MANAGEMENT LETTER REPORT FISCAL YEAR 2008 FINANCIAL STATEMENT AUDIT

Cotton & Company LLP audited Fiscal Year (FY) 2008 financial statements of the U.S. Equal Employment Opportunity Commission (EEOC), and this document discusses eight matters involving internal control that warrant management attention. The status of management's actions on prior-year recommendations is in the appendix.

1. BUDGETARY POSTING LOGIC

We identified three instances of invalid budgetary posting logic during FY 2008 testing, two of which are repeat conditions from FY 2007 (a and b, below):

a. EEOC did not record a budgetary payable to recognize the budgetary effect of a capital lease liability as of September 30, 2008.

The United States Standard General Ledger (USSGL), as published by the Financial Management Service of the Department of the Treasury, states:

…the agency must have sufficient budgetary resources up front to cover the present value of the lease payments discounted using the Treasury interest rates.

The USSGL goes on to require that Delivered Orders – Obligations, Unpaid, be credited to recognize the budgetary payable when the capital lease liability is recorded.

FY 2008 corrective actions were not successfully completed to resolve the issue. EEOC personnel stated that when capital leases were originally entered into, budget authority was not obligated to cover the entire value of the capital lease liability. Thus, they obligate and expend money each year to cover lease payments for that year.

b. EEOC posted invalid recoveries of prior-year obligations.

When correcting administrative data in Momentum, EEOC personnel processed deobligations of prior-year obligations, resulting in postings to GL Accounts 4871 (Downward Adjustments of Prior Year Undelivered Orders) and 4971 (Downward Adjustments of Prior Year Delivered Orders – Unpaid). Because the intent was not to actually deobligate funds, but change administrative data, recoveries of prior-year obligations should not have been generated.

We also identified instances in which recoveries were mistakenly generated when payments were made. Accruals were reversed to pay vendor invoices, resulting in postings to GL Account 4971.

As payments were made on these items, recoveries of prior-year obligations should not have been generated.

The USSGL defines amounts recorded in GL Account 4871 as:

The amount of recoveries during the fiscal year resulting from downward adjustments to USSGL account 4801, "Undelivered Orders - Obligations, Unpaid," that were originally recorded in a prior fiscal year.

Additionally, the USSGL defines amounts recorded in GL Account 4971 as:

The amount of recoveries that were originally recorded in a prior fiscal year during the fiscal year resulting from downward adjustments to USSGL account 4901, "Delivered Orders - Obligations, Unpaid.

c. EEOC did not reduce budgetary revenue when processing yearend deferred revenue accrual.

EEOC's Revolving Fund (RF) provides employment law training to customers for a set fee that customers are required to pay in advance. EEOC records these fees as earned revenue in both the budgetary and proprietary accounts at the time registrations are received, rather than when the training event occurs and the revenue has been earned. We identified this condition during the FY 2007 audit and included this improper accounting treatment in the FY 2007 Management Letter and the FY 2008 internal control report.

EEOC processed a yearend accrual in FY 2008 to properly recognize revenue that had been collected but not yet earned as deferred revenue. When this entry was processed, amounts were moved from GL Account 5200 (Revenue from Services Provided) and posted to GL Account 2320 (Deferred Revenue). Spending authority from offsetting collections (budgetary revenue) was not, however, reduced to recognize that the revenue was not earned and thus did not represent budget authority.

The USSGL prescribes the following entry for recording deferred revenue:

To record revenue received in advance.
Budgetary Entry
None

Proprietary Entry
Debit 1010 Fund Balance With Treasury
Credit 2320 Other Deferred Revenue

A budgetary entry should not be recorded when recording deferred revenue. Thus, budgetary revenue should have been reduced along with proprietary revenue when the yearend accrual was posted.

Recommendation

We recommend that the Office of the Chief Financial Officer (OCFO) implement training procedures to ensure that all financial personnel are familiar with budgetary accounting and reporting guidelines published by the Department of Treasury to ensure that all transactions are properly recorded.

