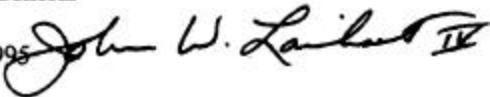


Office of Inspector General
U.S. House of Representatives
Washington, DC 20515-9990
MEMORANDUM

TO: Scot M. Faulkner
Chief Administrative Officer

FROM: John W. Lainhart IV
Inspector General

DATE: July 18, 1995 

SUBJECT: Audit Report - Continuation Of Member Services Operations Threatened
By High Operating Costs And Numerous Internal Control Deficiencies
(Report No. 95-CAO-08)

This is our final report on our evaluation of Member Services operations. The objectives of this audit were to obtain an understanding of the payroll processing functions and responsibilities; assess the adequacy of the system; assess reliability of payroll operations; and determine if there were any duplicate systems/applications in the office relating to payroll. An evaluation of the overall costs to operate Member Services versus the potential cost savings involved in contracting out these services was also conducted. In this report, we identified numerous internal control deficiencies that place Member Services at risk and made specific recommendations for corrective action. We also concluded that continuation of Member Services as a separate payroll system may not be cost-justified.

In response to our June 16, 1995 draft report, your office fully concurred with our findings, conclusions, and recommendations. The July 5, 1995 formal management response provided by the Director of Internal Controls and Continuous Improvement is incorporated into this final report and included in its entirety as an appendix.

We appreciate your office's positive response and concurrence with the recommendations and for the courtesy and cooperation extended to us by your staff. If you have any questions or require additional information regarding this report, please call me or David I. Berran 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

CONTINUATION OF MEMBER SERVICES OPERATIONS THREATENED BY HIGH OPERATING COSTS AND NUMEROUS INTERNAL CONTROL DEFICIENCIES

*Report No. 95-CAO-08
July 18, 1995*

RESULTS IN BRIEF

CONCLUSIONS

Cost Of Operations For Member Services

The current method of processing payroll for 440 Members and Delegates of the U.S. House of Representatives is not cost effective compared to contractors' estimates obtained by Price Waterhouse LLP. The cost estimates are based upon salaries and fringe benefits for Member Services employees as compared to the estimate based upon cost per check. Presuming the estimates represent near actual cost values, the Office of Finance could realize a potential savings of between \$35 and \$45 per paycheck or between \$180,000 and \$228,000 annually.

Internal Control Weaknesses

We identified numerous general and application control weaknesses that could adversely affect Member Services operations. The following illustrates the types of general control weaknesses noted in our review: computer facility controls were inadequate to reduce the risk of harm to employees and loss or damage to equipment and/or resources; a contingency plan and disaster recovery plan for Member Services has not been established that would minimize loss in the event of an unanticipated disaster or business interruption; security measures have not been implemented that would reduce the risk of users accidentally changing or destroying resources; and management has not adequately controlled the Member Services payroll check distribution process and access to check processing resources using dual controls.

The following represents the types of application control weaknesses that we identified: data integrity controls were inadequate to ensure the completeness, accuracy, and consistency of the data in the Members payroll system; a software maintenance program has not been established for upgrading the AS/400 and Liberty payroll system, and, as a result, multiple systems are utilized to process monthly payroll; segregation of duties for data entry, hardware operations, application programming, and security administration for the AS/400 hardware and Liberty application software has not been established; and unauthorized copies of word processing and

spreadsheet software are utilized for processing monthly Members payroll.

A sound internal control structure would ensure the accuracy, completeness, timeliness, and consistency of the data processed. To compensate for the identified deficiencies, Member Services has established an interdependent process to generate monthly payroll. This has created inefficiencies in the process.

RECOMMENDATIONS

We recommend that the Chief Administrative Officer (CAO) develop a proposal, for approval by the Committee on House Oversight to implement one of the following corrective actions:

Option 1: If the Office of Finance elects to procure a commercial off-the-shelf package to run Members' Payroll in-house, ensure that a system of internal controls as embodied in the recommendations contained in this report are in place and functioning, or

Option 2: If the Office of Finance elects to contract for Members' Payroll:

- (a) require certification from the selected vendor that an appropriate system of internal controls exists in the vendor's payroll processing operations, and
- (b) at a minimum, include specific language in the contract that acknowledges the Inspector General's right to audit and/or review the selected vendor's payroll processing operations.

We also recommended that, as an interim measure, certain recommendations that will correct system integrity exposures be implemented immediately, regardless of the payroll options currently being deliberated.

This report also contains numerous internal control recommendations that would not be applicable to Member Services if, as we understand, Office of Finance decides to contract for Members payroll processing. If, on the other hand, Member Services processing remains in-house, the applicable recommendations should be fully implemented.

MANAGEMENT RESPONSE

The Office of the CAO fully concurred with the findings, conclusions, and recommendations in this report. The CAO will present options for contracting Member Pay to the Committee on House Oversight for consideration at its July meeting. Internal control certification and Inspector General audit/review access will be included in any contract. The CAO identified a task group that is addressing all internal control issues with emphasis on the ones noted as priority. Action will be taken by mid-July to rectify all serious integrity exposures.

OFFICE OF INSPECTOR GENERAL COMMENTS

The CAO's response for Findings A through I is responsive and fully satisfy the intent of the recommendations. Therefore, we consider these recommendations resolved and anticipate closing them after the actions to be taken by the task group in mid-July are completed.

TABLE OF CONTENTS

TRANSMITTAL MEMORANDUM

RESULTS IN BRIEF i

I. INTRODUCTION

 Background 1

 Objectives, Scope, And Methodology 1

 Internal Controls 2

 Prior Audit Coverage 2

II. FINDINGS AND RECOMMENDATIONS

 Finding A: Member Services Payroll Operation Is Not Cost-Effective 3

 Finding B: Improvements Needed Over Computer Facility Controls 7

 Finding C: Contingency/Disaster Recovery Planning Needs To Be Established 11

 Finding D: Data Security Controls Should Be Implemented 13

 Finding E: Software Maintenance Program Is Non-Existent 18

 Finding F: Improvements Needed Over Data Integrity And Reliability 20

 Finding G: Controls over Members' Payroll Checks Need To Be Strengthened 23

 Finding H: Separation of Duties Needs To Be Enforced 25

 Finding I: Software Licensing Agreements Cannot Be Ignored 27

III. EXHIBITS

 Exhibit A: Contracting Out - Cost Comparisons 28

 Exhibit B: Summary List Of 25 Recommendations For Findings 'B' Through 'I' 29

IV. APPENDIX

 Appendix: CAO Management Response To The Draft Report 32

I. INTRODUCTION

Background

Responsibility for the disbursement of compensation for House Members was given to the Sergeant at Arms effective October 1, 1890 under 2 USC 80. Certain functions of the Sergeant at Arms were transferred to the Director of Non-legislative and Financial Services by Section 7 of House Resolution (H.Res.) No. 423, One Hundred Second Congress, on April 9, 1992. On January 4, 1995, with the enactment of H.Res. 6, One Hundred Fourth Congress, the Director of Non-legislative and Financial Services was replaced by the Chief Administrative Officer (CAO). Member Services was placed under the Office of Finance as a result of these resolutions.

