous e-mail
Date: Fri, 07 March 2003 15:20
To: _____, _____ (Frist)

As is the usual practice, please don't let anyone here know that I know all this.

_____
On March 21, 2003, Mr. _____ e-mailed Mr. _____ 169 documents represented to be the "Am Ex" folder.
Another example of Mr. _____ taking steps to protect others from finding out that he had accessed Democratic files occurred when he left the Judiciary Committee.
From: _____, _____ (Judiciary)
Subject: Old Files
Date: Wednesday, March 5, 2003 4:20 PM
To: _____, _____ (Frist)

It seems_____ has removed your old file folders you didn't want others to see-which is good because people here have started to access your old files. You should check the e-mail I just bcc'd you on because_____ and

_____asked for the Dear Colleague letter. I had no choice but to forward it to them. Good luck with everything!
_____

Another example from earlier that same date:

From: _____, _____ (Judiciary)
Sent: Wednesday, March 5, 2003 2:42 PM
To: _____, _____ (Frist)
Subject: FILES

You may need to e-mail_____ separately (just bcc: me on it) and instruct him to permanently remove the personal, confidential files from the system contained in the folders named "Rose" and "Personal." Everyone now has access to these files. I have already copies [sic] these onto my computer as your backup just in case. If there is anything else you need off of there before he deletes any more files, let me know and I'll get you taken care of. But you should probably express your concern that you don't want your private files available to everyone and just ask him to delete those two folders. I'll monitor the situation and let you know what happens.

_____

Six minutes later Mr. _____ e-mails Mr. _____:
From: _____, _____ (Frist)
Sent: Wednesday, March 05, 2003 2:48 PM
To: _____, _____ (Judiciary)
Subject: Files

Please delete my personal files from the stored files. They are in folders marked 'Personal" and "Rose" and "fillib".
_____
_____responds:
From:_____, _____ (Judiciary)
Sent: Wednesday, March 05, 2003 2:51 PM
To: _____, _____ (Frist)
Subject: RE: Files

No problem _____. I've deleted them.
_____
Mr. _____ advised investigators that "Rose" was the folder where Mr. _____ put the Democratic documents that Mr. _____ e-mailed to him. A review of the contents of this folder confirmed it contained Democratic documents. The e-mail exchange set forth above indicates that after Mr. _____ left the Judiciary Committee the System Administrator followed the Committee's usual practice and moved the documents from a former staff member's home directory into a folder in the shared directory. When this was discovered, Mr. _____ had the System Administrator delete the folder containing Democratic documents. In his last interview, Mr. _____ denied that he had ever downloaded any of the Democratic documents from Democratic folders, or Mr. _____'s e-mails to him. Instead, he stated that "Rose" contained possibly scanned copies of Democratic files he received from Mr. _____, or notes he made about those documents. The contents of "Rose" contradict Mr. _____'s statement.
After the Wall Street Journal article appeared on November 14, 2003, and the documents were posted on the public website, Mr. _____, Chief of Staff to Majority Leader Frist, called Mr. _____ into his office where Mr. _____ stated that he had accessed Democratic files in the past, but that he had not accessed anything since he had come to the Majority Leader's office.
As outlined by the e-mails set forth above, Mr. _____ continued to receive Democratic documents from Mr. _____ after he left the Judiciary Committee even though he was not able to access the files himself after he was taken off the Judiciary Committee's computer network. According to Mr._____, Mr. _____ during that meeting said, "I made a mistake." Mr. _____ denies this.
In his final interview Mr. _____ mentioned for the first time that a backup disc, made while he was at the Majority Leader's office, had just come into his possession. He told investigators that a friend of his from outside the Senate had made a backup disc for him and had recently reminded him of that. He declined to give investigators the name of the friend stating that he did not want to prolong this investigation. He also refused to give investigators the names of

his White House legislative contacts for the same reason. The existence of this backup disc and the lost file of Democratic documents leaves open the possibility that Mr. _____ has Democratic documents in his possession.