Management Response

Management did not agree with the finding or recommendation. Management stated:

Our review of the SGL indicated that the budgetary accounts were already recorded in Momentum at the time of the receipt of cash - the accounts that were posted in Momentum are:

- *Budgetary Accounts (USSGL transaction code C116):*
- *DR 4261 and CR 4060*
- *Proprietary Accounts:*
- *DR 1010 and CR 5200*

We recorded the Deferred Revenue at September 30 by DR 5200 and CR 2320 – Other Deferred Revenue. No budgetary entry needed to be done at the time of recognizing the deferred revenue because the budgetary accounts were already affected at the time of the cash receipts.

Auditor Comment

As stated in the Management Response, budgetary revenue was recorded in the general ledger at the time cash was received and proprietary revenue was posted. However, this budgetary revenue should not have been recorded at 9/30/08. Per the USSGL, no budgetary entry should be posted when deferred revenue is recorded. As a result, when processing the yearend adjustment to move revenue from earned to deferred, EEOC should have also processed an entry to reverse the budgetary entry that was posted when the earned revenue was recorded during the year. Not posting a reversal of the budgetary entry that was previously recorded caused EEOC to overstate budgetary revenue, as of 9/30/08. As such, this finding is still considered unresolved.

2. SUPPORTING DOCUMENTATION FOR TRANSACTIONS

EEOC personnel were unable to locate sufficient supporting documentation for several sample items selected for testing during FY 2008:

a. OCFO personnel could not provide support for two expense transactions and one undelivered order (UDO) balance selected for yearend testing and could only provide partial documentation for a second UDO balance selected for yearend testing.

b. Office of Human Resources (OHR) personnel could not provide sufficient documentation to support an increase in the annual leave balance of a separated employee that resulted in an increased lump-sum payment to the employee after separation.

GAO's *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1), page 15, states:

…all transactions and other significant events need to be clearly documented and the documentation should be readily available for examination.

Recommendation

We recommend that:

a. OCFO review and revise controls in place to ensure that documentation for all transactions is maintained and is readily available for review.
b. OHR obtain and file all documentation supporting personnel and payroll actions taken and ensure that this information is readily available for review upon request.

Management Response

Management concurs with the finding and recommendation a. No comment was received from management regarding finding and recommendation b.

3. CONTROLS OVER PROPERTY AND EQUIPMENT

Controls over property and equipment (P&E) were not effective in some instances. We identified the following conditions:

a. The Office of Information Technology (OIT) could not physically locate a server.

OIT personnel were unable to locate a Dell Server that was recorded in the property subsidiary ledger and the general ledger at September 30, 2008, stating that the item may have been in transit to EEOC's new headquarters office. We were unable to confirm the existence of the asset prior to the end of our field work.

GAO's *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1), page 14, states:

An agency must establish physical control to secure and safeguard vulnerable assets.

b. Inaccurate and incomplete property information was recorded in the general ledger.

We identified the following inaccuracies in our review of P&E general ledger accounts:

- Accumulated amortization for internal-use software in the Period 12 trial balance exceeded the acquisition cost. EEOC personnel did not reconcile the property subsidiary ledger to the general ledger before yearend and before providing these items for audit. This anomaly was not detected until we brought it to management's attention.
- An asset not meeting the $25,000 capitalization threshold was recorded as a capitalized asset in the general ledger. EEOC personnel did not review the property subsidiary ledger before yearend, and this error was not detected until we brought it to management's attention.
- An asset was erroneously posted to the general ledger twice. EEOC personnel mistakenly concluded that an asset had not been posted during conversion from Integrated Financial Management System (IFMS) to Momentum. Therefore, they processed a journal voucher (JV) entry to add the asset to the general ledger. We identified this item as already recorded in the general ledger when the JV was posted.
- Two assets that met the capitalization threshold were acquired in FY 2008 and recorded in the general ledger, but were not entered into the property subsidiary ledger until after September 30, 2008. This resulted in a difference between the general and subsidiary ledgers at yearend.

GAO's *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1), page 15, states that control activities should be in place:

…to ensure that all transactions are completely and accurately recorded.

c. Property certifications were not submitted in accordance with EEOC policy.

Many offices did not report on results of their physical inventories in a timely manner or at all. Thirteen offices submitted the property certification after the required due date, and three offices did not submit them at all. This condition was noted in FY 2007. FY 2008 corrective actions were not successfully completed to resolve this issue.

GAO's *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1), page 18, states:

Information should be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities.

