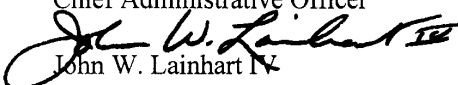


John W. Lainhart IV
Inspector General

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

TO: James M. Eagen III
Chief Administrative Officer

FROM: 
John W. Lainhart IV
Inspector General

DATE: December 9, 1998

SUBJECT: Audit Report - The Office Supply Service's Current Automated System
Does Not Meet The Needs Of The House (Report No. 98-CAO-16)

This is our final report on the Office Supply Service's Inventory/Accounting Management System. The objectives of this audit were to evaluate the effectiveness of the system and assess the accuracy, completeness, and reliability of data processed by the current Multiple Computer Business Applications (MCBA) system. In this report, we discuss system inadequacies, including the lack of functionality to accomplish essential tasks and inefficiencies affecting Office Supply Service's ability to carry out its operational responsibilities. The report also describes problems associated with software change, logical access, and operational controls surrounding the MCBA system, as well as, the integrity and reliability of data processed by the system. Accordingly, we made specific recommendations for corrective actions with respect to each identified problem.

In response to our June 12, 1998 draft report, your office concurred with our findings and recommendations. The October 14, 1998 management response is incorporated in this final report and included in its entirety as an appendix. The corrective actions taken and planned by your office are appropriate and satisfy the intent of our recommendations. Further, the milestone dates provided for implementing corrective actions appear reasonable.

We appreciate 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 Robert B. Frey III 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

THE OFFICE OF SUPPLY SERVICE'S CURRENT AUTOMATED SYSTEM DOES NOT MEET THE NEEDS OF THE HOUSE

*Report No. 98-CAO-16
December 9, 1998*

RESULTS IN BRIEF

CONCLUSIONS

Since its implementation in 1993, the Multiple Computer Business Applications (MCBA) system records and processes Office Supply Service's (OSS) supply store and gift shop inventory and accounting management activities. OSS relies on the MCBA system to support critical functions such as purchasing, inventory management and accounting. Despite the many MCBA system functions utilized by OSS, the current system does not adequately fulfill the needs of the House. Specifically, the MCBA system is not Year 2000 compliant. Further, we noted system inadequacies including the lack of functionality to accomplish essential tasks and inefficiencies in existing processes. This has required OSS personnel to manually carry out essential functions that could be automated. Inefficiencies, such as duplicate data entry and maintenance of similar data elements with different values between the MCBA system and the Federal Financial System (FFS), increase the potential for errors. As a result, OSS cannot be as efficient and effective as it could be in carrying out its operational responsibilities.

OSS's MCBA system does not have adequate software change, logical access, operational, and environmental controls. Consequently, the House cannot be assured that the inventory and accounting-related data is accurate, complete, and valid. Further, without adequate procedures to ensure computer system operational continuity, availability, and reliability, the House may not be adequately prepared to quickly recover from unforeseen disruptions, such as a prolonged outage or damage to the system and its data.

While OSS has established controls to assure the integrity (i.e., accuracy, completeness, and validity) of the MCBA data, current practices can be fine-tuned to improve integrity of this data. In particular, procedural changes surrounding MCBA data entry and adjustments impacting inventory quantities can minimize erroneous data. Inaccurate and incomplete inventory quantities in the system can cause the system to overstate or understate inventory quantities on hand. Without strengthening controls over MCBA data, OSS may not be able to rely on the data maintained within the application for decision-making purposes.

RECOMMENDATIONS

We recommend that the Chief Administrative Officer: (1) assign qualified resources and establish a level of effort work plan with implementation dates for the implementation of a Year 2000 compliant commercial-off-the-shelf solution to replace the MCBA system; and (2) validate

high-level requirements identified in this report, conduct more detailed analyses, and rank and select the most cost-effective COTS solution for meeting OSS's needs.

In addition, we made nine other recommendations aimed at improving internal controls and the integrity of data contained in the MCBA system. Specifically, we recommend that the Chief Administrative Officer: (1) document and implement policies and procedures requiring a comprehensive process for tracking, testing, and documenting all changes/modifications to the MCBA system, as well as any future replacement; (2) establish and implement a security policy, which addresses data sensitivity, data ownership, password administration requirements, and responsibilities for approving and periodically reviewing access levels, consistent with the risk of loss; (3) develop, document, and implement a disaster recovery/contingency plan for the MCBA system, and any future replacement; (4) perform an assessment of the current MCBA computer environment to identify the controls necessary to adequately protect computer assets and implement the required controls resulting from the assessment; (5) provide security awareness training to current MCBA users and the system administrator; (6) designate and train a back-up person to the system administrator; (7) establish procedures to ensure that sale clerks scan individual items, at the time of sale, into the POS system to ensure that inventory items are correctly reduced in the MCBA system and require the sales manager to review all sales for items that are not scanned individually through the POS system on a daily basis; (8) enforce compliance with OSS practice of recounting all items when the unit cost of items changes; and (9) require the inventory control supervisor to obtain sign-off, from the Director of Office Supply Service for all inventory system adjustments.

MANAGEMENT RESPONSE

In the Chief Administrative Officer's October 14, 1998 response to our draft report, the CAO concurred with our findings and all 11 recommendations (see Appendix). According to the response, the Associate Administrator of Media and Support Services recently established a MCBA System Review Team and assigned responsibility for completing tasks, which will culminate in a recommendation for a Year 2000 compliant COTS solution to replace or upgrade the MCBA system. Detailed task work will include validating high-level requirements identified in this report and conducting more detailed analyses. The team will submit its findings to the CAO by January 15, 1999.

In addressing the other nine recommendations, corrective actions were taken or planned to improve internal controls and the integrity of data contained in the MCBA system. According to the response, actions were completed for five of the nine recommendations and included: (1) conducting an assessment of the current MCBA computer system environment and, based on the assessment, implementing controls to protect the assets contained in the computer room; (2) completing security awareness training for its employees; (3) establishing procedures to ensure that sales clerks scan individual items at the time of the sale and the sales manager regularly reviews edit reports to ensure compliance with this policy; (4) establishing procedures requiring: (a) all receiving staff to re-count all supply items when the unit cost of the item changes, (b) all receiving staff to prepare a daily count sheet for new items received into inventory, and (c) the receiving and sales floor supervisors sign off on the daily count sheets and periodically verify them; and (5) requiring sign-off from the Director of Office Supply Service

for all inventory adjustments.

Other initiatives are underway or planned for addressing the remaining four recommendations. These include: (1) documenting all changes and modifications to the MCBA system, and preparing a comprehensive list of procedures for tracking, testing, and documenting all modifications to the system; (2) developing and completing a comprehensive security policy; (3) finalizing a complete disaster/contingency plan for the MCBA system; and (4) preparing a proposal, for submission to the CAO, to establish a Senior Systems Engineer position within House Information Resources (HIR) to support the MCBA system and then designating another HIR staff to serve in the back-up role. These initiatives are scheduled for completion by February 15, 1999.

OFFICE OF INSPECTOR GENERAL COMMENTS

The actions taken and planned by the CAO are responsive to the issues identified and, when fully implemented, should satisfy the intent of the recommendations. Based on the actions completed, we consider 5 of the 11 recommendations closed (see findings B and C in this report). Further, the milestone dates provided for completing actions on the remaining recommendations appear reasonable.