IX. Analysis of Other Possible Methods of Access to Documents from the Judiciary Committee Computer System.

While it is clear to investigators that the Democratic documents disclosed to the press in this case originated with Mr. _____'s accessing the files of Democratic staff who had open permissions, the investigation revealed other possible theories of how these documents might have become public. This section of the report addresses several of those theories and starting with the premise that the documents were, at least initially, taken from the computer system, presents several possible methods through which access could have been gained. This section of the report addresses some of the possible ways this might have occurred.

A. Hacking Into the System From the Outside

The SAA employs a number of technical, management and operational controls at the boundaries of the Senate network. These controls are designed to:

? Prevent unauthorized access to computers located inside the SAA;
? Allow controlled remote access by authorized Senate employees and vendors;
? Prevent interconnection between offices; and,
? Detect anomalies which may be indicative of potential security events.

The controls are both preventive and detective in nature. Multiple technologies provide these controls and they are deployed according to an overall "defense in depth" strategy. A diagram of the Senate's layered information security approach is attached at "N."

Some technical controls are monitored by network operations staff and some are monitored by an outside information technology security contractor. When potential security events are noted by either party, SAA staff is alerted. Despite not detecting any failure in these controls, the SAA periodically engages outside parties to evaluate their efficiency and effectiveness.

Remote access is provided only to authorized personnel upon request. Technical controls used for remote access include a two-factor authentication consisting of a time synch physical token (SecurID) and a personal identification number. These tokens are issued to Senate office representatives, who are then responsible for distributing and tracking them within their offices. Remote users are routed to their office subnet only. These remote connections are also monitored by the SAA's enterprise-wide detective controls. When anomalous behavior is detected (such as when a remote user's computer or laptop is believed to be infected with a virus or computer worm), the SAA identifies the user ID attached to the remote connection and notifies the proper System Administrator.

The SAA has not encountered any incident where unauthorized access by an outside intruder occurred to a Senate computer within its network boundaries.

B. PcAnywhere presented a security risk.

When the Committee's servers were being imaged for this investigation, pcAnywhere started up on the Primary Domain Controller. This led investigators to question whether this software was in any way involved in giving unauthorized users access to the Judiciary Committee network.

PcAnywhere is part of the standard SAA template installed on desktop workstations and laptop computers, primarily to allow the System Administrator, or the SAA Help Desk, to access the machines for troubleshooting purposes. As part of the standard installation, it is configured to require the workstation owner's express permission each time a System Administrator, or the Help Desk needs access. It is common to see pcAnywhere on a Senate user's workstation and the Judiciary Committee did allow the SAA's Help Desk to assist its staff by utilizing this application. PcAnywhere was most likely installed by the Committee's System Administrator because the servers were delivered by the SAA without software and the SAA does not have any records indicating that it subsequently installed the application.

The forensic explanation of why the pcAnywhere application automatically started during imaging of the Judiciary Committee server is that it was most likely part of a start-up routine established by the System Administrator, or a process that was set to start up at a specific time. The application was running silently in the background and was scheduled to be activated and begin "listening" for remote connections at the time it started up.

While it is not likely that pcAnywhere contributed to the disclosures in this case, the forensic review notes that it did present a vulnerability for the Judiciary Committee network. The program requires strict rules for obvious security reasons and the application on the Judiciary Committee server was explicitly configured less secure and contrary to its producer's recommendations. Unfortunately, because pcAnywhere did not log any user or program information, there was no way to determine if an unauthorized user attempted to break into the server.

