John W. Lainhart IV
Inspector General

Office of Inspector General
U.S. House of Representatives
Washington, DC 20515–9990

MEMORANDUM

TO: Scot M. Faulkner
Chief Administrative Officer

John W. Lainhart IV

FROM: John W. Lainhart IV
Inspector General

DATE: September 3, 1996

SUBJECT: Audit Report - House Information Resources Policies And Procedures Related To Electronic Mail Need To Be Improved (Report No. 96-CAO-07)

This report presents the results of our review of the events surrounding the April 1996 House electronic mail (E-mail) incident involving a Member's office. This review was initiated by the Committee on House Oversight's May 15, 1996 request. This initial request was expanded based on additional information provided in a June 24, 1996 memorandum from the Ranking Minority Member of the Committee on House Oversight. The objectives of this review were to (1) assess the events surrounding the improper retention and resending of old E-mail messages that had been previously deleted by the recipient, (2) assess the events surrounding the subsequent unauthorized deletion of the same E-mail messages that had been resent to the Member's office, (3) determine whether there was any political motivation or malicious intent behind the incident, and (4) identify areas for improvements to preclude unauthorized access to, and tampering with, Member, Committee, and House office data. In addition, we explored a concern raised in the June 24, 1996 request to evaluate the possibility that House Information Resources (HIR) personnel were less than candid in presenting the facts to the Federal Bureau of Investigation and HIR Security Manager. We also identified problems associated with the House E-mail problem resolution process and made recommendations to prevent recurrence.

In response to our July 17, 1996 draft report, your office generally concurred with the issues we identified surrounding the E-mail incident and both recommendations. Your office's written response is incorporated in this report and included in its entirety as an appendix. The corrective actions taken and planned by your office are appropriate and, when fully implemented, should adequately respond to the recommendations.

We appreciate your office's positive response and concurrence with the recommendations, and the courtesy and cooperation extended to us by your staff. If you have any questions or require additional information regarding this memorandum report, please call me or Craig Silverthorne at (202) 226-1250.

Attachment

cc: Speaker of the House
Majority Leader of the House
Minority Leader of the House
Chairman, Committee on House Oversight
Ranking Minority Member, Committee on House Oversight
Members, Committee on House Oversight

I. I INTRODUCTION

On May 15, 1996, the Committee on House Oversight (CHO) issued a memorandum requesting the Office of Inspector General (OIG) to review the circumstances surrounding a recent electronic mail (E-mail) incident involving the improper retention and resending of old E-mail messages that had been previously deleted by a Member office, and the subsequent improper deletion of the same E-mail messages from that Member's public E-mail box. The memorandum further asked that the OIG make any necessary recommendations to preclude unauthorized access to and tampering with the computer files of Member, Committee, and House offices. In response to this request, on May 16, 1996, the OIG tasked Ernst & Young LLP (E&Y) to perform this work since that firm had already been engaged to perform audits involving telecommunications management, security, and utilization at the House.

In a subsequent conversation with a staff member of the CHO, we were told that the Member's office had received information that the E-mail problems could be attributed to some political motivation. Further, on June 24, 1996, the Ranking Minority Member of the CHO issued a memorandum requesting that, as a part of its original May 15 request, the OIG explore an additional matter related to the Member's E-mail system. This additional matter involved a contention that HIR personnel assigned to deal with the earlier E-mail incident were less than candid in presenting the facts to the Federal Bureau of Investigation (FBI) and the House Information Resources (HIR) Security Manager.

Background

The Member Information Network (MIN) E-mail system is one of nine E-mail systems currently in use at the House. For all E-mail sent to the House from external sources, including the Internet, and E-mail outbound from the House, the House utilizes a SoftSwitch E-mail gateway, developed by Lotus Development Corporation, to serve as a translator between the House's nine disparate E-mail systems. SoftSwitch is a commercial, proprietary solution, and contains both hardware and software components. The E-mail application is comprised of Member public E-mail boxes, and an intermediate Gateway Interface File (GIF), both of which are mainframe-based. The GIF resides between the SoftSwitch and the E-mail boxes, and is a Virtual Storage Access Method (VSAM)[1] file which is used to store and forward E-mail. (The store and forward capability facilitates the routing of E-mail messages among the nine House E-mail systems.) In contrast, E-mail messages sent between House offices are handled directly by the MIN application and do not involve SoftSwitch or the GIF. The entire MIN E-mail application resides in a Customer Information Control System (CICS)[2] region on the mainframe. The MIN E-mail

[1] VSAM is an access method for direct or sequential processing of fixed and variable-length records on direct access storage devices. The records in a VSAM data set or file can be organized in logical sequence by a key field or in the physical sequence in which they are written on the file.