Member Services provides payroll and personnel functions for the Representatives and Delegates to the House of Representatives. A separate payroll system was developed for Members in response to the special requirements for Member benefits and pay dates. Member Services consists of two permanent employees and one employee of the Sergeant at Arms who works part time operating the computer system. Salary levels for this operation are budgeted at \$190,000. Long time, dedicated staff have ensured that various personnel and payroll functions of Member Services were addressed with the attention to detail that Members of Congress expected.

The payroll system is maintained on an IBM Application System/400 (AS/400) using Liberty payroll software purchased from Broadway & Seymour, Inc. in 1989. No updates to the software have been purchased since the initial procurement. The payroll system performs basic processing of Federal and state tax withholding and deductions and allotments, however, it does not track other deduction requirements such as health and life insurance group information, retirement reporting, U.S. Treasury bond purchases, month and year to date parking benefits, and Treasury reporting requirements. Also, because of budget restrictions that prevented Member Services staff from upgrading the Liberty software, a Personal Computer (PC) based database software called DataEase is used to track and process portions of Members' payroll concurrently with the Liberty payroll system.

Objectives, Scope, And Methodology

The objectives of the Member Services Payroll Audit were to (1) obtain an understanding of payroll processing functions and responsibilities, (2) assess the adequacy of the system by testing the accuracy, completeness, timeliness and consistency of the data processed by the office and system, (3) assess reliability of payroll operations through examination of security, backup and contingency procedures, and (4) determine if there are any duplicate systems/applications in the office relating to payroll. An evaluation of the overall costs to operate Member Services versus the potential cost savings involved in contracting out these services was also conducted.

We examined a sample of payroll records and supporting documentation for December 1994 and February 1995--representing approximately 10 percent from each file--and observed and documented the payroll processing operation. We reviewed Member salaries, and re-calculated taxes, and deductions, including health and life insurance, savings bonds, allotments, thrift savings, and retirement, to determine data accuracy based on the guidelines in effect at the time of payroll processing.

We conducted our review in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. The audit work included such tests and auditing procedures as were considered necessary under the circumstances. We conducted our audit work during the period October 1994 through May 1995.

Our review included the following steps:

- Reviewing applicable government-wide internal control criteria focusing on controls in computer base systems.
- Reviewing Member Services system documentation and policies and procedures.
- Conducting interviews regarding programming and testing activities and automated controls with Member Services staff and Office of Finance staff.

We reviewed the Office of Finance and Member Services at the House of Representatives. We also contacted the General Accounting Office (GAO) to review workpapers related to prior financial statement audits of the Sergeant at Arms.

Internal Controls

During this review, we evaluated internal controls over the payroll processing in Member Services. The internal control weaknesses we identified are described in the "Findings and Recommendations" section of this report.

Prior Audit Coverage

GAO is required to conduct financial audits of the Office of the Sergeant at Arms for each six month period. The last report issued was "*House Office of the Sergeant at Arms - Periods Ended December 31, 1993 and June 30, 1993*", GAO/AIMD-95-63, dated March 1995. During these periods, appropriated funds administered by the House Office of the Sergeant at Arms, principally, salaries and benefits of House Members, were reviewed. No findings were reported related to the financial audit of the office.

II. FINDINGS AND RECOMMENDATIONS

Finding A: Member Services Payroll Operation Is Not Cost-Effective

A conservative estimate as to the annual cost to process payroll for 440 Members and Delegates of the U.S. House of Representatives--a separate payroll system that was legislatively mandated under 2 USC 80 and placed under control of the Sergeant at Arms--is \$246,145, or more than \$46 per Member paycheck. This estimate does not include general overhead, e.g. rent, equipment, hardware, software, etc., that would increase the cost per paycheck. Private payroll contractors that have been contacted by Price Waterhouse LLP (Price Waterhouse), a contractor performing a financial statement and operational audits of the House for the Office of Inspector General (OIG), have estimated that they could process the payroll for as little as \$0.79 or as much as \$9 per paycheck, per month. Using these figures, we estimate the Office of Finance could realize a potential savings of between \$35 and \$45 per paycheck or between \$180,000 and \$220,000 annually.

Costs do not support Member Services continuation of payroll processing

Member Services staff consists of three people, one of which splits her time between Member Services and the House Identification Office. Budgeted salaries for Fiscal Year 1995 for these employees and one position that has been vacant due to retirement was approximately \$190,000. Fringe benefits, expressed as a percent of salaries, represents an additional 29.55 percent¹. The chart below illustrates the costs, excluding overhead, that make up payroll processing expenses.

Salaries:	Fringe Benefits:	Total Cost:	Per Check Cost:
\$190,000	\$56,145	\$246,145	\$46.62

Member Service employees, who are not formally trained data processors, operate the computer systems with little support and guidance from management. As discussed in the findings that follow, budgetary restrictions have prevented the purchase of updated equipment, software, and peripheral supplies. Training has not been available for the staff to obtain adequate working knowledge of the systems. Manual general ledger accounts are still maintained.

While every effort has been made to use the resources available to Member Services, there are inherent limitations to the outdated systems. The entire operation is conducted from the basement of the U.S. Capitol in a physical environment that is not conducive to data processing. Notwithstanding the costs involved, the system is flawed from an internal controls perspective

¹A fringe benefit rate of 29.55 percent is used, as prescribed by the Office of Management and Budget Circular A-76, for the Executive Branch cost-benefit calculations. This Circular sets government-wide standards for comparing government costs to those of private vendors.

that has the potential to compromise the integrity of the master file and bring the entire system to a standstill. (See Findings B through I that follow.) The only compensating control that, in our view, has mitigated this situation, is the quality of the staff and their dedication to Member Services operations.

Cost comparison data developed by Price Waterhouse indicates that the unit cost per check, based upon total number of employees, is considerably lower than present costs, regardless of the option chosen.

National Finance Center ²	Vendor 'A'	Vendor 'B'	Vendor 'C'
\$110.00/Person/Year (\$9.17/Check)	\$1.25/Check	\$1.00/Check	\$0.79/Check

These figures do not include implementation costs that vary from \$4 per employee per check (Vendor B) to 12-20 percent of annual processing fees (Vendor A). In addition, these figures are based on a population of 11,000 employees--the Members population of 440 may not qualify for the same rate. All but one of these options will still require some involvement with House staff to counsel Members and input pay data. Payroll processing is one financial management function that many organizations choose to contract out. Industry statistics show that contracting out payroll processing can be cost-effective if total in-house payroll processing costs are more than \$6 per paycheck. All the organizations that Price Waterhouse contacted emphasized that the prices they were providing were approximate and that actual costs might differ. A full description of the costs and other requirements that are involved in the various contracting out options is presented in Exhibit A of this report.