This Page Intentionally Left Blank

TABLE OF CONTENTS

TRANSMITTAL MEMORANDUM

RESULTS IN BRIEF

I. INTRODUCTION

Background1
Objectives, Scope, And Methodology2
Internal Controls3
Prior Audit Coverage3

II. FINDINGS AND RECOMMENDATIONS

Finding A: Steps Need To Be Taken To Implement An OSS Inventory/Accounting
Management System Which Will Meet The Needs Of The House 5
Finding B: Inadequate Information Technology Controls Could Hamper
OSS Operations10
Finding C: MCBA Data Integrity Can Be Improved16

III. EXHIBIT

Exhibit A: Commercial-Off-The-Shelf Evaluation Methodology20
Exhibit B: Commercial-Off-The-Shelf Alternatives Evaluation21

IV. APPENDIX

Appendix: Management Response To The Draft Report

This Page Intentionally Left Blank

I. INTRODUCTION

Background

The Office Supply Service (OSS) is primarily responsible for the purchase, sale, and delivery of office supplies through the Office Supply Store (Supply Store) for the U.S. House of Representatives (House). The Supply Store is located in the Longworth House Office Building and is only open to Members and other House employees. OSS is also responsible for operating a gift shop. The House Gift Shop (Gift Shop) is located next to the Supply Store in the Longworth House Office Building and is open to the Members, other House employees, and the public.

In 1993, OSS purchased and implemented the Multiple Computer Business Applications (MCBA) system from ProVAR, Inc. to record and process office supply store and gift shop inventory and accounting management activities. OSS relies on the MCBA system to support critical functions such as purchasing, inventory management and accounting. Integrated with the MCBA system is a point-of-sales (POS) system developed by Synchronics Inc., which enhances the MCBA system's capabilities to support OSS's sales and inventory functions for its office supply and gift shop operations. This system runs in a UNIX environment on an IBM RS/6000 midrange computer system. ProVAR, Inc. provided overall system support until December 31, 1997. Beginning in January 1998, the Business Information Group (BIG) took over system support and maintenance.

The MCBA system contains the following subsystems: General Ledger, Accounts Receivable, Accounts Payable, Inventory Management, and Purchasing. However, OSS is not using the General Ledger subsystem because the House uses the Federal Financial System (FFS) for general ledger recording and processing. OSS personnel are responsible for the supply store and gift shop daily accounting function which involves the recording and tracking of accounts receivable and accounts payable transactions for the supply store and gift shop operations in MCBA.

The Accounts Receivable subsystem is used to record virtually all orders purchased on a credit basis from the store. The data is used to generate monthly statements to Member, Committee, and other House offices and is fed into FFS through an automated interface.

The Accounts Payable subsystem is used to record liabilities related to Purchase Orders (POs) for the supply store and gift shop. The data is used by OSS to create vouchers for payment by the Office of Finance (Finance) and to track the status of POs. The actual check number for a given payment is recorded in FFS. Therefore, to respond to vendor inquiries on the status of a payment for a particular invoice, OSS uses the MCBA system to first determine whether a PO was vouchered and then accesses the FFS system for the actual payment information (e.g., check number).

The MCBA Inventory Management subsystem is used to track and monitor inventory items. The POS system is used for scanning bar coded purchases at the cash register and allows for automatic adjustments to inventory levels. The Inventory Management subsystem is also

capable of handling returned items. The subsystem provides for an automated re-order level, which can be used to trigger inventory purchases before quantities on hand become fully depleted. This subsystem uses the price averaging¹ method for computing sale prices for office supply and gift shop items. There is no markup on office supply items purchased for official use and a 20 percent markup on gift shop items. For personal purchases by House employees, there is a 10 percent markup on supply store items.

The MCBA Purchasing subsystem is used to initiate and track purchases, by allowing for the creation and updating of POs. These POs can be created for stock², special order³, and print⁴ items. The POs are used to track requested purchases, receipt of ordered items, and prepare requests for payments through Finance. The MCBA Purchasing subsystem is not used for approving POs, but instead serves as a monitoring and tracking system for POs.

For Calendar Year (CY) 1996, OSS sales were approximately \$6.5 million. As of December 31, 1996, OSS's inventory was \$800,190 and accounts payable was \$120,659.

Objectives, Scope, And Methodology

The objectives of this audit were to (1) assess the accuracy, completeness, validity, and timeliness of data processed by the MCBA system, and (2) evaluate the effectiveness of the system and planned enhancements to the system. More specifically, the audit included:

- Determining, through statistical sampling, whether the system contains accurate and complete information.
- Evaluating the adequacy of the MCBA system controls.
- Evaluating the adequacy of the physical and logical controls relevant to the MCBA system.
- Evaluating the adequacy of contingency planning relevant to the MCBA system.
- Determining whether the system meets its intended purpose.
- Determining whether appropriate system development life cycle methodologies have been or are being applied to planned enhancements to the system and that the enhancements include Year 2000 readiness.

¹This method of calculating the price of items, involves computing the total cost of all individual items within a type of supply store or gift shop item and then dividing this total cost by the number of the individual items to obtain an average cost. When costs per unit varies for a particular item, this method minimizes gains or losses by recalculating the average cost, thereby, updating the item price in the MCBA system.

²These items are part of the regular inventory which are frequently purchased from OSS and have to be periodically re-ordered.

³These items are not part of the regular inventory, but can be specifically ordered by OSS for the requesting office.

⁴These items include printing of business cards and customized stationery.

- Determining whether viable commercial-off-the-shelf (COTS) alternatives to the MCBA system are available that offer standard interfaces to financial management systems, such as the House's FFS.

The scope of the review was limited to OSS operations relative to the MCBA system. The period of audit coverage included activities associated with OSS between the beginning of the 104th and the first half of the 105th Congresses. Audit field work was conducted between November 1997 and March 1998.

We conducted our audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To gather and verify data, we interviewed key personnel, reviewed relevant documents, and performed appropriate tests of various processes and procedures. Specifically, we interviewed personnel in OSS and House Information Resources (HIR) as well as selected vendors. In addition, we applied applicable information systems audit guidelines used in the Federal government and private industry in evaluating system and internal controls.

Internal Controls

We performed a review of the internal controls related to the operation of the House's MCBA system. We identified several internal control weaknesses related to system operations, which are discussed in the "Findings and Recommendations" section of this report.

Prior Audit Coverage

No prior audits of the MCBA system have been conducted.

This Page Intentionally Left Blank

II. FINDINGS AND RECOMMENDATIONS

Finding A: Steps Need To Be Taken To Implement An OSS Inventory/Accounting Management System Which Will Meet The Needs Of The House

Despite the many MCBA system functions utilized by OSS, the system does not adequately fulfill the needs of the House. Specifically, the MCBA system is not Year 2000 compliant and system inadequacies include the lack of functionality to accomplish essential tasks and inefficiencies in existing processes. This has required OSS personnel to manually carry out essential functions that could be automated. Inefficiencies, such as duplicate data entry and maintenance of similar data elements with different values between the MCBA system and FFS, increase the potential for errors. As a result, OSS cannot be as efficient and effective in carrying out its operational responsibilities as it could. Furthermore, OSS needs to assign qualified resources, establish work-plans, and conduct the essential analyses for the replacement of the MCBA system.

Criteria for information system development or acquisition is well established

Well-run information system development or acquisition efforts generally are managed using a formal System Development Life Cycle (SDLC) methodology. This methodology is set forth in the Chief Administrative Officer's June 1996 policy document entitled *Management Policy For System Development Life Cycle*. The policy provides for the implementation of a formal SDLC process which enables management to minimize the risks associated with developing, purchasing, maintaining, and implementing systems within the House. The core process includes a framework for upper management participation in strategic planning for development projects and a process for managing the various projects under development.