Recommendation

We recommend that OCFO:

a. Implement training procedures to ensure that all personnel are aware of EEOC policies and procedures over capitalized equipment to ensure that information recorded in the general ledger and subsidiary ledger is accurate.

b. Review and refine controls over the reconciliation of the property subsidiary ledger to the general ledger to ensure that differences are identified and resolved in a timely manner.
c. Report offices that do not submit property certifications in accordance with established policy to the Office of the Chair and require that delinquent offices explain why certifications were not returned within the required timeframe.

Management Response

Management concurs with the findings and recommendations.

4. CONTROLS OVER UNDELIVERED ORDERS AND ACCOUNTS PAYABLE

We identified several instances of invalid UDO and accounts payable balances during FY 2008 testing.

We selected a sample of 60 aged accounts payable during FY 2008. EEOC personnel stated that 8 of these items were no longer valid, because they were residual amounts left over from payments already made or were old payables no longer needed.

OMB Circular A-136, Financial Reporting Requirements, Section 3, Balance Sheet, defines an accounts payable as:

...amounts owed by the reporting entity for goods and services received from other entities...

We selected a sample of 52 UDOs for testing during FY 2008—23 during our review of aged UDOs and 29 as part of our substantive sample of UDOs. EEOC personnel stated that 15 of the aged items were no longer valid, because the recorded UDO balance was not needed at year end and should have been deobligated, or because the goods or services were received, thus the amount should have been accrued as of September 30, 2008. Additionally, we determined that 3 of the UDOs selected as part of our substantive sample of UDOs were invalid, because goods or services were received during FY 2008, and thus accruals should have been processed to record these items as delivered orders – unpaid.

OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, Section 20, Terms and Concepts defines an obligation as:

…a binding agreement that will result in outlays, immediately or in the future.

This condition was noted during the FY 2007 audit. FY 2008 corrective actions were not successfully completed to resolve this issue. During FY 2008, EEOC transitioned from IFMS to Momentum. As a result of this transition, the review of outstanding accounts payable and UDOs was not performed until yearend and was not due from all EEOC offices until October 31, 2008. Many of the responses we received indicated that invalid items were being closed as part of this

review and would be closed as of October 31, 2008. We considered these items to be invalid as of the September 30 fiscal yearend date.

Recommendation

We recommend that OCFO:

a. Revise review procedures over aged accounts payable and UDOs to require that all EEOC offices respond by the fiscal year end to ensure that invalid items are identified and deobligated before yearend financial reports are prepared.
b. Review and refine controls over the accrual process to ensure that accruals are processed to recognize goods and services that have been received.
c. Implement procedures requiring EEOC personnel to identify accounts payable over 3 months old and determine their continued validity. If valid, we recommend that EEOC personnel contact vendors to obtain invoices and ensure timely liquidation. If invalid, we recommend that EEOC personnel remove payable amounts from the accounting system.

Management Response

Management concurs with the findings and recommendations.

5. QUALITY CONTROL PROCEDURES OVER FINANCIAL STATEMENTS

EEOC's quality control procedures over compilation and presentation of financial statements and related footnote disclosures were insufficient to detect errors, omissions, and inconsistencies in the reported information. During our review of the FY 2008 financial statements and the Performance Accountability Report (PAR), we identified the following:

- The following footnote disclosures were not presented in accordance with OMB Circular A-136:
    - The Earmarked Funds Footnote (Note 15) did not present assets, liabilities, net position, costs, and revenues for earmarked funds as required.
    - The Accounts Receivable Footnote (Note 3) did not present the methodology used to calculate the allowance for doubtful accounts as required.
    - The Undelivered Orders Footnote (Note 2) did not present all undelivered orders as required.
- Certain FY 2007 information reported in the footnote disclosures did not tie to audited FY 2007 information, and explanations were not provided in the footnotes. In addition, some footnote disclosures and amounts contained mathematical errors, were reported with incomplete data, and were inconsistent with other disclosures.
- Information on some supporting schedules did not tie to the trial balance or to the footnotes.
- EEOC was unable to provide support to adequately explain a prior-period adjustment.

While most of these errors were corrected after we brought them to the attention of management, it is the responsibility of the reporting agency, not the external auditor, to ensure that information reported in the financial statements is accurate, complete, and presented in accordance with applicable guidelines.