Operational costs overtake internal controls considerations for the present

The eight internal control findings that follow address deficiencies that a basic system of internal controls is designed to prevent. The recommendations that we designed to correct those deficiencies, if properly implemented, would be sufficient to satisfy the requirements for an acceptable system of internal controls. However, several key events have taken place since the beginning of our audit that directly impact our final audit position with respect to Member Services. First, as a result of the OIG's May 12, 1995 report, entitled *Proposed New Financial Management System Will Not Meet The House's Needs And Should Be Terminated* (Report No. 95-CAO-02), management has decided to terminate that project and develop a comprehensive set of functional requirements for a new financial management system (FMS). In the interim, however, the House has agreed to explore options available for a new FMS including commercial off-the-shelf software packages and cross-servicing agreements with other Federal

²The National Finance Center (NFC) will not process Members' payroll unless it is combined with the rest of the House staff. Otherwise, this option is not a viable option for replacing Member Services payroll processing.

agencies. Included in the new FMS were personnel and payroll modules to handle House employee personnel/payroll needs. Management is now faced with the option of contracting out staff payroll that would eliminate the possibility of merging Members' payroll with the existing payroll system, a recommendation we thought worth exploring until now. Second, on April 6, 1995, the Associate Administrator, Office of Finance, issued a memorandum to Member Services staff indicating that their positions have been abolished and that the Office of Finance would be taking control of Member Services payroll processing until a more permanent solution could be arranged, indicating to us that contracting out Members' payroll was a viable option.

Considering these events and the cost information presented above, it is apparent that implementing all of our recommendations, some of which will undoubtedly increase the costs of Member Services' operations, may not be in the best interests of the House at this time. (Exhibit B to this report contains a summary of the recommendations associated with each finding that would be needed to implement a system of internal controls to safeguard Member Services. Recommendations marked with an asterisk represent changes that normally have a cost associated with their implementation; recommendations marked with a diamond involve serious integrity exposures that should be immediately implemented. These latter recommendations will cost little or nothing to implement and will afford some measure of security until the transition to a new system is completed.) Although a system of internal controls over Members' payroll is needed, investing additional resources, at this time, to develop a complete control structure for a system that may be replaced or contracted out is not a prudent option.

Recommendations

We recommend that the Chief Administrative Officer develop a proposal, for approval by the Committee on House Oversight, to

1. Implement one of the following corrective actions:

Option 1: If a commercial off-the-shelf package is selected to replace Members' payroll in-house, ensure that a system of internal controls, as embodied in the recommendations contained in Exhibit B, are in place and functioning, or

Option 2: If the Office of Finance elects to contract for Members' payroll:

(a) require certification from the selected vendor that an appropriate system of internal controls exists in the vendor's payroll processing operations, and

(b) at a minimum, include specific language in the contract that acknowledges the Inspector General's right to audit and/or review the selected vendor's payroll processing operations.

We also recommend that the Chief Administrative Officer:

2. Immediately implement those recommendations in Exhibit B (marked with a diamond, '•') that involve serious integrity exposures, as an interim measure, independent of the payroll options being deliberated.

Management Response

The CAO will present options for contracting Member Pay to the Committee on House Oversight for consideration at its July meeting. Internal control certification and Inspector General audit/review access will be included in any contract. A task group is addressing all internal control issues with emphasis on the ones noted as priority. Action will be taken by mid-July to rectify all serious integrity exposures.

Office of Inspector General Comments

The CAO's response for Findings B through I is responsive and fully satisfy the intent of the recommendations. Therefore, we consider these recommendations resolved and anticipate closing them after the actions to be taken by the task group in mid-July are completed.

Finding B: Improvements Needed Over Computer Facility Controls

Controls surrounding any computer operations facility require physical protection, environmental support, and management of hardware maintenance so that access is restricted and the equipment is maintained in a secure and controlled environment. Appropriate data center controls assist in reducing risk of harm to employees and loss or damage to equipment resources. During our review of the computer facility, room HB-1, that houses the Member Services operations, we noted deficiencies concerning (1) the lack of procedures for physical access, (2) ineffective environmental controls, (3) lack of preventive hardware maintenance procedures, and (4) undocumented backup and recovery procedures. These deficiencies have the potential to disrupt payroll operations, delay Members' pay, cause harm to personnel, destroy vital information, and/or interrupt operations indefinitely.

Physical access procedures

- Physical access to the combined operations and computer facility is controlled by the Capitol Police, an intrusion alarm system, and a key lock. We reviewed the authorized access list provided to the Capitol Police documenting who is authorized to activate and deactivate the intrusion alarm system and we noted that this list includes all employees of the Sergeant at Arms, including one former employee of Member Services who retired in 1994. To deactivate the alarm system and gain access to room HB-1, an employee calls the Capitol Police, provides his/her name and badge number and, upon verification, the Capitol Police operator will deactivate the intrusion alarm system. Only one full time Sergeant at Arms employee who works part time to support Members' payroll requires access to room HB-1. All other employees of the Sergeant at Arms do not have job functions that require access to this room. Additionally, there is one lock to room HB-1 and four keys manufactured for this door. These keys belong to the Member Services personnel, the Sergeant at Arms operations employee mentioned above, and a retired Member Services employee. Member Services does not have exit clearance procedures in place that would have required surrendering the key to room HB-1 and removing the retired employee from the authorized access list maintained by the Capitol Police. As a result, this particular individual has had access and could gain entry to the Member Services facility since the individual's time of retirement to the present.

During office hours, the door to HB-1 is locked. A telephone, with a dedicated telephone number located outside the door, is used to initiate entry. The Member Services staff answers the door when the telephone rings without requiring identification of the visitor prior to admittance. The door has no screening device, such as a peep hole or a one-way mirrored viewer, that would facilitate visitor identification from within. In addition, during work hours, Member Services employees have cause to be absent from room HB-1 and normal procedures do not require activation of the alarm. The door is secured by a regular key lock at these times and a note is posted on the door stating that personnel will return in a

few minutes. Procedures have not been established to safeguard the employees, sensitive data files, and equipment by preventing access by unidentified visitors or by securing the facility when it is vacant.

The Computer Security Act of 1987 (Public Law 100-235, January 8, 1988), Section 2.(a), states that "The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use". Also, Federal Information Processing Standards (FIPS) Publication 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management*, Section 5, Physical Protection of ADP Facilities, addresses the requirements for physical protection of the computer facility and establishes the process of permitting access to the facility by authorized persons while denying access to others. This publication provides action items including one for physical security as detailed below.

"Identify critical ADP areas including the computer room, data control and conversion area, data file storage area, programmer's area, forms storage area, maintenance area, and mechanical equipment room, and then provide adequate physical protection and access control."

The limited physical access controls in place for the operations and computer facility of Members' payroll is due to the small office size. No one has identified security risks beyond the use of the alarm system during non-work hours. The access lists have not been updated after staff turnover since exit clearance procedures do not exist.

Former employees are still identified as authorized, even after January 1995 updates to the list of authorized individuals. Unauthorized access could be obtained during business hours if valid personnel are not present. Inadequate physical controls could allow for improper disclosure of sensitive Member personnel and payroll information.

Environmental controls for the AS/400

- Environmental controls in place over HB-1 are inadequate. The only environmental control in place is one fire extinguisher located immediately outside the facility. There is no fire suppression system in place, such as Halon or water sprinklers. In the adjacent hallway, numerous cables are strung throughout the ceiling with no safety precautions to ensure that the cables are insulated. Also, fire and safety procedures have not been established. As a result, the staff has not been made aware of the need for an evacuation plan or additional fire suppression equipment.