Best practices dictate that entities perform a thorough requirements analysis to provide a clear basis of user needs before acquiring information resources. Conducting a cost/benefit analysis of viable alternatives is also essential to evaluate and compare various alternatives for meeting requirements. Cost/benefit analyses should also include a description of each of the alternatives and their costs, a description of quantifiable and non-quantifiable benefits, a description of the weighted decision criteria reflecting the specific environment of the organization, and a decision matrix comparing each alternative. These two analyses are early steps employed in a formal SDLC methodology, which provides a structured approach to managing a system acquisition and implementation project throughout its life cycle. Conducting a requirements analysis, performing a cost/benefit analysis, and documenting those results are essential SDLC processes required to not only adequately justify management's decisions and expenditures, but also to provide much needed information for project development and implementation.

The MCBA system is not Year 2000 compliant

The Year 2000 date issue is one of the most significant problems facing organizations relying on information technology today. Business success and continuity will be dependent upon the ability of business applications, package solutions, and system software to process dates beyond December 31, 1999. Presently, the MCBA system is not Year 2000 compliant. This means that

the system cannot correctly handle date-related transactions beyond December 31, 1999. Without remediation, the Year 2000 will be processed as the year "00", which currently represents the Year 1900. The continued use of the current two-digit year representation will cause many basic functions of computer systems to fail in the Year 2000, such as programs returning incorrect results or ending abnormally. OSS is aware of the need to address this important issue and initiated inquiries with the current vendor to identify possible remediation solutions. However, we have identified several COTS solutions that are Year 2000 compliant and, as discussed later in this Finding, better meet the CAO's needs.

OSS does not use the MCBA system effectively

The MCBA system functionality is not being fully utilized. OSS uses four (Purchasing, Inventory Management, Accounts Receivable and, to a limited extent, Accounts Payable) of the five MCBA subsystems. OSS records all Purchase Orders (POs) into the Purchasing subsystem. As supply items are received and sold, the inventory quantities and costs are automatically updated in the Inventory Management subsystem. However, OSS is not using the Accounts Payables subsystem effectively. This subsystem is used only on a limited basis due to the implementation of FFS. Currently, the MCBA Accounts Payable subsystem is not automatically updated to reflect appropriate FFS payment information (e.g., check number). This creates a need to access both systems and to implement manual work-around procedures, such as maintaining manual files of historical accounts payable payment information.

In addition, the Accounts Payable subsystem has the capability to track and produce credit memo⁵ aging reports, however, OSS has not taken advantage of the subsystem for tracking the status of credit memos. Credit memos represent an acknowledgement of the value of returned item(s) to be credited with the next purchase. The memos are maintained in a manual file in the OSS Accounts Payable section and are reflected as adjustments to the respective accounts payable records. Presently, OSS relies on the inventory-receiving supervisor to review credit memo files on a monthly basis. Manual review of credit memos can result in credit memos being missed and outstanding for several months. These inefficiencies are primarily due to inadequate MCBA programming and subsequent training on the features and capabilities of the MCBA system.

Further, the MCBA system as implemented and utilized results in duplicative processes because there is no automated interface between the MCBA system, which was operational prior to the installation of FFS. For example, OSS is required to enter PO-related information into the FFS Accounts Payable subsystem, however, FFS assigns a different purchase order number, requiring OSS to track two sets of PO numbers. Similarly, OSS must set up vendor information in both systems. FFS separately assigns a vendor identification code, which requires OSS to track two vendor identification codes. Office account numbers are also different between the two systems. Thus, OSS is burdened with tracking two identification codes for the same vendors and two office account numbers for the same offices, which creates the potential for errors. Additionally,

⁵OSS receives credit memos from vendors which reflect goods returned to the vendor for varying reasons (e.g., damaged items and quantities in excess of original order).

manually re-keying information (i.e., into FFS) is inefficient and creates greater opportunities for introducing errors in translation between the MCBA and FFS codes.

According to OSS personnel, when the MCBA system was originally implemented, it was interfaced with the House's Financial Management System (FMS). Since then, FMS has been replaced by FFS, which is expected to be an interim solution. Because of the interim nature of FFS, the House continued to use the original interface. All account code conversion was designed as a front-end to FFS processing of MCBA transactions. However, no automated interface is currently available to permit FFS to periodically update MCBA. Thus, the need to access both systems for information adds to and complicates OSS's day-to-day operations. Presently, the House is in the process of planning for a permanent financial management system solution. The FFS Steering Committee is overseeing this effort.

We also noted MCBA system limitations that prevent OSS from operating more efficiently. For example, the current system does not allow OSS to record and track multiple vendor payment addresses. Address changes are occasionally needed, however, the system does not provide management a mechanism to track the changes made, who made the changes, and whether the changes were appropriate.

Other viable COTS alternatives are available

OSS has not fully completed the following essential analyses needed to replace the MCBA system prior to Year 2000:

- Identification of needed changes to current OSS inventory/accounting business activities. This should include the identification of existing capabilities, new or changed business requirements, and opportunities for increased economy, efficiency, and effectiveness.
- Identification of functional and operational requirements (e.g., performance, reliability, compatibility, safety, and security) including any requirements associated with the changes to current business activities, and data requirements necessary to meet OSS's needs.
- Formulation of alternative courses of action, including the acquisition of COTS solutions, that are technologically feasible and will best satisfy OSS's business requirements.
- Preparation of a gap analysis for each alternative, which identifies where each alternative fails to meet OSS's requirements.
- Identification of life-cycle costs and benefits associated with each alternative.

As part of this audit, we researched available COTS alternatives to determine whether products existed that would meet OSS's high-level operational needs and offer standard interfaces to financial management systems, such as the House's FFS. The methodology included steps for (1) identifying and documenting high-level functional requirements for OSS's information systems operational needs, (2) ranking the functional requirements based on priority, (3) identifying all COTS alternatives, and (4) performing a gap analysis of alternatives to identify the most viable COTS alternatives. (The detailed methodology is discussed in Exhibit A, *Commercial-off-the-Shelf Evaluation Methodology*, of this report.) While the steps in our methodology did not include a cost analysis of COTS alternatives, we nevertheless collected product cost information from each vendor to facilitate detailed analysis by OSS.

The results of the COTS alternative work are summarized in Exhibit B, *Commercial-off-the-Shelf Alternatives Evaluation*. This summary includes a brief description of the high-level information system requirements, specific COTS alternatives, and the products' capabilities compared to OSS's requirements. We identified 19 alternatives, which could meet most of OSS's high-level requirements. Based on the gap analysis of the high-level information system requirements (see Exhibit B), the following five COTS alternatives identified in Figure 1 were the top-ranked products in meeting OSS's information system requirements⁶:

Figure 1: Top-Ranked COTS Alternatives

<i>Software</i>	<i>Vendor</i>
Macola 7.0	Macola Software
MTX Millenium+ Accounting	MTX International
Visual Accounting	RealWorld Corp.
Solomon IV	Solomon Software
Excellence Series	Southware Innovations

Although we narrowed the COTS alternatives from 19 to 5, OSS needs to validate the high-level requirements—this validation could result in the identification of top-ranked COTS alternatives different from the ones we identified. In addition, OSS must identify the detailed functional and operational requirements (e.g., performance, reliability, compatibility, safety, and security), including any requirements associated with the changes to current business activities and data requirements necessary to meet OSS's needs. OSS must also contact each of the vendors of the top-ranked COTS alternatives to research and obtain information necessary to determine the ability of each COTS alternative to meet the detailed functional and operational requirements. The selection process should further include an operational capabilities demonstration for each of the top-ranked (or recommended) alternatives. Finally, in order to select the most cost-effective solution for meeting OSS's information system needs, OSS needs to select the best alternative based on a gap analysis against the detailed requirements, cost/benefits analysis, and the operational capabilities demonstration of each top-ranked COTS alternative.