C. The Anthrax Incident in October 2001

Some of those who were interviewed for this investigation speculated that the involvement of the SAA during the

anthrax incident in October 2001 may have resulted in the relaxation of security controls for the Committee. According to the ASAA-CIO, the Judiciary Committee computer systems were unaffected by the Anthrax incident on October 15, 2001. During the temporary relocation of some Judiciary Committee staff to the Postal Square Building from November 2001 through January 2002, the SAA provided access to the Judiciary Committee network from Postal Square to accommodate workstations that were set up there for the use of the Judiciary Committee staff. This involved setting up a separate subnet for the Committee's workstations in Postal Square and then giving that subnet access through the Senate network routers to the Judiciary Committee subnet. The setup did not include, or require any changes to the host-based security on the Judiciary Committee servers. Anyone who wanted to access a resource on the Judiciary Committee network still had to log on to the server with a valid user name and password and have the appropriate permissions.

It is also important to note that the Nominations Unit, located at this time in the Dirksen building, did not require relocation. Mr. _____ worked at his same workstation throughout the incident. Additionally, because the Committee's servers were located in the Dirksen Building, the System Administrator still had physical access to the server to perform whatever administrative tasks needed to be done.

D. Poor Physical Security/Computer Security Controls

Throughout the course of this investigation, several systemic flaws in both the physical security and computer security practices within the Judiciary Committee were identified as potential compromise points for sensitive documents. While the investigation has revealed that these vulnerabilities did or currently do exist, in no way did the investigation reveal that they contributed to the particular accessing and compromise of the documents in this case. Nevertheless, this report will note the security deficiencies identified in interviews of current and former Judiciary Committee staff to advise the Committee of potential vulnerabilities.

The Committee has never had documented computer security rules. While the Sergeant at Arms offers training and recommendations to the Systems Administrators assigned to Senate offices, there is no requirement that a Systems Administrator abide by those recommendations, or attend training.

One of the consistent computer security problems identified was the issuance and maintenance of passwords needed to access the Judiciary Committee server. Interviews with numerous Committee staff members revealed that many of them were issued predictable passwords that were identical to their username. For example, a staff member named John Doe would be issued a username of "JohnD," and his password would also be "JohnD." The individual would never be prompted to change, or customize his password. Interviews revealed that, while some staff members took it upon themselves to change their passwords, many did not (even as this inquiry was ongoing). In contrast, access to the e-mail server set up by the SAA staff requires a more stringent alphanumeric password, and the system forces the user to change his/her password after a preset number of days.

Another common password weakness identified was the issuance of generic and predictable passwords for interns, such as "intern1," "intern2," etc. Finally, there seemed to be a pattern of staff members sharing passwords. An administrative assistant for one subcommittee kept a list of user names and passwords for all staff members who worked for one Senator. Other staff members said that they would sometimes share their passwords with co-workers for various reasons, while others indicated that they would leave their passwords on, or near their workstation.

Another common computer security flaw identified was staff members not logging off the Judiciary Committee server, or not turning off their computers when leaving their workstations. The majority of staff members interviewed said they did not regularly turn off their computers upon leaving their workstations, including when they left work at the end of the day. This is particularly problematic because, unlike many current system configurations, the Judiciary Committee server does not automatically log a user off the system after a predetermined period of inactivity.

When this investigation commenced the Committee did not have an up-to-date list of which staff members had access to the network through remote access via SecureID. SAA records indicated the Committee had 16 active remote access cards, but the SAA does not track the names of individuals within the Committee who are given the cards. When this investigation began, the Committee's System Administrator was unable to account for all of the active remote access cards. While this is a potential vulnerability, users with remote access still need a valid username and password to access the network so it is unlikely the lack of inventory control contributed to access by an unauthorized person.

Another security vulnerability identified was that, upon leaving for other jobs, staff members would sometimes download several, if not all, of their files onto compact discs, or other types of storage media. At least one of the authors of the compromised memoranda posted on the internet in this case had done so, although the author said the compact disc containing the questioned files was accounted for.

Several vulnerabilities were also identified in terms of physical security of documents within the Judiciary Committee offices. Interviews revealed that most offices did not have a system for disposing of sensitive documents. Most documents (draft copies of memos, etc.) were just thrown in the regular trash. Other than classified material such as FBI files, no distinction was made in the sensitivity of other documents. There was no regular practice of using locking

waste bins, burn bags, shredders, or any other devices to enhance operational security. In fact, many of those interviewed indicated that sensitive documents were regularly left out on desks. Additionally, several staff reported that office doors were left unlocked at night.