In addition, there are no temperature and humidity controls in the room to protect the computer system. No backup power supplies are available to provide continuous air

conditioning or emergency lighting in the case of an emergency. Emergency power shutoff procedures that explain how to power down the AS/400 and other computer hardware in the facility do not exist.

FIPS Publication 31, Section 2.1, Fire Safety, addresses the sensitivity of computer facilities to fire damage and disruption of operations, while Section 3, Supporting Utilities, addresses the dependency of every computer facility on supporting utilities: electric power, air conditioning and other such as communications circuits, and water supplies, for its operations.

Since the Members' payroll function has historically been located with the Sergeant at Arms' office in the U.S. Capitol, the lack of standard environmental controls for computers was not considered in the office modernization efforts. The Member Services office has no preventive or detective fire suppressant system or emergency backup power supply. As a result, if a disaster of any type (i.e., fire, overheating of equipment, etc.) occurred, the risk of harm to employees and loss of equipment and data would be high.

Preventive hardware maintenance procedures

- Preventive maintenance for the AS/400 hardware equipment is not being performed on a routine basis. Currently, the Office of Systems Management (OSM) manages the maintenance agreements for the House of Representatives. However, we found that a hardware maintenance contract does exist between IBM and the House of Representatives. Though OSM routinely bills the Sergeant at Arms for AS/400 maintenance, IBM has not invoiced for AS/400 equipment maintenance.

FIPS Publication 31, Section 4.2, Management of Hardware Maintenance, addresses the importance of establishing adequate policies and procedures for management of hardware maintenance. Effective maintenance management should include: determining the optimum schedule and scope of preventive maintenance; and reporting and performing statistical analysis on hardware failures.

Office of Finance officials have not considered the implications of establishing and implementing a preventive maintenance schedule. Furthermore, even though a maintenance contract exists, it appears that Member Services is unaware that the AS/400 is covered on the House of Representatives maintenance agreement and, as a result, has not obtained routine maintenance. Without routine maintenance procedures, the potential exists for equipment failure or poor hardware performance to occur which could result in delayed monthly Members' payroll.

Backup and recovery procedures

- Backup and recovery procedures have not been established for the AS/400. Currently, if an unexpected system recovery needs to be performed, reliance is placed solely with contacting and explaining the problem to an IBM Customer Service representative. Under the current scenario, management is totally dependent on IBM Customer Service to guide them through system recovery and restore the system to normal operations.

Internal control policies and procedures that are commonly accepted throughout the government and private industry prescribe that standard procedures should be established for data processing operations covering all significant hardware processes, including restart and full recovery operations. Office of Finance officials have not established and implemented backup and recovery procedures that would ensure a complete recovery or a minimized interruption. As a result, the inability to backup and recover operations could affect monthly payroll processing and delay or prevent the Member Services' ability to generate payroll checks. Additionally, reliance on IBM Customer Service only highlights the fact that the staff has never had formal AS/400 computer operations training that would allow them to maintain the system on their own.

In summary, computer facility controls for Member Services are inadequate and a controlled environment that would prevent access to equipment and data files does not exist. Also, controls and procedures to ensure employee safety are entirely ineffective.

Recommendations

See discussion on disposition of recommendations in Finding A, pages 4 and 5.

Management Response

See discussion of management response in Finding A, page 6.

Office of Inspector General Comments

See discussion of Inspector General comments in Finding A, page 6.

Finding C: Contingency/Disaster Recovery Planning Needs To Be Established

As government and private industry organizations place more reliance on automated systems, an approved and workable contingency/disaster recovery plan becomes of paramount importance. During our review, we noted that Member Services had not established a contingency/disaster recovery plan. Member Services also had no formal procedures for the backup of critical data files and programs and for the recovery of information system services in the event of an unanticipated disaster or business interruption. Without an established and tested contingency/disaster recovery plan, Member Services cannot ensure that Members' payroll would continue to operate in the event of a disaster. The need to set a contingency plan in motion could occur at any time due to the potential threat of natural disaster, loss of power supply, terrorism, or other illegal acts. It would be fair to assume that any such unanticipated act could affect the entire U.S. Capitol complex.

The Office of Management and Budget (OMB) Circular A-130, *Security of Federal Automated Information Systems*, Appendix III.3.a.[3] mandates that "Agencies shall establish policies and assign responsibilities to assure that appropriate contingency plans are developed and maintained by end users of information technology applications. The intent of such plans is to assure that users can continue to perform essential functions in the event their information technology support is interrupted. Such plans should be consistent with disaster recovery and continuity of operations plans maintained by the installation at which the application is processed." Although not required to follow OMB mandates, these requirements provide generally accepted information systems guidance that is appropriate for any well-controlled computer facility. The contingency plan for Member Services should be established in conjunction with the House of Representatives' overall contingency plan. Member Services' operations plan should be coordinated with the House-wide contingency plan to ensure that major processing efforts required for Members' payroll operations have been identified. Also, internal control policies and procedures that are commonly accepted throughout the government and private industry organizations prescribe that procedures should be established to help protect critical files, programs, and system documentation from fire or other natural disasters. These procedures should be formally documented, periodically updated and tested, and contain the detailed steps computer operations personnel should take in the event of an emergency.

Office of Finance officials have not considered the implications of not establishing contingency/disaster recovery planning on Member Services payroll. As a result, the concern that a natural disaster (i.e., water pipe damage, power failure, fire, or electrical storms) or other situation (i.e., bomb threat, or terrorist situation) would occur that would limit or prevent access to the Member Services facility has never been considered. The potential that access to the facility, data files, and processing equipment may be delayed or unavailable in the event of a business interruption should be considered. The loss of equipment and data files may substantially interrupt or prevent normal operations or create the potential embarrassment of not being able to meet Members' payroll. Without any type of contingency/disaster recovery plan in

place, Member Services cannot ensure that a business interruption would be minimized in the event of a disaster. Failure to recover in a timely manner would significantly affect the processing of Members' payroll.

Recommendations

See discussion on disposition of recommendations in Finding A, pages 4 and 5.

Management Response

See discussion of management response in Finding A, page 6.

Office of Inspector General Comments

See discussion of Inspector General comments in Finding A, page 6.

Finding D: Data Security Controls Should Be Implemented

The concept of data security refers to the safeguards built into a system that permit control over who has access to use system devices, data, and programs and to prevent accidental or intentional change or destruction of system resources. Appropriate security measures can be implemented to reduce the risk of users accidentally changing or destroying resources. With this as background, we reviewed key controls relating to the AS/400 security configuration that should be inherent in any computer system. Based upon this review, we noted that (1) IBM-supplied security settings have not been modified since system installation in 1989, (2) the system security level setting does not adequately restrict access, (3) IBM-supplied user profile default passwords have not been changed, and (4) modifications to the system key lock have not been consistently applied. These security measures were not modified from the default values because Member Services was a single operation located in a restricted environment. However, under this security configuration, the security controls over hardware and software can be compromised resulting in a potential loss of data and system integrity.

IBM-supplied security default values

Default values that are set by the vendor to facilitate installation have not been modified since installation. For example, the default value that permits logging to the audit journal has not been turned on; the maximum number of sign-on attempts that are invalid has not been changed; and a combination of password formatting options has not been implemented to strengthen the environment.