To ensure that all the appropriate steps are completed, OSS needs to assign a project manager and implementation team and establish a work plan and milestones. The work plan should indicate the level of effort and availability of resources for each major task and time frames for completion. The completion of the analyses and the success of selecting and implementing a new system will greatly depend on the qualifications of individuals assigned and the amount of time they devote to the project.

Recommendations

We recommend that the Chief Administrative Officer:

⁶The gap analysis of the 19 alternatives was based on high-level requirements and not on detailed requirements. Without the benefit of detailed requirements, the above list may not include the best alternatives.

1. Assign qualified resources and establish a level of effort work plan with implementation dates for the implementation of a Year 2000 compliant COTS solution to replace or upgrade the MCBA system.
2. Complete the following analyses:
 - Identify needed changes to current OSS inventory/accounting business activities. This should include the identification of existing capabilities, new or changed business requirements, and opportunities for increased economy, efficiency, and effectiveness.
 - Validate high-level requirements in Exhibit B.
 - Identify the detailed functional and operational requirements (e.g., performance, reliability, compatibility, safety, and security), including any requirements associated with the changes to current business activities and data requirements necessary to meet OSS's needs.
 - Contact each of the vendors of the top-ranked COTS alternatives identified in OSS's analysis to research and obtain information necessary to determine the ability of each COTS alternative to meet the detailed functional and operational requirements.
 - Obtain an operational capabilities demonstration for each top-ranked COTS alternative.
 - Select the best alternative based on a gap analysis against the detailed requirements, cost/benefits analysis, and the operational capabilities demonstration of each top-ranked COTS alternative.

Management Response

The CAO concurred with this finding and both recommendations (see Appendix). According to the response, the Associate Administrator of Media and Support Services established, on July 8, 1998, a MCBA System Review Team, consisting of staff members from various offices within the CAO's organization. The team is responsible for completing tasks, including those listed in Recommendation 2, which will culminate in a recommendation for a Year 2000 compliant COTS solution to replace or upgrade the MCBA system. The team will complete all work and submit its findings to the CAO by January 15, 1999.

Office of Inspector General Comments

The actions taken and planned are responsive to the issues identified and, when fully implemented, should satisfy the intent of the recommendations. Furthermore, the milestone date for completing these actions appears reasonable.

Finding B: Inadequate Information Technology Controls Could Hamper OSS Operations

OSS's MCBA system does not have adequate software change, logical access, operational, and environmental controls. Consequently, the House cannot be assured that the inventory and accounting-related data is accurate, complete, and valid. Further, without adequate procedures to ensure computer system operational continuity, availability, and reliability, the House may not be adequately prepared to quickly recover from unforeseen disruptions, such as a prolonged outage or damage to the system and its data. The MCBA system deficiencies can be attributed to the lack of formal written procedures, awareness of established requirements, staff training, and a back-up system administrator.

Criteria for information technology controls is well established

National Institute of Standards and Technology's (NIST) Federal Information Processing Standards (FIPS) Publication 106, entitled "Guideline on Software Maintenance," prescribes guidelines for achieving a strong, disciplined, and clearly defined approach to software maintenance. The primary purpose of change control (or change management) is to assure smooth operational continuity and orderly evolution of the system. Effective change control is necessary to ensure that all system software installation and maintenance requirements are performed in a structured and controlled manner and provide management with a chronological history of all software modifications. Key change management control points ensure that all changes to hardware and software are formally requested, adequately tested, and approved to minimize the risk of errors and irregularities in the production processing environment. Although the House is exempt from NIST directives, this guidance provides a best practices approach for handling software installation and maintenance.

HISPOL002.0, *The United States House of Representatives General Information Security Guidelines for Protecting Systems from Unauthorized Use*, establishes an overall, comprehensive set of guidelines for the responsible and secure use of House information systems and network resources. These guidelines are applicable to all House Officers and require strong logical access, operational, and environmental controls for application systems.

Within the private sector, best practices include software change, logical access, operational, and environmental security controls and safeguards that are commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of system information. Changes to system and application programs should be made in a controlled environment where all modifications are reviewed and approved by someone other than the person who made the changes. In addition, information systems security and control practices recognize the importance of proper administration and implementation of security settings to provide adequate segregation of duties. The assignment of more restrictive logical access privileges serves as a precautionary measure to minimize the risk of accidental or unauthorized actions that could compromise the integrity of information and disrupt operations. Further, management should develop and maintain a disaster recovery/contingency plan which defines the roles and responsibilities, and the approach/methodology to be adopted. The plan should include detailed back-up policies and procedures, including storage of back-up tapes at an off-site storage facility. Finally, management should assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g., fire, dust, power, excessive heat and humidity).

OSS does not have adequate change controls procedures over the MCBA system

The current MCBA system's functionality is not adequately documented. While a User Manual is kept in the computer room, the manual it is not up-to-date, does not represent the current system, and is the only copy available for all MCBA system users. Also, OSS personnel were uncertain whether they have the source code for the MCBA system. To add to the uncertainty of the baseline system, OSS does not maintain a list of changes to the system. The lack of documentation and extent of changes that have been made to the system has forced OSS to rely on its experienced users for application system functionality and operational knowledge.

Normally, when OSS needs a change to the MCBA system, they contact the vendor. A vendor representative evaluates the specific request to determine whether software solutions already exist or software changes are needed to accommodate OSS's system requirement. If a software change is needed, the vendor representative completes a Software Modification Request (SMR) form and faxes the form to OSS for approval. OSS reviews the adequacy of the information and proposed change and, once comfortable with the proposed change, approves the SMR. When an SMR has been completed, the vendor contacts OSS and installs the software on the system through dial-up access. The changes are tested by OSS personnel, who enter test transactions through a "dummy" account created on the system and verify that the changes function as expected.

We noted the following deficiencies in the MCBA system change process. First, even though OSS is required to sign-off on the SMR form, they do not retain or track the forms internally. This makes it impossible to account for all the changes made to the MCBA system since its implementation. We were unable to determine the specific application system requirements or the number, extent, or cost of the changes made to the MCBA system. Second, there were no formal test plans prepared or test results documented to indicate whether the testing performed is comprehensive. Finally, when OSS accepts the software modification, OSS does not have a formal process of authorizing transfers to the production environment with the use of forms and approval signatures. Instead, the vendor representative is notified by telephone to move the change into the production environment. The vendor representative then dials into the system and copies the new code into the production environment.

Without a formal system change process, which includes system baseline documentation and change and testing documentation, there is no assurance that modifications made to the system are justified, authorized, and adequately tested prior to implementation. Unauthorized or improperly tested changes could result in further operational difficulties, such as performance problems, denial of service, and integrity and security exposures. For example, when the vendor transmits requested changes to OSS's environment, the vendor may introduce changes, other than those requested, into the environment. Furthermore, should staffing changes occur, new personnel cannot easily understand the application system requirements and the implementation of those requirements, the system changes needed or the rationale for those changes, system maintenance requirements, and operational requirements. Thus, in the long run, OSS cannot ensure orderly evolution of the application and continuity of system operations.