X. Recommendations for the Future

A. Referral for Sanctions

Upon receipt and review of this report the Committee will have before it decisions to make about whether to refer individuals identified in this report for disciplinary, or criminal sanctions. The Chairman's letter authorizing the Sergeant at Arms to conduct this investigation requested only fact-finding and it is beyond the scope of this report to recommend any particular sanction for individuals identified in this report as having access to Democratic files. However, it is clear that one of the considerations before the Committee is what steps should be taken next. The Chairman and Senator Leahy have specifically asked whether a crime has been committed. Accordingly, this section of the report will address the criteria for possible referrals for disciplinary action and for criminal prosecution to the Department of Justice. It should be noted that any referral to a non-Senate entity - whether made by an individual, the Committee, or the Senate - could be problematic if that outside entity decides to conduct further investigation, or inquiry in a manner deemed inappropriate by Members.

1. Possible Ethics Committee Referral

Rule 29.5 of the Standing Rules of the Senate provides:

Any Senator, officer, or employee of the Senate who shall disclose the secret or confidential business or proceedings of the Senate, including the business and proceedings of the committees, subcommittees and offices of the Senate shall be liable, if a Senator, to suffer expulsion from the body; and if an officer or employee, to dismissal from the service of the Senate, and to punishment for contempt.

When this Rule was amended in 1992 by Sen. Res. 363 to include the protection of business of committees, Senator Mitchell outlined the reasons why the protections afforded confidential business, or proceedings of the Senate should be expanded to cover committees, subcommittees, and offices. He stated:

...candid discussions among Members depend upon a trust that is based, in part, on a willingness of all Members to abide by the practices of the Senate. Those practices place responsibility for certain decisions, such as the decision whether to release confidential information, in the hands of the Senate as a whole, or in committees of the Senate, rather than in individual Senators. The unilateral decision by a Member or employee to release confidential committee information is inconsistent with the Senate's practice of making such decisions openly and collectively. Arrogation of this responsibility by individuals can destroy mutual trust among Members and be harmful to the institution. Congressional Record, October 8, 1992, p. 17836.

The legislative history of this amendment also explains that while the Select Committee on Ethics would have jurisdiction to consider an allegation of Rule 29.5, "[almost always, questions about leaks should be addressed first by Members or committees or offices themselves." Id.

The Select Committee on Ethics also investigates unethical and improper conduct which may reflect upon the Senate, even though that conduct does not violate a written law, Senate rule, or regulation. S. Res. 338, 88th Cong., 2d. Sess. (1964), as amended by S. Res. 110, 95th Cong., 1st Sess. (1977).

The Ethics Committee procedures may provide the Judiciary Committee with an avenue for determining whether a criminal referral to the Justice Department is appropriate. While it would not be able to exercise jurisdiction over former Senate employees, it may be willing to consider reviewing the report of this investigation for possible criminal referral.

2. State Bar Attorney Disciplinary Boards

Model Rule 8.4 of the American Bar Association's Model Rules of Professional Conduct states that it is professional misconduct for a lawyer to, among other things, "(c) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation." The comments to this Rule are instructive:

(2)...a lawyer should be professionally answerable only for offenses that indicate lack of those characteristics relevant to law practice. Offenses involving violence, dishonesty, breach of trust, or serious interference with the administration of justice are in that category.

This investigation did not identify the states where any of the attorneys interviewed are licensed to practice law. The Committee may decide to refer attorneys subject to a rule similar to 8.4 to the attorney disciplinary boards where they are licensed to practice law. One significant note of caution in considering type of referral is that it may open doors to state disciplinary boards asserting jurisdiction over Senate attorneys where in the past they have not. Additionally, the Committee would be expected to cooperate in any subsequent investigation, the details and avenues of which may

be beyond what it originally anticipated.
3. The Justice Department
If the Committee were to refer this report to the Justice Department, prosecution might be considered under the Computer Fraud and Abuse Act. The provision of this law most likely to apply in this case is 18 U.S.C. section 1030(a)(2)(B). It provides:
(a) Whoever -
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -
(B) information from any department or agency of the United States;
shall be punished under subsection (c) of this section.