- The default value of 'NONE' has not been changed for the AS/400 audit journal setting. With the audit journal setting not activated, transactions are not recorded. If transactions are not recorded, audit trails will not be maintained and security-related events will not be logged to the audit journal. FIPS Publication 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Section 5, Systems Security, states that "Closely allied to the access control mechanism is the ability to account for who had access to which data. The control mechanisms form the basis for reports on data usage. These reports, known as audit trails, can be designed to list all system activity, all data accesses, unusual activity, etc. Such a report can be examined to unauthorized disclosures of data." When transactions are not recorded and security-related violations are not being logged, reviewed, and followed up on in timely manner, the potential for unauthorized manipulation of data could occur. Also, an ineffective use of audit trails limits the ability to trace and document transaction logging and review inappropriate or questionable access.
- The maximum number of invalid sign-on attempts has not been changed since installation. The AS/400 allows the security officer to define the maximum number of unsuccessful sign-on attempts from one to infinity. Since Member Services has not modified the default value, there are excessive invalid sign-on attempts allowed by local and remote users. Incorrect

sign-on attempts can result from a user log-on identification (ID) that is not correct, a password that is not correct, or a user trying to sign-on a display station for which authority has not been granted. Internal control policies and procedures that are generally accepted throughout the government and private industry prescribe that the number of sign-on attempts be limited and the most commonly used standard is three. This allows three attempts to enter the correct information. Usually three attempts are enough to correct typing errors but low enough to help prevent unauthorized access. After the three attempt limit has been reached, the user ID is suspended and must be reset by the security administrator. An unrestricted number of unsuccessful sign-on attempts can result in repetitive attempts without restriction by unauthorized personnel to access the AS/400.

- Users are not forced to change their own passwords on a regular basis and are not prevented from re-using old passwords. Also, users are not prevented from selecting very short, easily guessed passwords because formatting rules are not in effect. The AS/400 security setup has many password formatting options that would make it difficult for someone to gain access to the system by randomly attempting to guess passwords. However, the default values that permit password formatting options have not been modified. Some of the fundamental components of securing computer environments include: (1) password intervals, (2) repeated use of passwords, and (3) password length. We reviewed these components for the AS/400 security setup and the results of that review are summarized below.
 - There is no expiration interval for which a password is valid. As a result, passwords are not required to be changed and can remain the same indefinitely.
 - There is no restriction to prevent a user from using the same password repeatedly for 32 password changes. IBM established the default of 32 repeats of the same password for all AS/400 systems. Using the same password would counteract the control requirement that is to prevent possible discovery of passwords by unauthorized users. A reasonable restriction on repeat passwords should be imposed to enhance security by preventing users from specifying passwords previously used.
 - The minimum number of characters required in a password is set to 1. Although the maximum number of characters has remained constant at 10, the minimum value should not be lower than 6 to administer an adequate security configuration.

Internal control policies and procedures that are generally accepted by government and private industry prescribe that access security software should be properly installed with all parameters appropriately set; i.e., a reasonable number of password attempts, time out features, length of passwords, changing passwords routinely, access privileges, etc. Without adequate data security administration, security controls over hardware and software can be compromised resulting in a potential loss of data and system integrity.

According to Member Services staff, the primary decision not to modify the default values rests with a joint decision between IBM and the Sergeant at Arms. This decision was based on a recommendation from IBM that since Member Services was a single operation located in a

restricted environment, the default settings would be adequate.

System access controls

The system security level currently specified for the AS/400 does not adequately restrict access. The AS/400 supports four global security levels that define the degree of security checking performed by the operating system: the first level, indicating no security; the second level, indicating sign-on security; the third level, indicating resource security; and the fourth level, indicating system integrity. The system security value assigned is set to the sign-on security level (the second level).

The AS/400 second level security is configured to activating password and menu security and requiring a user ID. This level allows users to have system-wide access to all objects and does not require the resource and operating system security features to be activated. This security level may be appropriate if special authorities have been removed from user profiles, and if users are restricted to menus limiting their capabilities to those necessary to perform their defined job functions. However, our review of user profiles indicates that access to special authorities has not been restricted. Special authority allows a user to perform system control operations, such as saving the system, controlling other users' jobs, using the system service tools, controlling spooled files, and creating user profiles. Also, the sign-on security level is a security risk because, by default, the system gives the user authority to access or delete any object on the system after sign-on.

Properly administered access privileges are an inherent part of internal control policies and procedures that are generally accepted by government and private industry. Access security software should be properly installed with all parameters appropriately set, including access controls.

The primary reason for the current security configuration is that management has not been adequately trained to perform the data security administration functions for a mid-size computer system. As a result, management has not adequately considered global security considerations to ensure that access to system and data libraries is restricted and that access has been granted on a need to know basis. Therefore, the system security level is not set at a sufficient level to provide an appropriate level of security. Inadequate security configuration compromises data and system integrity, access to data and system files and permits the potential for improper use of Members' payroll.

IBM-supplied passwords

We tested each of the six IBM-supplied user profile using the default passwords published in the AS/400 security documentation. Five of the six user profile passwords had not been changed since the original system installation in 1989. As a result, OIG staff was able to browse, add, delete, and change any record in the entire Members' payroll system and any system value for the AS/400. Fortunately, the modem attached to the AS/400 was inoperable and dial-in was not possible. As a result, access to Member information, by way of the default passwords, was not possible since external entry to the system was inoperable.

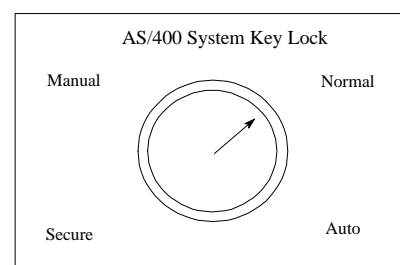
The AS/400 operating system is shipped from the factory with 20 predefined user profiles. These user profiles are used for job responsibilities for the security officer, full service functions to display and alter, basic service functions, programmer, work station user and system operator roles. Fourteen are internal profiles whose password prevents anyone from using them to sign-on to the system. The other six user profiles are intended to be used to sign-on to the system. Each of these six is given the same password as the profile user ID and these profile names and passwords are clearly printed in the AS/400 documentation. Upon system installation, the six IBM-supplied user profile passwords should be changed whether or not the user profile is used.

Internal control policies and procedures that are generally accepted within the government and private industry, and included in IBM's AS/400 documentation, recommend that passwords should be changed for the IBM-supplied user profiles as soon as the system is received.

The primary reason for the lack of customization for the security configuration is that management has not been adequately trained to perform the data security administration responsibilities for a mid-size computer system. As a result, management has not adequately considered global security considerations to ensure that access to vendor supplied log-on IDs had been restricted. Consequently, Members' payroll information could have been severely compromised if access to the IBM-supplied user profiles was permitted through an operable modem.

System key lock maintenance

The AS/400 is equipped with a four-position system key lock (manual, normal, auto, secure). Each of the positions allows for a different level of system control. The system key lock is used to limit the functions that can be performed from the system panel. The system panel includes the computer's control panel, the main power switch, and the manual system restart button. These buttons and switches can



be used to physically override or abort logical operations (i.e., switch off the computer or re-start the system).