This situation has occurred because OSS does not have any documented policies and procedures requiring a comprehensive process for tracking, testing, and documenting changes associated with the MCBA system. Such guidelines would provide OSS an important framework to ensure effective and reliable system operation. Also, the MCBA system administrator does not have extensive technical background and has not received any formal training related to change control procedures and their importance to the system environment. As a result, the system administrator is not familiar with the specific requirements or steps in a generally accepted change management process.

Logical access controls need to be improved

Access controls to the MCBA system are not adequate. The following logical security access deficiencies were identified:

- Users as well as the system administrator were not required to periodically change passwords.
- User passwords could be easily guessed.
- Terminals did not time-out after a period of inactivity.
- Accesses to the system through the host/network and dial-up were not monitored.
- Inactive profiles or logon IDs were not periodically reviewed and removed from the system.

Additionally, there are currently two modem dial-up connections that are used for remote access by vendor representatives. These modems are required so that the representatives can dial-in to transmit changes to the system. However, the modems are continuously connected rather than disconnected until needed. Furthermore, the system administrator did not know the telephone numbers for the modems connected to the RS/6000 or who has access to them. In an environment with external connections, it is critical that the system administrator be aware of this risk area and periodically monitor external access to the system.

Users access and system privileges are normally provided on a "need to have" basis, consistent with job responsibilities. We noted that OSS did implement security profiles at the system level; however, we could not determine whether current users access and system privileges are appropriate because documentation supporting requests and approvals is not adequately maintained. This problem is exacerbated by the lack of a defined data security policy addressing user access and system privileges, and periodic reviews of user profiles and privileges as precautionary measures to minimize the risk of unauthorized actions that could compromise the integrity of MCBA data and/or disrupt operations.

Without effective security controls over information resources and user access to such resources, OSS substantially increases the risk of unauthorized access and modifications to, and disclosure of, important House operational data. Consequently, OSS cannot be assured that information resources were sufficiently protected from fraud, waste, unauthorized use, and mismanagement.

Operational and environmental controls over the computer environment are weak

OSS is largely responsible for providing for its own information technology needs, including operational procedures and environmental controls. Presently, the Accounting Supervisor has dual roles within OSS. Although her position description lists her as responsible for office supply-related accounting functions, she also serves as the office's system administrator in a defacto capacity. In this latter capacity, she administers and operates the MCBA system, performing such duties as running batch processes, troubleshooting system problems, performing daily system back-ups, etc.

The system administrator performs a full nightly back-up of the MCBA system. As a byproduct of the back-up process, the system automatically prints a report to indicate whether problems were encountered during the process. The system administrator reviews this report daily. If no problems were encountered, the back-up tapes are stored in a secured vault within OSS. However, we learned that back-up tapes are not archived nor rotated to an off-site storage location. Back-up tapes should be archived for a specific period of time to permit recovery of prior versions of programs or data, if necessary, and rotated to an off-site storage facility in the event a disaster occurs at the computer facility. In addition, there is no back-up person within OSS designated to carry out the system administrator's responsibilities in her absence. In emergencies, OSS indicated that they can revert to manual procedures, but acknowledged that they are largely dependent upon the vendor for system recovery assistance.

We also noted that the room housing the RS/6000 does not have adequate environmental protection controls. On more than one occasion, we observed that the air conditioner in the room was inadvertently shut off at the end of the day by maintenance personnel, causing the room temperature to rise to unacceptable levels. This situation could cause the hardware to overheat and become permanently damaged. The air conditioner should run constantly to provide an acceptable temperature level to protect the House's investment in the computer hardware. We also noted no fire extinguisher in the room to protect the computer hardware and programs from fire damage. According to OSS, the room, in which the IBM RS/6000 resides, was not originally designed to be a computer room and, as a result, still needs to be retrofitted to meet the current use.

We identified several factors contributing to operational and environmental weaknesses. First, OSS does not have policies and procedures addressing the management and security of MCBA. However, during the course of the audit, we learned that the CAO had prepared security guidelines to be implemented CAO-wide for approval by the Committee on House Oversight. The security guidelines contained in HISPOL002.0, entitled *The United States House of Representatives General Information Security Guidelines for Protecting Systems from Unauthorized Use*, which include requirements to alleviate the weaknesses discussed in this finding, was approved on February 4, 1998. Rather than preparing separate security guidelines specific to MCBA, OSS can adopt and implement this policy. Second, while OSS has some back-up and recovery procedures, it does not have a comprehensive, documented disaster recovery/contingency plan to address protection of equipment and information so that it is available on a timely basis to meet mission requirements and to avoid disruptions and substantial losses. Continued reliance on one system administrator without a back-up staff member and a high degree of reliance on a third party to provide support in the event of an emergency increases operational risk. Third, the Accounting Supervisor does not have the necessary technical

background to perform the system administrator job. The Accounting Supervisor has not received any formal training on generally accepted system operation procedures, such as nightly system back-ups and batch processing. The MCBA system operates in a complex UNIX environment that requires a thorough understanding of this environment for administration purposes. The risks in this environment are very high if not administered and operated appropriately. Finally, management has not assessed its environmental controls to determine whether they are adequate to protect the computer assets.

Recommendations

We recommend that the Chief Administrative Officer:

1. Document and implement comprehensive policies and procedures for tracking, testing, and documenting all changes/modifications to the MCBA system, as well as any future replacement.
2. Implement a security policy, which addresses data sensitivity, data ownership, password administration requirements, and responsibilities for approving and periodically reviewing access levels, consistent with the risk of loss. At the minimum, the policy should address:
 - Password change frequency, such as every 60 days, for users and system administrators.
 - Use of unique passwords consisting of alphanumeric and special characters.
 - Procedures for logon sessions to "time-out" or re-entry of passwords after a period of inactivity.
 - Security administrator responsibilities, including approvals and periodic reviews of user logon IDs and access privileges for appropriateness with job responsibilities, removal of inactive user accounts and privileges, monitoring of unauthorized attempts to gain access to the system, monitoring of vendor and contractor accesses, and monitoring of remote access.
 - Disconnecting modems when not in use.
3. Develop, document, and implement a disaster recovery/contingency plan for the MCBA system and any future replacement.
4. Perform an assessment of the current MCBA computer environment to identify the controls necessary to adequately protect computer assets and implement the required controls resulting from the assessment. At a minimum, these controls should include ensuring that the air conditioner in the computer room runs constantly to provide an acceptable temperature level and fire extinguishers are available to protect the House's investment in computer hardware.
5. Provide security awareness training to current MCBA users and the system administrator. In particular, provide more detailed technical training for the system administrator so that he/she can implement stronger and more effective controls.

6. Designate and train a back-up person to the system administrator.

Management Response

The CAO concurred with this finding and all six recommendations (see Appendix). According to the response, actions were completed for Recommendations 4 and 5. In addressing Recommendation 4, the Architect of the Capitol conducted an assessment of the current MCBA computer system environment on August 1, 1998. Based on this assessment, an acceptable temperature level for the air conditioner in the computer room was set and a fire extinguisher was installed to protect the assets contained in the computer room. The response further indicated the CAO's intent to relocate the MCBA replacement system, once procured, in the protected environment within HIR's computer center. Relative to Recommendation 5, OSS completed security awareness training for its employees on September 17, 1998.