[2] CICS is an IBM software product that enables transactions entered at remote terminals to be processed

system and associated CICS region are maintained by HIR staff.

On Thursday, April 25, 1996, numerous old E-mail messages dated from November 14, 1995 that had been previously deleted by the Member's office were redelivered to the Member's public mail box. On Friday, April 26, the old messages were discovered by a staff member of the Member's office and immediately reported to HIR. When attempting to analyze this incident on Monday, April 29, 1996, HIR officials and a staff member of the Member's office found that the messages were missing from the E-mail box.

Concerned about the possibility of political motivation or malicious intent by unauthorized parties, the Member's office contacted the FBI's National Computer Crimes Division to conduct an investigation of the incident. As a result, the FBI conducted a preliminary investigation. In addition, the HIR Security Manager conducted a separate investigation. The FBI's investigation found no criminal intent or violation of Federal law. Therefore, the FBI did not open a case and concluded their investigation on May 17, 1996. Similarly, the HIR Security Manager's summary report cited that the incident occurred as a result of a maintenance error and that no evidence of criminal or malicious activities was found. However, the HIR Security Manager's summary report contained a suggestion to improve internal procedures and limit access to the E-mail system, which is consistent with Recommendation 1 in this report.

Objectives, Scope, and Methodology

The objectives of this review were to (1) assess the events surrounding the improper retention and resending of old E-mail messages that had been previously deleted by the recipient, (2) assess the events surrounding the subsequent unauthorized deletion of the same E-mail messages that had been resent to the Member's office, (3) determine whether there was any political motivation or malicious intent behind the incident, and (4) identify areas for improvements to preclude unauthorized access to, and tampering with, Member, Committee, and House office data. In addition, we explored an additional concern raised by the Ranking Minority Member of the CHO in a June 24, 1996 memorandum involving the possibility that HIR personnel were less than candid in presenting the facts to the FBI and HIR Security Manager. Consequently, this review was limited to investigating this particular E-mail incident. Other telecommunications issues--that is, management, economy, efficiency, and effectiveness of operations, security, utilization, and disaster recovery--are being evaluated as part of the OIG's comprehensive telecommunications audits currently underway.

concurrently by user-written application programs. It includes facilities for building, using, and maintaining databases, such as the House's E-mail systems.

Our work was primarily conducted at HIR in Washington, D.C. In addressing the incident, we focused our review on the circumstances surrounding the House E-mail events and actions of HIR staff in handling the incident, especially those actions occurring from the date of message delivery through resolution. In conducting this review, we performed the following specific tasks:

- Interviewed all HIR staff (i.e., HIR Security Manager, Integration Group Director, Distributed Systems Manager, Systems Administrator, E-mail Administrator, and MIN/Internet Administrator) involved in investigating and resolving the E-mail incident.

- Conducted telephone interviews of the Member's Press Secretary and the FBI agent who investigated this incident.

- Reviewed the investigation summary prepared by the HIR Security Manager and examined applicable HIR management policies and practices.

- Reviewed the process in place for handling E-mail messages sent to the House from external sources, including the Internet.

- Reviewed HIR's File Reorganization Unload Process (hereinafter referred to as REORG)[3] program source code.

- Observed and participated in online tests of the functionality of the E-mail system and REORG program to validate our understanding of the procedures involved.

We conducted our review in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

[3] REORG is an E-mail reorganization operation, consisting of a series of automated programs. The programs are designed to unload and sort the mail, uncatalog previous backup files, load data files, etc. This process includes steps for purging E-mail messages that have been deleted by the recipient and E-mail messages that are over a predetermined number of days old (e.g., typically 25, 30, or 60 days old).

Internal Controls

This review included evaluating the internal controls related to this specific E-mail incident. The review identified internal control weaknesses involving the administration and maintenance of the House E-mail systems, which are discussed in this report. Other internal controls related to the House E-mail systems are being evaluated as part of the ongoing telecommunications audits and will be addressed in subsequent audit reports.