At the onset of the audit, the system key lock was set to 'manual'. During the latter portion, we noted that the system key lock was set to normal. In response to our questions, Member Services personnel told us that the lock setting is positioned to accommodate what they are doing with the system at any given point in time. However, we found that procedures do not exist that would support the change in the system key lock setting. Member Services staff change the setting based on instructions from IBM personnel. Also, the system keys are physically kept in the lock and are not maintained in a secure location.

With the system key lock in the 'manual' position, the AS/400 can be switched on and off by anyone who has access to the main power switch. In addition, in the 'manual' position, a user is able to select a different initial program load (IPL, i.e., system startup) or use dedicated service tools to bypass AS/400 security settings, such as an exclude feature. With the system key lock in the 'normal' position, the ability to manually IPL and access the main power switch is restricted. Also, access to dedicated service tools is prevented. With the system key lock positioned to either 'auto' or 'secure', users are prevented from manually starting the system or using dedicated service tools. 'Secure' is the most protected setting; however, if there are no remote users, 'auto' provides the same level of security as 'secure'.

Internal control policies and procedures that are in place throughout the government and private industry support setting the security key lock switch to the 'secure' or the 'auto' position, and removing the key from the AS/400 system. The key should be kept under tight physical and procedural controls. The key lock switch setting should be verified routinely by visual inspection. Based upon discussions with staff, we learned that the system key lock has only been changed by IBM personnel when they are physically in the facility performing maintenance on the equipment. However, this has not been performed in several years. System administration and logical controls designed to ensure authorized access to sensitive data are inadequate.

Recommendations

See discussion on disposition of recommendations in Finding A, pages 4 and 5.

Management Response

See discussion of management response in Finding A, page 6.

Office of Inspector General Comments

See discussion of Inspector General comments in Finding A, page 6.

Finding E: Software Maintenance Program Is Non-Existent

A software maintenance program has not been established for upgrading the AS/400 and Liberty payroll systems. The original operating and application software purchased in 1989 has never been upgraded. Although software maintenance has been budgeted, management has never approved the allocation of funds for software upgrades. Improvements to application software could alleviate duplication of efforts by allowing the system generated functions and calculations to process the required information. The inflexibility of the "as is" vendor software, coupled with the budgetary constraints, has forced Member Services staff to utilize a parallel, PC-based database software (DataEase) system, to track and process Members' payroll concurrently with the Liberty payroll system. However, when multiple systems are used for processing any application system, controls over the source of entry are diminished. A single source of entry provides application integrity whereby each originating and processing point can be identified and maintained in a controlled environment.

The payroll system performs basic processing of Federal and state tax withholding and deductions and allotments. However, it does not track other deduction requirements such as health and life insurance group information, retirement reporting, thrift savings, and U.S. Treasury bond purchases; nor does it track Treasury reporting requirements. Furthermore, the Liberty payroll system does not accumulate year to date parking benefit information and, as a result, this information is calculated in the DataEase system and reentered into the Liberty payroll system for payroll processing.

The Paperwork Reduction Reauthorization Act of 1986 requires Federal agencies to periodically evaluate and, as needed, improve the accuracy, completeness, and reliability of data and records contained in Federal information systems. In order to achieve this, attention must be paid to the formulation and execution of a software maintenance plan.

Member Services staff explained that funding for software upgrades was budgeted but an expenditure was never approved by the Sergeant at Arms due to dollar restrictions. As a result, the staff has had to resort to unusual means (i.e. parallel, complimentary processing) which has proven to be particularly effective, although redundant and therefore wasteful, in processing Members' payroll. Inadequate software management has led to the use of parallel systems to process payroll, thus decreasing the controls over data entry.

Recommendations

See discussion on disposition of recommendations in Finding A, pages 4 and 5.

Management Response

See discussion of management response in Finding A, page 6.

Office of Inspector General Comments

See discussion of Inspector General comments in Finding A, page 6.

Finding F: Improvements Needed Over Data Integrity And Reliability

Data integrity and reliability provide for greater useability of data to achieve the purpose of the system. In testing controls over data integrity, we sought to review the completeness, accuracy, and consistency of the data in the system. Completeness of the data refers to the presence of all required data elements, while data accuracy establishes whether the data values have been entered and processed correctly. Data consistencies indicate proper relationships between related data elements and related records and files. All of these factors help to confirm that data generated from the system is reliable and useable.

The importance of data integrity has been addressed through the establishment of standards to control the factors affecting integrity and reliability of data. GAO's *Standards for Internal Controls for Federal Agencies* requires proper classification of transactions and events. "Transactions and other significant events are to be promptly recorded and properly classified." GAO's *Evaluating Internal Controls in Computer-Based Systems* requires that "on-line data validation and editing should be performed as early as possible in the transaction processing cycle to ensure that errors are detected and corrected quickly. Transactions and data fields should be edited for valid characters, sign, format, content, etc. This editing should be on all data fields even though an error may have been detected in an earlier field of the same transaction."

OMB's *Model Framework for Management Control Over Automated Information Systems* establishes control requirements for application systems. These include:

- Transactions are valid--the information system must process only data that represent legitimate events.
- Information is complete--all valid data, and only those data, are to be processed by the information system.
- Information is accurate--data must be free from error during all phases of processing, within defined levels of tolerance.

We selected two judgmental samples from the payroll records of December 1994 and February 1995--approximately 10 percent from each file--to assess the quality and reliability of the data processed. We reviewed Member salaries and recalculated taxes and deductions, including health and life insurance, savings bonds, allotments, thrift savings, and retirement. Using guidelines in effect at the time of payroll processing, data accuracy for most data fields was high. We identified a considerable number of errors but they all fell below an acceptable error rate of two percent for both samples.

However, state tax withholdings for states tested, that had a standard deduction or allowance, were not always correct. Of the 45 sampled Members for December 1994 and the 50 sampled Members for February 1995, we determined that Massachusetts, Maryland, and Georgia taxes

were withheld at a higher rate than required in these periods. Our sample included one Member from Massachusetts, one from Maryland, and two from Georgia. As a result of our recalculations, we identified differences resulting from the tax withholding on the standard deductions. In other words, income that should not be taxed under the state tax codes was included in the tax calculations. Projecting the differences to the twenty-nine Members from these states, we identified approximately \$3,670 being overwithheld annually.

We found that for states not requiring income tax, Member Services consistently entered the same dependent deductions for the state withholding fields as were identified on the Federal withholding and allowances form (W-4). Although this does not affect the accuracy of net pay for the Members, data maintained in the AS/400 does not match the supporting documentation in the Member files.

In addition, the deductions from Members' gross pay were not consistently reported. For example, thrift savings deductions were reported in both the 401K deduction field and the Thrift Saving deduction field. Also, inconsistencies in the reporting of the thrift savings amount were discovered. For five of the ninety-five Members sampled, the thrift savings amount reported was actually the amount for Federal Employee's Retirement System (FERS) retirement. Furthermore, thrift savings deduction amounts were not accurately labeled for eight of ninety-five of the Members in our combined sample and in one instance we found thrift savings identified as an allotment.