Other initiatives are underway or planned for addressing the remaining recommendations. These include: (1) documenting all changes and modifications to the MCBA system, and preparing a comprehensive list of procedures for tracking, testing, and documenting all modifications to the system by February 1, 1999; (2) developing and completing a comprehensive security policy by February 1, 1999; (3) finalizing a complete disaster/contingency plan for the MCBA system by February 15, 1999; and (4) preparing a proposal, for submission to the CAO by October 16, 1998, to establish a Senior Systems Engineer position within HIR to support the MCBA system and, once this position is in place, designating another position in HIR to serve the back-up role.

Office of Inspector General Comments

The actions taken and planned are responsive to the issues identified. Based on the actions completed, we consider Recommendations 4 and 5 closed. However, with respect to Recommendation 5, we trust that OSS will provide more detailed technical training for the system administrator commensurate with his/her job responsibilities.

The actions currently underway and planned, when fully implemented, should satisfy the intent of Recommendations 1, 2, 3, and 6. Further, the milestone dates for completing these actions appear reasonable.

Finding C: MCBA Data Integrity Can Be Improved

While OSS has established controls to assure the integrity (i.e., accuracy, completeness, and validity) of the MCBA data, current practices can be fine-tuned to improve the integrity of this data. In particular, procedural changes surrounding MCBA data entry and adjustments impacting inventory quantities can minimize erroneous data. Inaccurate and incomplete inventory quantities in the system can cause the system to overstate or understate inventory quantities on hand. Without strengthening controls over MCBA data, OSS may not be able to rely on the data maintained within the application for decision-making purposes. These weaknesses can be attributed to the lack of appropriate monitoring procedures to ensure supply items are scanned individually into the POS terminals, inconsistent implementation of procedures to verify inventory quantities in the MCBA system, and lack of proper segregation of duties and adequate procedures for approving and tracking all adjustments to inventory quantities in the system.

Best practices support implementing controls to ensure the integrity of information system data

Reliable information is a fundamental cornerstone for any organization or business process to achieve its objectives effectively. The Information Systems Audit and Control Foundation's *CobiT: Control Objectives For Information and Related Technology* provides best practices to ensure that data remains complete, accurate, and valid during its input, update, and storage. *CobiT* cites that transaction data entered for processing (people-generated, system-generated, or interfaced inputs) should be subject to a variety of controls to check for accuracy, completeness, and validity. Procedures should also be established to assure that input data is validated and edited as close to the point of origination as possible. In addition, *CobiT* cites that organizations should establish procedures for processing data that ensure separation of duties is maintained and that work performed is routinely verified.

The MCBA system contains inaccurate and incomplete data

The MCBA system contains information, such as cost and inventory data, that is critical to the ongoing operations of OSS. The system uses a cost averaging method to compute the average cost of the office supply and gift shop items and, accordingly, computes the sales price. The supply order process is heavily dependent upon the quantity level in the MCBA system. OSS sets quantity thresholds for each supply item in the system. When the items drop to the predetermined threshold, the system automatically identifies the item for re-order.

We noted that sales clerks do not consistently scan items separately into the POS terminals. If items appear to be similar, rather than scanning each item individually, the sales clerk will scan the first item and then manually enter the total quantity of that item into a POS terminal. Often items appear to be similar but, in fact, are different and have different inventory bar codes. Therefore, without scanning each item individually, the inventory quantities on-hand for one item would be overstated and understated for another, causing inaccurate inventory quantities to be recorded.

As a means of verifying the quantities in the MCBA system, OSS management requires its employees to recount quantities on-hand when the unit cost of re-ordered supply items has changed. In these instances, receiving personnel are required to perform a physical inventory of the applicable stock/gift items to ensure that the quantities reflect actual inventory on-hand (e.g., newly ordered items plus existing inventory items) and make any necessary adjustments to quantities in the MCBA system. Applying this practice when cost of supply items change simply provides OSS the opportunity to ensure that the system computes the correct average cost and sale prices. Despite OSS's intent, we learned that the manual practice of recounting inventory items is not consistently followed. Therefore, necessary adjustments may not be made to the system inventory quantities.

To determine the integrity of MCBA's inventory data, we conducted sample tests for accuracy and completeness⁷. We randomly selected 25 types of supply items (e.g., pens, binders, etc.) and physically counted the quantities on-hand. We compared the quantities on-hand to the inventory quantities recorded in the MCBA system. Of the 25 types of supply items, we noted MCBA quantities differed for 10 types of supply items. The 10 types of supply items resulted in a total variance of 81 individual items between the quantities on-hand and the information in the system. Conversely, we randomly selected 25 types of supply items recorded in the system and traced them back to the physical quantities on-hand in the stock room and sales floor. Of the 25 types of supply items, we identified discrepancies for 8 types of supply items. The 8 types of supply items resulted in a total variance of 21 individual items between the information recorded in the system and the quantities on-hand.

Although our tests started before OSS opened for business, it was not completed until after the store opened. Since we realize that the sale and movement of inventory items during business hours could contribute to the discrepancies found, we compared our results to those of OSS's year end physical inventory. Based on this comparison, we found that OSS also identified discrepancies with the same supply items.

Inaccurate and incomplete data in the system results in overstated or understated inventory items. Overstated inventory items could cause OSS to re-ordered supplies earlier than required. Conversely, when items are understated, supply items would not be available when they are needed. Without employing better controls over the inventory data, OSS cannot rely on the data maintained within the MCBA system for decision-making purposes.

⁷We applied random sampling techniques, using a 90 percent confidence level and 20 percent upper precision limit, to determine sample size. Confidence levels, also referred to as reliability, reflect the probability that the auditor's statistical conclusion will be correct. The acceptable upper precision limit is a percentage that is equated to the maximum permissible deviation rate. Deviation in excess of the acceptable upper precision limit would cause the auditor to reduce the reliability level.

Factors contributing to MCBA data integrity problems

These MCBA data integrity weaknesses can be attributed to several deficiencies. First, OSS does not appropriately monitor sales clerks to ensure that supply items are scanned individually into the POS terminals. Second, OSS does not enforce the practice of re-counting and updating the inventory quantities in the MCBA system when the unit cost of items changes. Third, OSS lacks proper segregation of duties and adequate procedures for approving and tracking all adjustments to inventory quantities in the MCBA system. For example, the inventory control supervisor is allowed to receive, count, and adjust the MCBA inventory without any compensating controls, such as requiring an individual in another area to validate proposed inventory adjustments and approve those adjustments. In addition, no audit trail is maintained for approval of adjustments to inventory.

Recommendations

We recommend that the Chief Administrative Officer:

1. Establish procedures to ensure that sale clerks scan individual items, at the time of sale, into the POS system to ensure that inventory items are correctly reduced in the MCBA system and require the sales manager to review all sales for items that are not scanned individually through the POS system on a daily basis. This review can be facilitated by using an edit report, listing the number of manual quantity entries, on a daily basis.
2. Enforce compliance with OSS practice of recounting all items when the unit cost of items changes. Count sheets should be prepared on a daily basis for new items received into inventory and signed off by an employee responsible for completing the inventory count. The inventory control supervisor should periodically verify count sheets.
3. Require the inventory control supervisor to obtain signoff from the Director of Office Supply Service, for all inventory system adjustments.

Management Response

The CAO concurred with this finding and all three recommendations (see Appendix). According to the response, OSS established procedures to improve data integrity in MCBA, effective August 1, 1998. The procedures included requirements for ensuring that (1) sales clerks scan individual items at the time of the sale and the sales manager regularly reviews edit reports to ensure compliance with this policy; (2) all receiving staff re-counts all supply items when the unit cost of the item changes, and prepares a daily count sheet for new items received into inventory, and the receiving and sales floor supervisors sign off on the daily count sheets and periodically verify them; and (3) the Director of Office Supply Service signs for all inventory adjustments.