Prior Audit Coverage

Since this review was intended to focus on a specific incident, there was no prior audit coverage directly related to the issues described in this report. However, the OIG previously issued three audit reports addressing security access control weaknesses involving the Member's E-mail and the House E-mail systems. These reports are summarized below:

House Computer Systems Were Vulnerable To Unauthorized Access, Modifications, And Destruction (Report No. 95-CAO-18, dated July 18, 1995): This report disclosed serious internal control weaknesses throughout all processing environments, including HIR operations and office-level systems at Member, Committee, and House office locations. One of the weaknesses addressed the need to develop and implement security controls over E-mail messages. In short, major improvements were needed to strengthen controls over the integrity, confidentiality, and availability of information and systems at the House. The report contained 19 recommendations to correct the internal control weaknesses and strengthen controls over House information resources. HIR agreed to correct the deficiencies identified and is taking corrective actions.

Internet Security Weaknesses (Report No. 95-CAO-03, dated July 18, 1995): This report noted serious weaknesses surrounding access to the House network and Member office systems via the Internet through external agencies on CapNet. The report disclosed the capability for unauthorized individuals to access Member systems and read E-mail in a Member's correspondence management system. As part of the audit, we exploited a "back door" into the House network and were able to read a Member's E-mail and other data, and send an E-mail message to the OIG posing as that Member. The report contained 10 recommendations to correct the internal control weaknesses and prevent recurrence. HIR agreed to correct these deficiencies and is taking the necessary corrective actions.

Information Systems Security Weaknesses (Report No. 95-CAO-01, dated May 3, 1995): This report noted serious weaknesses surrounding remote dial-in to House office-level systems. The report identified the capability for unauthorized individuals to access Member systems and read E-mail in a Member's correspondence management system. The report further described the ability to change outgoing correspondence in a Member's system to alter the position of the Member on a sensitive issue. The weaknesses highlighted the risks associated with dial-in access and the need for improved security over access to sensitive House computer resources by unauthorized individuals. The report contained eight recommendations to correct the internal control weaknesses and prevent recurrence. HIR agreed to correct these deficiencies and is taking the necessary corrective actions.

II. SUMMARY OF THE APRIL 26, 1996 E-MAIL INCIDENT

As discussed below, the April 26, 1996 E-mail incident that occurred in the Member's office resulted from an error during system troubleshooting by an HIR employee, and no political motivation or malicious intent was identified during this review. Nevertheless, we noted weaknesses associated with the system maintenance/troubleshooting process and HIR employee access capabilities that can compromise the confidentiality of House data. In addition, HIR did not have adequate procedures in place to resolve reported problems in an orderly manner. (See Finding and Recommendations section of this report.)

Old E-mail messages redelivered to Member's office

On Thursday, April 25, 1996, an HIR systems administrator was involved in troubleshooting performance problems within a CICS region. The MIN Mail application also resides in this CICS region. During this troubleshooting process, the HIR staff member was using a "snapshot" file, which was a subset of the November 14, 1995 production VSAM E-mail file, to facilitate the copying of standardized file attributes. (The retention and use of snapshot files are standard procedures for system maintenance or troubleshooting.) However, in addition to the standardized file attributes, the snapshot file also contained the text from actual E-mail messages from November 14, 1995. Thus, in the process of copying the file attributes from the November 14, 1995 snapshot, the actual E-mail text was inadvertently copied into the production E-mail environment. As a result, the November 14, 1995 messages were subsequently redelivered to the Member’s public E-mail box. The messages (approximately 101) were discovered and reported to HIR by a staff person of the Member’s office on Friday, April 26, 1996.

Deletion of old E-mail messages sent to Member's Office

According to HIR officials, when they attempted to analyze the problem on Monday, April 29, 1996, they found the November 1995 messages had been deleted from the Member's public E-mail box. The Member's staff confirmed that the November 1995 messages had not been deleted by anyone in the Member's office nor were they authorized for deletion by anyone in the office. The HIR systems administrator told us that the disappearance of the E-mail messages could be attributed to an automated system procedure, the REORG process, which contains a routine designed to purge deleted E-mail messages and all other E-mail messages older than

30 days. However, HIR could not produce any System Management Facilities[4] listings that would provide detailed information of the activities during the period between April 26 and April 29, 1996, and verification of the exact version of the REORG programs that ran on April 26. In the absence of such information, we could not conclusively determine how the old messages in the Member's public E-mail box were deleted.