Furthermore, for Members of the One Hundred Third Congress that received two days pay in 1995 in compensation for the remainder of their term of office, Member Services opted not to withhold Federal or state income taxes. This was done so that Member Services did not have to record the information on the DataEase database system used to track tax withholdings. The new Congress was sworn in on January 3rd, thus requiring compensation for the departing Members for the first two days of the year. Due to the extensive time required to process documents for the newly elected Members, Member Services minimized the time involved in processing the January 1 - 2, 1995 payroll by eliminating the need to submit tax data and withholding amounts to the Internal Revenue Service and the state tax offices. Officials in Member Services stated that this practice had been followed for previous Congresses and they had never considered the effect on data accuracy. The amount of tax liability for any one Member was not significant.

Member Services employees cannot access the source code to change the calculations and have not received training to obtain the technical expertise needed to understand system calculations and properly update tax tables for withholding amounts. In addition, no application support was provided to the staff to accommodate system problems, such as the inconsistencies of Members' deductions.

In summary, due to the inconsistencies in which the data is processed, the Office of Finance

cannot be assured that the Members' payroll is accurately computed. Furthermore, the inconsistency of the reporting of deduction amounts creates the potential for thrift savings and allotments to be reported incorrectly. Also, the decision not to withhold Federal or state taxes for Members who received two days pay in 1995, while not financially significant, creates a situation of underremittance of tax liability by these Members. Therefore, the reporting of net income for tax purposes, as well as withholdings for Federal and state taxes, may not be accurate.

Recommendations

See discussion on disposition of recommendations in Finding A, pages 4 and 5.

Management Response

See discussion of management response in Finding A, page 6.

Office of Inspector General Comments

See discussion of Inspector General comments in Finding A, page 6.

Finding G: Controls Over Members' Payroll Checks Need To Be Strengthened

Management is not adequately controlling Member Services' payroll check distribution process and access to check processing resources, using dual controls. In November 1994, the check signing machine and key, signature stamp, and blank checks were physically located in the Member Services facility. We reported this as an exposure to the Office of Finance, who took immediate corrective action to physically relocate and secure the equipment in Room 140 of the Cannon Building. We included an assessment of their actions during this phase of the review to determine their effectiveness. As a result, we determined that: (1) the vault lock combination in Room 140 of the Cannon Building has not been changed in at least 2 years; (2) the signature stamp for signing Members' payroll checks is stored in the same area as the check printing machine; (3) backup tapes for monthly check data are stored in an unsecured box in the vault; and (4) separation of duties is not established for vault access and access to the check resources. In addition, no independent review of the check process is performed to ensure the integrity of checks used and processed.

GAO's *Standards For Internal Controls in the Federal Government* requires that key duties and responsibilities in authorizing, processing, recording, and reviewing transactions be separated among various individuals. In addition, access to resources and records is to be limited to authorized individuals, and accountability for the custody and use of resources is to be assigned and maintained. These standards also require periodic comparisons of the resources with the recorded accountability to determine whether the two agree.

Management has not ensured that duties of key personnel in the Member payroll check process are adequately separated and that the check process is administered under dual controls. Also, management has not established and implemented adequate procedures to ensure that access to Member payroll check resources is limited to authorized persons acting within the scope of their authority. In addition, no process or procedures for independent review or off site storage of payroll back up tapes have been established or implemented.

Due to the lack of dual controls and separation of duties over the Member payroll check process, the check signing machine by unauthorized officials can be used to issue checks; House employees that no longer need access can access Members' payroll check resources; unauthorized checks can be issued to inappropriate individuals and for inappropriate amounts; and historical data for Member payroll check processing is not secure. Inadequate controls over checks could allow for the misappropriation of assets.

Recommendations

See discussion on disposition of recommendations in Finding A, pages 4 and 5.

Management Response

See discussion of management response in Finding A, page 6.

Office of Inspector General Comments

See discussion of Inspector General comments in Finding A, page 6.

Finding H: Separation Of Duties Needs To Be Enforced

Separation of duties is based on the concept of the division of labor or tasks so that several people will be performing several tasks and not one person will be doing all tasks. This provides checks and balances in the system to ensure that one person's work is verified by another person. In computerized application systems, separation of duties not only involves the division of tasks among people, but the division of tasks among automated processing steps. With regard to Member Services, duties have not been separated for the data entry, hardware operations, application programming, and security administration functions for the AS/400 hardware and Liberty application software. These duties are performed by one individual whose primary responsibility is in Identification Services for the Sergeant at Arms. If the total Members' salaries were not fixed, the potential for collusion would exist since the ability to enter data, change code, and operate the computer system and PCs is combined. Also, given that the security administration function can add, change, and delete user profiles, any type of system operation could be performed at any time.

We realize that in Member Services, which is a two full-time and one part-time employee office, an ideal condition of separation of duties may not be possible. In these instances where office size limits or prevents management from taking advantage of this control, compensating controls such as next line supervisory review or use of independent monitors can be very effective and offset the limited controls that otherwise exist. In this instance, a compensating control would be the degree that supervisory review is performed to ensure that one person is performing his/her responsibilities in a proper manner. For this operation, the only compensating control is the control total verification of payroll information between the Liberty application software system and the PC-based system. However, verification of control totals does not ensure the accuracy and validity of any individual payroll records contained in the system.

GAO's *Standards for Internal Controls in the Federal Government* establishes requirements for separation of duties. The requirements specify that "duties and responsibilities should be assigned systematically to a number of individuals to ensure that effective checks and balances exist." This necessitates that job functions for data entry, hardware operations, application programming and security administration should be segregated.

As described above, only two full-time employees and one part-time employee have been assigned the responsibility for performing the Member Services payroll function. There are no additional employees available to separate the job functions. Due to the size of the Member Services staff, separation of duties is not adequate to ensure that errors and irregularities are promptly identified and corrected. In addition, there are no acceptable compensating controls in place to offset the exposures created by the lack of separation of duties.

Recommendations

See discussion on disposition of recommendations in Finding A, pages 4 and 5.

Management Response

See discussion of management response in Finding A, pages 4 and 5.

Office of Inspector General Comments

See discussion of Inspector General comments in Finding A, page 6.

Finding I: Software Licensing Agreements Cannot Be Ignored

Unauthorized copies of word processing, spreadsheet, and database software are utilized for processing monthly Members' payroll. PC-based software for correspondence and reconciliations has been budgeted, but management never approved the allocation of funds. As a way around this budgetary blockade, staff brought software from home to accommodate day-to-day word processing needs for minor correspondence and document preparation and spreadsheet software for accumulating year to date parking benefit information. The DataEase database software, used to track taxes, health insurance, retirement, and thrift savings deductions, was not licensed to Member Services. The DataEase software was licensed to the Sergeant at Arms and copied by Member Services to meet the need for tracking the deductions. As a result, Member Services is in violation of software licensing agreements.

Internal control policies that are generally accepted by government and private industry require standard procedures be established to prohibit the use of any unauthorized, unlicensed copies of software.