Office of Inspector General Comments

The actions taken are responsive to the issues identified and satisfy the intent of the recommendations. Thus, we consider all three recommendations closed.

Exhibit A

Commercial-Off-The-Shelf Evaluation Methodology

This exhibit presents an overview of the methodology used to identify suitable COTS alternatives which offer standard interfaces to a financial management system, such as the House's Federal Financial System. Our work was conducted in four phases described below.

Phase I: Developed high-level system requirements for MCBA

- Obtained original Request for Proposal for the current MCBA system
- Obtained vendor contract for current system
- Obtained Year 2000 documentation
- Met with OSS and HIR personnel to discuss system functionality
- Documented and reviewed business process flow charts
- Reviewed MBCA contract
- Discussed system change requests
- Reviewed the MCBA system Users Manual
- Mapped process flow to system functionality
- Documented high-level requirements analysis

Phase II: Ranked system requirements

- Categorized requirements into four categories (i.e., functional, technical, external dependencies, and vendor requirements)
- Reviewed and ranked functionality based on priority
- Discussed priorities with OSS

Phase III: Identified COTS alternatives

- Researched Internet to identify alternate COTS products
- Researched C&L database (DataPro) for alternate COTS products
- Researched Dialog Database
- Researched Lexis/Nexis Database
- Identified and contacted 300 vendors for information and details

Phase IV: Performed a gap analysis for best COTS alternatives

- Identified the ability/inability of each COTS alternative to meet high-level requirements
- Identified 19 out of 300 COTS alternatives, which could meet most of high-level requirements

Exhibit B**Commercial-Off-The-Shelf Alternatives Evaluation**

In this exhibit, we present the COTS alternatives for meeting OSS's inventory/accounting system needs. Figure 2 lists the specific names and the vendors of the 19 viable COTS alternatives based on our evaluation of the 300 potential products. Figure 3 shows OSS's information system requirements, the priority⁸ of each requirement, and the corresponding capabilities of each of the 19 applications with respect to the individual requirements. The bottom of Figure 3 shows the total number of gaps (i.e., where the product capabilities do not meet the high-level information system requirements) by product.

Figure 2: Viable COTS Alternatives

<i>Software</i>	<i>Vendor</i>
Visual Accountmate 3.1	Accountmate Software
Accpac for Windows	Accpac International
Accura Applications	Accura Software
Agama	Agama Software
Armor Software	Armor Systems
CDI Control Series	Concepts Dynamics
Cyma IV Accounting. for Windows	Cyma
Great Plains Dynamics C/S+	Great Plains Software, Inc.
AccWare	Icode
Macola 7.0	Macola Software
MTX Millenium+ Accounting	MTX International
Navision Financials	Navision Software
Platinum SQL	Platinum Software Corp.
Visual Accounting	RealWorld Corp.
Solomon IV	Solomon Software
MAS 90	State of the Art
Excellence Series	Southware Innovations
Impact Encore	Syspro Impact Software
Quantum MCBA	Business Information Group

⁸Each requirement was ranked as "High", "Medium", or "Low", based on the level of importance to OSS.

Figure 3. Comparison of COTS Alternatives With Functional Requirements

Products/Requirements		Priority	Visual Accountmate	Accpac for Windows	Accura Applications	Agama	Armor Software	CDI Control Series	Cyma IV Acctg. For Windows	Great Plains Dynamics C/S+	AccWare	Macola 7.0	MTX Millennium+ Acctg.	Navision Financials	Platinum SQL	Visual Accounting	Solomon IV	MAS 90	Excellence Series	Impact Encore	Quantum MCBA	
Purchasing Cycle	Enter & maintain POs for stock, special, & print orders	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Application accommodates bid pricing information	High	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	
	POs can be changed on-line	High	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	All POs entered during the day can be printed	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Selective (ad-hoc) printing of POs	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Customization of POs on creation	High	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Inquiry of POs can be done using key data elements	High	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Ability to integrate common vendor info. with FFS	High	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	
	Electronic faxing of POs to vendors	Low	○	○	✓	✓	✓	○	○	○	○	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	○
	Maintain an audit trail of changes to POs	High	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Ability to provide an aging of POs	High	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗		
Inventory Management	Receive and increment inventory levels for stock items	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Decrement inventory levels at time of sale	High	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Generate a return memo and process returns to vendors	High	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Process and transfer goods bet. multiple phys. locations	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Maintain and print Inventory Master Listing (all items)	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Maintain a Vendor Master Listing	Medium	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Maintain MIN/MAX levels for item reordering	High	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Various pricing methods are needed (avg., cost, etc.)	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Modify quantities and unit pricing on-line	High	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Compatible with POs subsystem and scanning	High	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	
	Track items using UPC or in-house bar codes	High	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Customer returns are posted as inventory updates	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Mark/note special orders as delivered	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	
	Audit trails (reports) available for all changes to invent	High	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Legend: ✓ Product capabilities and/or features meet the requirement listed.
 ✗ Product capabilities and/or features do not meet the high priority requirement listed.
 ○ Product capabilities and/or features do not meet medium or low priority requirement listed.

Figure 3. Comparison of COTS Alternatives With Functional Requirements (Continued)

Products/Requirements		Priority	Visual Accountmate	Accpac for Windows	Accura Applications	Agama	Armor Software	CDI Control Series	Cyma IV Acctg. For Windows	Great Plains Dynamics C/S+	AccWare	Macola 7.0	MTX Millennium+ Acctg.	Navision Financials	Platinum SQL	Visual Accounting	Solomon IV	MAS 90	Excellence Series	Impact Encore	Quantum MCBA	
Accounts Receivable and Accounts Payable	Produce a daily cash proof report by location	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Generate detailed monthly billing statements	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Generate a receiving report by PO	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	
	Ability to track open invoices on-line	Medium	✓	○	✓	✓	○	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Generate special order forms	High	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓
	Capable of tracking monthly payments by vendor	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Track C/R from orig. receipt to posting to ind acct.	Low	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	○
	Ability to monitor transactions by type	High	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Make vendor payments by electronic funds transfer	Low	○	○	✓	○	○	○	○	○	○	○	○	○	✓	✓	○	○	○	○	○	○
	Integrate with Point-of-Sales (POS) System	High	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
	Maintain a record of A/R credits (customer returns)	Low	✓	✓	✓	✓	✓	○	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	○
	Ability to modify & track prices charged to customers	High	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Technical Requirements	Year 2000 Certified	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Non-mainframe architecture	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Re-use current hardware	High	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	
	Compatible with a mainframe financial system	High	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗	
	Compatible with Procurement Desktop	High	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	
	Comprehensive report writer	High	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security Features	User password authentication	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Audit trails by user, transaction etc.	High	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Total No. of "X" or Gaps In High Priority Functional Requirements By Product				6	8	10	7	6	6	5	8	6	3	3	4	8	3	1	4	2	5	6

Legend: ✓ Product capabilities and/or features meet the requirement listed.
 ✗ Product capabilities and/or features do not meet the high priority requirement listed.
 ○ Product capabilities and/or features do not meet medium or low priority requirement listed.