Furthermore, during the course of the audit, we found that the Integration Group and Enterprise Computing Group personnel, as well as other HIR personnel, have the capability to access and delete Member, Committee, and House office E-mail messages without leaving an audit trail. From this perspective, it is possible that the November 14, 1995 messages could have been manually removed. Such an action, if it did occur would be contrary to existing policies of both Groups, which prohibit personnel from unauthorized access, viewing, and modification of E-mail messages (see Finding and Recommendations section of this report). The issue of other HIR personnel (i.e., personnel outside the Integration and Enterprise Computing Groups) having the capability to access the E-mail systems and data will be addressed further as part of our ongoing comprehensive telecommunications audits and discussed in the subsequent audit reports.

During this review, our work was limited to interviews and an analysis of the program source code. In reviewing the program source code, we verified that what the HIR systems administrator told us could explain the deletion of the November 14, 1995 E-mail messages. We learned that SoftSwitch puts the system date on all E-mail messages coming into the House from external sources. Typically, the system date is the message date. This same program logic could have been applied to the November 1995 messages that were inadvertently copied into the production environment. That is, when the November 14, 1995 messages originally came into the House via the Internet, SoftSwitch date-stamped the messages with the current system date--which, at that time, was November 14, 1995. The messages were then temporarily stored in the GIF, and the system dates were passed to the GIF index file. On April 25, 1996, when the November 1995 messages were inadvertently reintroduced into the GIF, the system dates of November 14, 1995 and the actual messages were passed from the GIF to the MIN application database as new messages, which were subsequently delivered to the Member. On April 26, 1996, when the REORG process was initiated, the deletion program read the November 14, 1995 system dates from the MIN database and deleted the messages. Therefore, considering the logic of the programs involved, we find it reasonable to conclude that the messages could and should have been deleted by the REORG process.

[4] The System Management Facilities is a control program feature that provides the means for gathering and recording information that can be used to evaluate system usage and activities.

Misinterpretation of information

When the Members's staff person discovered the old E-mail messages in the Member's public mail box on April 26, he immediately sent an E-mail message to HIR asking for help. On the following Monday, April 29, an employee in HIR's Integration Group called the staff member to discuss the problem. During this conversation, the HIR employee made references indicating that "trainees" or "new people" were working with the Member public E-mail boxes. During a second telephone conversation, another HIR employee stated that "the other side was messing with the E-mail." The HIR employee was referring to employees on "the other side" of the hallway, in the Enterprise Computing Group. However, based upon these two conversations, the staff member in the Member's office inferred that there was some type of political motivation behind the incident. Despite this inference, we found no indications of any political motivation or malicious intent behind this incident.

Additional issue involving HIR employees' cooperation with the FBI and HIR Security Manager

During the course of our audit, we addressed the additional concern raised in the June 24, 1996 memorandum from the Ranking Minority Member of the CHO. This concern involved the possibility that HIR personnel were less than candid in presenting the facts to the FBI and HIR Security Manager. However, we were unable to develop any evidence to substantiate this contention. We interviewed the HIR personnel involved in this incident and found them to be candid with respect to their interpretations and opinions. We compared the information they provided us with that obtained by the FBI and HIR Security Manager, and found no indications that would lead us to suspect that any of the HIR personnel were less than candid with the FBI and HIR Security Manager.

Conclusion

In conclusion, the April 26, 1996 E-mail incident that occurred in the Member's office resulted from an error on the part of an HIR employee during system troubleshooting. We further concluded that the deletion of the November 14, 1995 messages could and should have been attributed to the REORG process. However, we noted that some HIR personnel had the capability to access and delete Member, Committee, and House office E-mail messages without leaving an audit trail (see Finding and Recommendations section in this report). With respect to HIR's handling of this problem, in our view, what should have been a relatively simple E-mail problem to explain and resolve, unfortunately, was misinterpreted as an incident with partisan overtones. These conclusions are consistent with the results of two separate investigations conducted by the FBI and HIR Security Manager.