Member Services staff included a request for \$50,000 for operating expenses in its Fiscal Year 1994 budget submission that was approved but not authorized for expenditure by the Chief Administrative Officer. Without realizing that they were violating software licensing agreements, Member Services staff turned to their own resources to obtain the needed software in order to meet Members' payroll operational needs.

Controls surrounding the use of unlicensed software is inadequate. The use of unauthorized software exposes the Office of Finance to the possibility of a lawsuit by the vendors for illegal use of their software.

Recommendations

See discussion on disposition of recommendations in Finding A, pages 4 and 5.

Management Response

See discussion of management response in Finding A, page 6.

Office of Inspector General Comments

See discussion of Inspector General comments in Finding A, page 6.

Exhibit A**Contracting Out - Cost Comparisons**

	NFC	Vendor A	Vendor B	Vendor C
Unit cost	\$110/person/ year	\$1.25/check	\$1.00/check	\$.79/check
Annual processing fees (biweekly)*	\$1,210,000	\$357,500	\$286,000	\$225,940
Annual processing fees (monthly)*	N/A	\$165,000	\$132,000	\$104,280
Implementation costs	Varies	12%-20% of annual processing fees	\$4/employee	Varies
Client system requirements	3270 connection	Novell network with Netware, IBM-compatible PCs	Novell network with Netware, IBM-compatible PCs	IBM-compatible PCs with modem
Payroll distributed	Biweekly	Monthly or biweekly	Monthly or biweekly	Monthly or biweekly
House staff required	To counsel employees and input pay data	To counsel employees and input pay data	\$4/check to outsource	To counsel employees and input pay data
Access charges	Included	Included	N/A - client owns data	N/A - client owns data
Payroll re-run charges	Included	Included	N/A - system checks built in	N/A - system checks built in
Tax filings	Included	Included	\$1.25/check	Included
Postage	Included	\$.37/mailed check	Included	Included
Checks printed at	Treasury	Vendor or client	Vendor or client	Vendor
* Based on 11,000 employees.				

Source: Price Waterhouse LLP

Exhibit B (3 pages)

SUMMARY LIST OF 25 RECOMMENDATIONS
FOR FINDINGS 'B' THROUGH 'I'

Finding B:

We recommend that the Chief Administrative Officer direct the Associate Administrator, Office of Finance to:

- (1) Implement adequate security measures, including (a) timely updating of authorized individuals and adequate accounting of keys, to ensure that improper disclosure of sensitive Member information will not occur and (b) limiting access to Room HB-1 to only those individuals whose specific job functions require such access.
- (2)* Establish and implement adequate environmental controls and procedures to ensure the safety of office personnel and to minimize potential loss of equipment, data, and Member information.
- (3)* Implement a vendor preventive maintenance schedule to reduce potential equipment failure or interruption which may delay monthly distribution of Members' paychecks.
- (4)* Establish and implement backup and recovery procedures to ensure that computer operations, for significant hardware processes, can continue uninterrupted.

Finding C:

We recommend that the Chief Administrative Officer instruct the Associate Administrator, Office of Finance to:

- (1)* Establish a business resumption and contingency plan and assign responsibilities to appropriate individuals.
- (2)* Ensure that Member Services disaster recovery policies and procedures are developed, routinely tested, and adequately maintained.

Finding D:

We recommend that the Chief Administrative Officer instruct the Associate Administrator, Office of Finance to:

- (1) Review and evaluate the entire security administration functions of the AS/400.
- (2)❖ Modify system installed default values to reflect a secure and controlled environment.
- (3)❖ Modify the system security level so that access is adequately restricted and system integrity

Legend: * represents recommendations that normally have a cost associated with their implementation.

• involves recommendations where serious integrity exposures exist and should be immediately implemented.

can be achieved.

- (4)❖ Change the IBM-supplied user profiles default passwords.
- (5)❖ Develop and implement procedures for monitoring the system key lock as well as the physical security of the keys.

Finding E:

We recommend that the Chief Administrative Officer instruct the Associate Administrator, Office of Finance, to obtain technical assistance to help Member Services staff:

- (1) Review the payroll process and application documentation in order to implement application program changes to eliminate the processing on parallel systems.
- (2) Evaluate current and future system requirements and upgrade system software to meet the requirements of the House of Representatives.

Finding F:

We recommend that the Chief Administrative Officer instruct the Associate Administrator, Office of Finance, to:

- (1)❖ Obtain qualified assistance to help Member Services staff review the source code and related data for state tax withholding to ensure the accuracy and reliability of the formulas and data related to tax deductions;
- (2)❖ Direct Member Services to implement procedures to ensure that taxes are withheld from formerly elected Members during transition periods.
- (3)❖ Ensure that thrift savings and other deductions are properly identified.

Finding G:

We recommend that the Chief Administrative Officer instruct the Associate Administrator, Office of Finance, to:

- (1) Establish and implement adequate procedures to separate duties and responsibilities over the member payroll check process and implement dual control for check processing procedures.
- (2) Limit access to resources to authorized individuals and periodically monitor and maintain currency of authorizations.
- (3)❖ Establish periodic combination lock changes for the Finance vault, particularly when key individuals change jobs.
- (4)❖ Ensure that backup tapes for monthly payroll are stored in an off-site location with adequate security.
- (5) Implement procedures so that an independent review of checks be performed to ensure the

Legend: * represents recommendations that normally have a cost associated with their implementation.

• involves recommendations where serious integrity exposures exist and should be immediately implemented.

accuracy of the check log and integrity of checks processed.

Finding H:

We recommend that the Chief Administrative Officer instruct the Associate Administrator, Office of Finance, to obtain technical assistance to help Member Services staff:

- (1) Review the responsibilities between the data entry, hardware operations, application programming, and security administration functions for the AS/400 computer system and Liberty application software.
- (2)❖ Identify and implement compensating controls that would improve separation of duties for each job responsibility.

Finding I:

We recommend that the Chief Administrative Officer instruct the Associate Administrator, Office of Finance, to:

- (1)❖ Determine the extent and eliminate the use of unlicensed software in Member Services.
- (2)❖ Implement procedures to ensure compliance with copyright laws and prevent the use of unauthorized software.

Legend: * represents recommendations that normally have a cost associated with their implementation.

• involves recommendations where serious integrity exposures exist and should be immediately implemented.

APPENDIX

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

APPENDIX

MEMORANDUM

TO: Robert B. Frey III
Deputy Inspector General

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

DATE: July 5, 1995

SUBJECT: Draft Audit Report - Member Pay

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. Specific comments on each recommendation follow. If there are any questions or additional information required regarding this reply, please contact me at (202) 226-1854.

Finding A

Recommendations 1& 2: Options for contracting Member Pay will be presented to the Committee on House Oversight for consideration at its July meeting. Internal control certification and Inspector General audit/review access will be included in any contract.

Recommendation 3: A task group is addressing all internal control issues with emphasis on the ones noted as priority. Action will be taken by mid-July to rectify all serious integrity exposures.

Findings B through I: A task group is addressing all internal control issues. Because it is anticipated that the CHO will accept the CAO recommendation to contract out Members' payroll services by October 1, 1995, action will probably not be required on items other than the most serious. A meeting will be scheduled for mid-July with the Inspector General to review accomplished and proposed actions.