For purposes of 18 U.S.C. section 1030:

- the term "exceeds unauthorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the access-er is not entitled so to obtain or alter; 18 U.S.C. section 1030(e)(6).

- the term "department of the United States" means the legislative, or judicial branch of the Government, or one of the executive departments enumerated in section 101 of title 5; 18 U.S.C. section 1030(e)(7).

When Congress amended 18 U.S.C. section 1030 in 1996 by adding section (a)(2)(B), it meant to address a gap in the law's coverage. The legislative history states:
The second gap is the significant limitation on the privacy protection given to information held on Federal Government computers. Specifically, the prohibition only applies to outsiders who gain unauthorized access to Federal Government computers, and not to Government employees who abuse their computer access privileges to obtain Government information that may be sensitive and confidential. Senate Report 104-357, 104th Cong., 2d Sess., August 27, 1996, p. 4.

The legislative history also indicates that section (2)(B) was meant to cover government employees who "obtain information" by merely reading it. Id.
18 U.S. C. section 1030(a)(2)(B) is a misdemeanor punishable by a fine and/or not more than one year imprisonment. A referral to the Department of Justice could be made by either contacting the United States Attorneys' office for the District of Columbia or the Criminal Division's Computer Crimes and Intellectual Property Section. A prosecution under this section could result in litigation involving the article I, section 6 of the Constitution (speech and debate), the First Amendment (freedom of the press issues), the Fourth Amendment (issues relating to the search of computer records), and the definition of "unauthorized access' under the statute. And, while a criminal investigation could commence upon referral to the Department of Justice, a Senate Resolution would be needed to introduce documents or testimony into a Grand Jury or at trial. See Senate Rule 11.
In informal briefings prior to the issuance of this report, Committee Members asked about the possibility of pursuing a false statement case against Mr. _____ for being untruthful with investigators. The relevant statute, 18 U.S.C. section 1001, provides:
(A) Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully -

(2) makes any false, fictitious, or fraudulent statement or representation;
shall be fined under this title or imprisoned not more than 5 years, or both.

The statue specifically addresses false statements in the context of legislative investigations:
(C) With respect to any matter within the jurisdiction of the legislative branch, subsection (a) shall apply only to -
(2)any investigation or review, conducted pursuant to the authority of any committee, subcommittee, commission, or office of the Congress, consistent with applicable rules of the House or Senate.

Members have also inquired about whether persons who received copies of the Democratic documents violated the law by receiving stolen property. The relevant statute under which prosecution might be considered provides:
Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted --

Shall be fined under this title or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $1000, he shall be fined under this title or imprisoned not more than one year, or both. 18 U.S.C. section 641.

In addition to the statutes set forth above, a referral for prosecution may raise issues of whether any laws of the District of Columbia were violated in this matter. While this report does not intend to present an exhaustive consideration of all possibly applicable criminal statutes, the District's prohibition against taking property without right is another statute that local prosecutors might consider. It provides:
A person commits the offense of taking property without right if that person takes and carries away the property of another without right to do so. A person convicted of taking property without right shall be fined not more than $300 or imprisoned not more than 90 days, or both. DC ST 22-3216 (1981).