Finally, we found no indications that would lead us to suspect that any of the HIR personnel assigned to deal with the E-mail problem were less than candid in presenting information to the FBI and HIR Security Manager.

III. FINDING AND RECOMMENDATIONS

Finding: Improvements Are Needed Over E-mail Troubleshooting Processes, Policies, And Procedures

HIR's system maintenance snapshot file procedures used for system troubleshooting can compromise confidentiality of information when maintenance errors occur. Further, contrary to certain HIR guidelines, HIR did not have sufficient controls over employees' access to Member, Committee, and House office E-mail data. As a result, management has no assurance that HIR personnel will not inappropriately access, view, and modify Member, Committee, and House office E-mail data. In addition, we noted that HIR's problem resolution process was ineffective in controlling the resolution of the reported E-mail problem. In this case, the problem analysis and resolution process resulted in the communication of inaccurate information within HIR and to the Member's staff. The underlying reason attributed to the resending of deleted E-mail messages was the fact that there were no HIR policies and procedures in place to prohibit the copying or use of live data for testing or maintenance purposes. Similarly, HIR did not have a formal organization-wide policy addressing unauthorized access, viewing, and modification of E-mail messages or a requirement to hold individual employees accountable for their actions. Finally, HIR lacked a formal problem resolution process to track, elevate, and resolve E-mail problems reported by Member, Committee, or House offices.

Copies of actual E-mail messages should not be used for troubleshooting

According to HIR employees, copies of live E-mail messages, known as "snapshot files", were occasionally used to help diagnose E-mail performance problems (e.g., unexpected backlogs of undelivered messages) and to facilitate copying of file attributes. These snapshot files contain both file attribute information and actual E-mail messages. At the present, there is only one snapshot file (the one of November 14, 1995) on the system.

While it is common to use test data that is representative of actual data the system will need to process, the use of copies of live data presents the following risks:

- access to the copy may not be adequately restricted to preserve confidentiality of sensitive data, and

- the data could be erroneously copied into the production environment.

While we recognize that snapshot files may be useful for analyzing and resolving E-mail performance issues, in order to preserve message confidentiality they should not contain actual E-mail messages. Furthermore, only attribute information needs to be recorded on the snapshot files in order to perform troubleshooting.

HIR personnel should be prohibited from unauthorized access to, and modifications of, Member, Committee, and House office E-mail

HIR personnel in both the Integration Group and Enterprise Computing Group have the capability to access and delete Member, Committee, and House office E-mail messages without leaving an audit trail. These actions are inconsistent with existing group guidelines and requirements. A March 25, 1996 memorandum issued by the Integration Group Director reminded employees that they were in positions of trust as custodians of information owned by other organizations and information about the operations of other organizations. The memorandum cautioned employees on accessing and discussing such information without the consent of the data owners and without a compelling work-related need. The memorandum further reminded employees that violations of confidence or privacy intrusions of any sort would not be tolerated. The Enterprise Computing Group requires their employees to sign a "Confidentiality Statement," acknowledging that they understand the issue of preserving confidentiality of House data and agree to maintain confidentiality. The document also states that every effort is made to ensure that HIR staff is prevented from access to the content of data and communications messages. This confidentiality/accountability statement, however, has not been consistently required of employees within the group.

Furthermore, there is no formal HIR-wide policy to prohibit unauthorized access, viewing, and modification of E-mail messages or requirement to hold individual employees accountable for their actions. We were also aware that other HIR personnel, who are not in the Integration and Enterprise Computing Groups, have the capability to access the E-mail systems, files, and data. In the absence of an HIR-wide policy, management has no assurance that all HIR personnel are aware of management's position regarding appropriate and inappropriate access to Member, Committee, and House office data files. In addition, if such a policy did exist, without a separate mechanism--like requiring all HIR employees to sign a confidentiality/accountability statement--to hold individual employees accountable for their actions, management could not be assured that every employee was aware of HIR's policy and the consequences of violating such a policy.