James M. Eagen III
Chief Administrative Officer

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

MEMORANDUM

To: John Lainhart
Inspector General

From: Jay Eagen
Chief Administrative Officer

Subject: CAO Response to Audit Report of Office Supply Service's Inventory/Accounting System

Date: ~~OCT~~ 14 1998

Thank you for the opportunity to comment on the Draft Audit Report of Office Supply Service's Inventory/Accounting System. We have carefully reviewed the recommendations in the draft report and are in general support of them. Our specific comments and response to each recommendation are provided below:

Finding A: Steps Need To Be Taken To Implement An OSS Inventory/Accounting Management System Which Will Meet The Needs of the House.

Recommendation 1 We recommend the Chief Administrative Officer assign qualified resources and establish a level of effort work plan with implementation dates for the implementation of Year 2000 compliant COTS solution to replace or upgrade the MCBA system.

CONCUR

On July 8, 1998, the Associate Administrator of Media & Support Services established a MCBA System Review Team that consists of Jerry Bowles (OSS), Patty Mattimore (OSS), Mike Douglass (OPP), Tom Coyne (MSS), and Mike Frazier (HIR). The team has agreed to complete ten separate tasks that will culminate in a recommendation for a Year 2000 compliant COTS solution to replace or upgrade the MCBA system. The team will submit its findings to the CAO by January 15, 1999.

- Recommendation 2** We recommend the Chief Administrative Officer complete the following analyses:
- Identify needed changes to current OSS inventory/accounting business activities. This should include the identification of existing capabilities, new or changed business requirements, and opportunities for increased economy, efficiency, and effectiveness.
 - Validate high-level requirements in Exhibit B.
 - Identify the detailed functional and operational requirements (e.g., performance, reliability, compatibility, safety, and security), including any requirements associated with the changes to current business activities and data requirements necessary to meet OSS's needs.
 - Contact each of the vendors of the top-ranked COTS alternatives identified in OSS's analysis to research and obtain information necessary to determine the ability of each COTS alternative to meet the detailed functional and operational requirements.
 - Obtain an operational capabilities demonstration for each top-ranked COTS alternative.
 - Select the best alternative based on a gap analysis against the detailed requirements, cost/benefits analysis, and the operational capabilities demonstration of each top-ranked COTS alternative.

CONCUR

All of the steps listed above are part of the work plan for the MCBA System Review Team. This work will be completed by January 15, 1999.

Finding B: **Inadequate Information Technology Controls Could Hamper OSS Operations**

Recommendation 1 We recommend the Chief Administrative Officer document and implement comprehensive policies and procedures for tracking, testing, and documenting all changes/modifications to the MCBA system, as well as any future replacement.

CONCUR

OSS has assigned two employees the responsibility for documenting all changes and modifications to the MCBA system. A comprehensive list of procedures for tracking, testing, and documenting all modifications to the system is being prepared by HIR and OSS personnel, and will be completed by February 1, 1999. In addition, the Office of Human Resources is preparing a proposal to establish a Sr. Systems Engineer position within HIR to support the MCBA system. The proposal will be completed and sent to the CAO by October 16, 1998.

Recommendation 2 We recommend the Chief Administrative Officer implement a security policy, which addresses data sensitivity, data ownership, password administration requirements, and responsibilities for approving and periodically reviewing access levels, consistent with the risk of loss. At the minimum, the policy should address:

- Password change frequency, such as every 60 days, for users and system administrators.
- Use of unique passwords consisting of alphanumeric and special characters.
- Procedures for logon sessions to “time-out” or re-entry of passwords after a period of inactivity.
- Security administrator responsibilities, including approvals and periodic reviews of user logon IDs and access privileges for appropriateness with job responsibilities, removal of inactive user accounts and privileges, monitoring of unauthorized attempts to gain access to the system, monitoring of vendor and contractor accesses, and monitoring of remote access.
- Disconnecting modems when not in use.

CONCUR

A comprehensive security policy is being developed by HIR and OSS and will be completed by February 1, 1999.

Recommendation 3 We recommend that the Chief Administrative Officer develop, document, and implement a disaster recovery/contingency plan for the MCBA system or any future replacement.

CONCUR

Effective August 1, 1998, OSS revised its policy for storage of backup tapes and now stores the tapes in a fireproof safe at an off-site location. A complete disaster/contingency plan for the MCBA system will be finalized by February 15, 1999.

Recommendation 4 We recommend that the Chief Administrative Officer perform an assessment of the current MCBA computer environment to identify the controls necessary to adequately protect computer assets and implement the required controls resulting from the assessment. At a minimum, these controls should include ensuring that the air conditioner in the computer room runs constantly to provide an

acceptable temperature level and fire extinguishers are available to protect the House's investment in computer hardware.

CONCUR

On August 1, 1998, the Architect of the Capitol conducted an assessment of the current computer system environment. An acceptable temperature level was set and a fire extinguisher has been installed to protect the assets contained in the computer room. Based on these actions, this recommendation should be closed.

Once a new system has been identified and procured, it will reside in the protected environment within HIR's computer center. Placement of the new system within this environment will ensure that the Office of the CAO continues the practice of adequately protecting its computer assets.

Recommendation 5 We recommend that the Chief Administrative Officer provide security awareness training to current MCBA users and the system administrator. In particular, provide more detailed technical training for the system administrator so that he/she can implement stronger and more effective controls.

CONCUR

OSS completed security awareness training for its employees on September 17, 1998. Based on these actions, this recommendation should be closed.

Recommendation 6 We recommend that the Chief Administrative Officer designate and train a back-up person to the system administrator.

CONCUR

The Accounting Supervisor has been performing many of the duties typically assigned to a system administrator. As noted above, the Office of Human Resources is preparing a proposal to create a Senior Systems Engineer position with HIR to support the MCBA system. The proposal will be completed and sent to the CAO by October 16, 1998. Once this position is in place, the back-up role will be assumed by another Sr. Systems Engineer within the Information Management section of HIR.

Finding C: MCBA Data Integrity Can Be Improved

Recommendation 1 We recommend that the Chief Administrative Officer establish procedures to ensure that sale clerks scan individual item, at the time of sale, into the POS system to ensure that inventory items are

correctly reduced in the MCBA system and require the sales manager to review all sales for items that are not scanned individually through the POS system on a daily basis. This review can be facilitated by using an edit report, listing the number of manual quantity entries, on a daily basis.

CONCUR

Effective August 1, 1998, OSS established procedures to ensure that Sales Clerks scan individual items at the time of the sale. The Sales Manager is regularly reviewing edit reports to insure compliance with this policy. Based on these actions, this recommendation should be closed.

Recommendation 2 We recommend that the Chief Administrative Officer enforce compliance with OSS practice of recounting all items when the unit cost of items changes. Count sheets should be prepared on a daily basis for new items received into inventory and signed off by an employee responsible for completing the inventory count. The inventory control should periodically verify count sheets.

CONCUR

Effective August 1, 1998, OSS established procedures concerning inventory control. All of the Receiving staff now re-count all items when the unit cost of the item changes. The Receiving staff prepares a daily count sheet that consists of new items received into inventory. Both the Receiving and Sales Floor supervisors sign off on the daily count sheets and the count sheets are periodically verified. Based on these actions, this recommendation should be closed.

Recommendation 3 We recommend that the Chief Administrative Officer require the inventory control supervisor to obtain signoff from the Director of Office Supply Service, for all inventory system adjustments.

CONCUR

Effective August 1, 1998, OSS established procedures that require sign-off from the Director of Office Supply Service for all inventory adjustments. Based on these actions, this recommendation should be closed.