A prosecution under a District of Columbia or any federal statute would implicate many of the same issues outlined above as likely to be presented by a prosecution under 18 U.S.C. section 1030. In deciding whether to pursue a prosecution arising from the facts of this investigation, prosecutors will apply the usual standard of review in considering whether to pursue or decline the case: whether there is evidence of a prima facie case and a reasonable probability of conviction, i.e, whether the admissible evidence will probably be sufficient to obtain and sustain a conviction. Other considerations influencing prosecution include whether there is a substantial federal interest affected and if there exists an adequate, noncriminal alternative to prosecution. United States Attorney Manual, section 9-27.220.
B. Immediate Steps to Enhance Computer Security for the Committee
Separate servers were provided to the Judiciary Committee during the pendency of this investigation. The Committee now has two System Administrators - one for the Republican staff and one for the Democratic staff. This will eliminate any concern that users' files have open permissions allowing those of the other party to view their documents. It does not, however, ensure that permissions are set properly to secure users' home directories from the view of other users on the same server, or that other vulnerabilities addressed in this report will not recur. To ensure the future security of the Committee's computer system, the SAA recommends additional training, enhanced security practices and a complete, prospective security audit.
The Committee leadership should require that its System Administrators' enroll in additional training programs with an emphasis on security policies. This training is provided on a regular basis by the Senate's Joint Office of Education and Training Office. Additionally, the Committee should require mandatory and recurring user training also with an emphasis on security policies and best practices. Users generally did not understand the difference between their home directories, shared folders, and their local hard drives, how to protect their passwords, or the importance of not leaving their computer running when away from their desks. This training could be provided by the System Administrator's or through the Joint Office of Education and Training. The Committee should also consider incorporating ethics training into an orientation program for new employees to ensure they understand the Senate's expectations for ethical conduct that meets the highest professional standards.
There are several security practices that should be implemented by the Committee immediately if it has not already done so:
? Review permissions setting to ensure proper restrictions;
? Establish and enforce strict password policies;
? Ensure that operating system logs are capturing the required security information;
? Start a Security Awareness Campaign to educate users; and
Develop a tracking system for inventory of hardware, remote access cards and other computer-related assets.

Regardless of the efforts of the Committee to enhance security since the beginning of this investigation, the SAA strongly recommends a prospective audit of the network by a party outside of the Committee. The audit would be focused on security and compromise protection. It will provide an assessment of the efficiency and effectiveness of current physical and logical controls over the computerized information systems and recommendations for improvement. The SAA believes this proactive review is necessary for the Committee to maintain a consistently available network with efficiency and security in mind. The audit could be conducted by the SAA, the General Accounting Office, or a private contractor. On February 20, 2004, the Chairman and Ranking Member sent a letter to the General Accounting Office to commence this important audit.

C. Measures to Enhance the Security of Computer Networks Senate-Wide

It is incumbent upon the SAA to take all steps necessary to ensure that the vulnerabilities identified during this review of the Judiciary Committee do not exist elsewhere among the Senate offices. As a result of the lessons learned during this investigation, the SAA will ask the leadership of the Senate to consider the following:

? Establishment of a technical skills assessment and certification program for current System Administrators

? A continuing technical education requirement for System Administrators

? Minimal qualification standards for new System Administrators A Computer Security Best Practices Manual for the Senate developed by the Sergeant at Arms in conjunction with the Committee on Rules and Administration

? Mandatory Ethics and Professional Responsibility training for all new employees

? Mandatory Computer Security Training for all new employees

XI. Conclusion

This investigation depended entirely on the voluntary cooperation of those who were asked to be interviewed. While investigators followed leads and interviewed many individuals as a result of learning their names during interviews, it remains possible that there are other current or former members of the Senate community who have knowledge of the open nature of the Judicary Committee computer system who have not come forward or been identified. This was evidenced most recently in press reports on March 2, 2003, when a former Grassley intern was reported to have knowledge of Committee computer security system vulnerabilities. His name was not been provided to investigators when they asked for all employees (paid, interns, and detailees) who worked for the Committee from June 2002 to the present. There are likely to be other individuals who had access to the Committee's computer system whose were not provided to investigators.

The tremendous amount of computer data in this case also leaves open the possibility that additional evidence could be discovered by investing substantially more time and money in analyzing individual workstations, print logs, and e-mails.