Subsequent to the completion of our field work, the CHO passed a resolution, entitled *Electronic Communications* and dated July 31, 1996, stating that Members have a reasonable expectation of privacy with respect to their electronic communications and unauthorized interception, use, or disclosure of electronic communications in the performance of official duties is a violation of Federal law. The resolution further directed the Associate Administrator for HIR to prepare and issue policies, which ensure that electronic communications are secure from unauthorized disclosure, for approval by the CHO within 30 days. In addition, the resolution requires certain employees to execute an oath (or affirmation) of nondisclosure of private or privileged electronic communications. The policy and nondisclosure directives contained in this resolution resolve our concerns related to the issues described above. Therefore, we are not making recommendations related to these areas.

HIR's problem resolution process is not sufficiently coordinating and controlling E-mail problems reported

We determined that HIR's problem resolution process was ineffective in coordinating and controlling the resolution of the E-mail problems reported. When the delivery of old previously deleted messages was reported to HIR by a staff person of the Member's office, there were several communications between members of his staff and different HIR personnel. We found that the responsibility for the E-mail system is separated between two functional groups within HIR--the Enterprise Computing Group and the Integration Group. Each group has different responsibilities, creating the need for several HIR individuals to get involved. The confusion, indicative of the delineation of responsibilities, resulted in the dissemination of misleading or inaccurate information which, in turn, unnecessarily escalated concerns among employees in HIR and on the Member's staff.

In our view, HIR can minimize future miscommunication and premature conclusions by establishing a formal, more structured, approach for resolving problems reported by Member, Committee, and House offices. Clearly defined policies and procedures dictating how these situations should be tracked, escalated, resolved, and the manner and content of follow-up communications with the individual reporting the problem will greatly reduce the potential for dissemination of inaccurate information. In addition, specific procedures are needed to address how the problem will be tracked and monitored until resolution and timely supervisory review of problem handling and resolution.

Recommendations:

We recommend that the Chief Administrative Officer (CAO) ensure that the Associate Administrator of HIR:

1. Evaluates the necessity for using snapshot files in troubleshooting E-mail problems or whether the practice could be discontinued without causing excessive additional troubleshooting costs. At a minimum, procedures should be established to remove actual E-mail message text from all snapshot files, including the file currently on the system.

2. Develops and implements formal procedures addressing responsibilities for tracking, escalating and resolving E-mail problems, and the manner and content of follow-up communications with the individual reporting the problem. The procedures should also require timely supervisory review of staff's handling and resolution of E-mail and other

information systems-related problems.

Management Response

On July 17, 1996, the Office of the CAO generally concurred with this finding and both recommendations (see Appendix). As indicated in the response, HIR has implemented a procedure to immediately delete the snapshot files that are occasionally needed for troubleshooting, once the problem is resolved. Further, on June 10, 1996, HIR formed a consolidated House E-mail Support Team within the Enterprise Computing Group to more effectively carry out its E-mail responsibilities and functions, and improve customer service. However, in transferring staff performing House E-mail functions into the Enterprise Computing Group, the CAO elected not to transfer the MIN/Internet Administrator due to the small percentage of time required of the Administrator to support MIN mail, the technical knowledge of MIN required for the E-mail portion of the work, and the pending replacement of the MIN mail. As an alternative, the Administrator understands that House E-mail will be his highest priority work when the need arises. The Administrator will also attend regularly scheduled weekly E-mail staff meetings to stay abreast of House E-mail activities. The CAO also stated that they established a separate help desk manned by contractor personnel to better respond to users' E-mail questions and problems. He also stated that they were assessing existing weaknesses in their procedures for tracking and monitoring E-mail problems and would correct them.

Included in the response, the CAO disagreed with our view in the draft report of the functionality of the REORG program and provided additional information to clarify the functionality of the REORG program. The CAO stated that a review of the REORG program source code confirmed that the program acts on the message date and the associated comment lines in the program reaffirmed this logic. He further asserted that the REORG process would have flagged for deletion any unfiled message over 60 days old, and thereby would certainly have removed the November 1995 messages in April 1996.

Office Of Inspector General Comments

The CAO's actions are responsive and satisfy the intent of our first recommendation. Therefore, we consider Recommendation 1 closed. Further, the actions taken and planned related to Recommendation 2 are responsive and, when fully implemented, should satisfy the intent of our recommendation.

Finally, with regards to the REORG program, we received inconsistent information during the course of our audit and were unable to determine the completeness of the information and documentation we reviewed. To expedite the completion of this audit, we elected to issue the draft report to elicit a formal position from the CAO on the REORG program's operations with respect to deleting old messages. Therefore, we appreciate the clarification on the operation of the REORG program and have subsequently performed followup work to confirm the CAO's assertion. During this process, we received additional software programs supporting the CAO's statement and verified the information provided us. Based on the additional programs we reviewed, we agree that the REORG program could and should have deleted the November messages. However, with the limited information available, we were unable to verify whether the version of the program source code we reviewed was the same version executed on Friday, April 26, 1996. Nevertheless, we have revised the content of the report to reflect the information provided to us and the results of our followup work.

Scot M. Faulkner
Chief Administrative Officer

APPENDIX

Office of the
Chief Administrative Officer
U.S. House of Representatives
Washington, DC 20515–6860

MEMORANDUM

TO: John W. Lainhart IV
Inspector General

FROM: Thomas J. Simon
Director of Internal Controls & Continuous Improvement

DATE: July 17, 1996

SUBJECT: Response to Draft Audit Report – House Information Resources Policies and Procedures Related To Electronic Mail Need To Be Improved

---

We appreciate the opportunity to comment on your draft report. We deeply appreciate your efforts and are in general agreement with the findings and recommendations. A clarification and specific comments on each recommendation follow. If there are any questions or additional information required regarding this reply, please contact me.

CLARIFICATION:

House Information Resources believes there is one aspect of the report that is inaccurate. In the second paragraph under the caption *Results of the April 1995 E-mail Incident* there is the following statement:

> "We found that the program was designed to check the date the message entered the MIN system and could not recognize the actual date of the original message."

The above refers to the weekly database reorganization process and is the basis for the erroneous conclusion that the "November" records could not have been automatically deleted during reorganization and therefore must have been deleted by some other means.

Actually, the reverse is true.

The File Reorganization Unload program specifically acts on the *message date*, not the system activity date. A review of the program source code (which had not been changed since January) confirms this to be true and several lines of comments in the source code specifically spell out this logic. There is no doubt that the reorganization process would have immediately flagged for deletion any unfiled message over 60 days old and would certainly have removed November records in the April timeframe.

The confusion is easy to understand because MIN E-Mail uses the same file structure and software facilities as does all the other MIN applications which generally permit updates of records. In MIN E-Mail, however, records cannot be updated. Once a message has been sent, it cannot be altered. If it is forwarded, replied to, etc. a new message is generated and the original message is copied as part of the text of the new. If MIN E-Mail were acting on the system activity date, the messages would have been seen at the outset as April messages, not November.

RESPONSE TO RECOMMENDATIONS:

Following are House Information Resource's responses to the recommendations.

Recommendation 1:

Occasionally as part of problem resolution in MIN Mail, it is necessary for the technicians to create a snapshot copy of the House E-Mail MIN gateway file. HIR has implemented procedures in which the snapshot copy of the file will be deleted immediately upon resolution of the problem.

Recommendation 2:

On June 10, 1996 a consolidated House E-Mail Support Team was formed within the Enterprise Computing Group under the direct management of Peggy Hyland. The team was created to eliminate overlapping management, improve communication among team members, expedite problem resolution and establish consistent priorities for all team members. This objective of this team is to:

1. stabilize the e-mail system and provide the highest possible level of service to our customers
2. develop the recommendation for the messaging support system

To achieve the above objectives. the staff performing House E-mail administration and system administration of the individual mail packages have been transferred into Enterprise Computing, where the support of the central switch and gateways is performed. Due to the small percentage of time required of the MIN/Internet Administrator to support MIN mail, the technical knowledge of MIN required for the E-mail portion of the work, and the pending replacement of MIN mail, a transfer to Enterprise Computing will not be made. The MIN/Internet Administrator and his management understand that when called upon, House E-mail is to be his highest priority work assignment. The MIN Administrator attends the regular weekly E-mail staff meetings. A Help Desk, staffed with contract personnel. is being established to improve the responsiveness to users for e-mail administrative requests and problem resolution.

Existing procedures for troubleshooting, monitoring and problem tracking of House E-mail are being reviewed and will be improved where weaknesses exist. The House E-Mail Support Team has daily meetings with management and weekly meetings with HIR's Associate Administrator. Technical Service Representative (TSR) managers and other technical support personnel who may be called upon. as required. for their expert advise.