OMB Circular A-127, Federal Financial Systems, Section 6 – Policy, states that federal financial systems:

…shall provide complete, reliable, consistent, timely and useful financial management information….

Recommendation

We recommend that OCFO improve quality control procedures for reviewing final versions of financial statements and related footnotes prior to submission to auditors, to ensure that financial information to be reported in PARs is complete, accurate, consistent, and timely.

Management Response

Management concurs with the findings and recommendations.

6. SECURITY VIOLATIONS REVIEW

EEOC did not review security violations for the Federal Personnel/Process System (FPPS), Hyperion, and Momentum systems proactively and in a timely manner. Management has not established policies for reviewing security violations for outsourced systems and for reviewing them in a timely manner. EEOC places responsibility of security violation reviews on the National Business Center (NBC). NBC, however, does not perform security violation reviews at the application level for the outsourced system. Reviews performed by NBC cover only the infrastructure and operating system portions for which it is responsible. Its reviews do not include applications, which are the responsibility of EEOC.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 1, Recommended Security Controls for Federal Information Systems: AU-6 – Audit Monitoring, Analysis, and Reporting, provides the following guidance:

The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Recommendation

We recommend that EEOC management develop and implement policies and procedures for ensuring that application security violations for outsourced applications are appropriately reviewed and reported.

Management Response

Management concurs with the findings and recommendations.

7. SEGREGATION OF DUTIES

EEOC has not formally identified and documented incompatible duties for the FPPS and Momentum applications. Management was unable to provide documentation regarding an analysis of what roles should be segregated because of incompatible job functions.

NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems (July 2008), provides the following guidance:

AC-5.1: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

IT Governance Institute, CoBIT 4.1, PO 4.11, Segregation of Duties, provides the following additional guidance:

Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorized duties relevant to their respective jobs and positions.

Recommendation

We recommend that EEOC develop policies for formally analyzing and reviewing all roles to identify incompatible duties. Additionally, we recommend that EEOC develop and document a process outlining functions that have been identified as having incompatible abilities. The results should be incorporated into the account request process to ensure individuals are not requesting incompatible duties.

Management Response

Management concurs with the findings and recommendations.

8. APPLICATION CONTROLS REVIEW

EEOC did not have controls to ensure that management appropriately reviewed, documented, and addressed client-control considerations for the FPPS, Hyperion, and Momentum applications. These applications are addressed by a Statement of Auditing Standards (SAS) 70 Type II report. Client controls, identified in the SAS 70 reports, highlight user-organization

internal control responsibilities that the outsourced-provider relies upon to achieve a secure operating environment. These represent, at a minimum, controls for which EEOC is responsible to ensure that outsourced applications and data are protected adequately. EEOC does not have a process to ensure that these controls are in place.

NIST SP 800-53 Revision 1, Recommended Security Controls for Federal Information Systems, SA-9 External Information System Services, provides the following guidance:

The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.

Ultimately, the responsibility for adequately mitigating risks to organization's operations and assets and to individuals arising from use of external information system services remains with the authorizing official, not with the service provider.

Recommendation

We recommend that EEOC develop policies and procedures for reviewing SAS 70 reports for outsourced systems and ensuring that all appropriate security and management personnel are involved in the application review process, especially the SAS 70 reviews. We recommend that security and management personnel be involved in the control design and implementation process.

Management Response

Management concurs with the findings and recommendations.

APPENDIX
STATUS OF MANAGEMENT'S ACTIONS ON PRIOR-YEAR RECOMMENDATIONS
FISCAL YEAR 2008 FINANCIAL STATEMENT AUDIT
U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

See Attachment 2 for Management responses to unresolved prior year findings and recommendations.

Recommendation	Status as of November 7, 2008
FY 2007 conditions related to Budgetary Posting Logic:	Unresolved. Repeat

a. We recommend that the Office of the Chief Financial Officer (OCFO) implement training procedures to ensure that all financial personnel are familiar with accounting and reporting guidelines published by the Department of Treasury to ensure that all transactions are properly recorded.	conditions in FY 2008.
b. We recommend that EEOC review the posting logic within Momentum to ensure that only valid postings are made when payment transactions are processed. We also recommend that EEOC consider implementing procedures to periodically analyze GL postings to ensure that the desired effect is being achieved within the financial systems.	Modified recommendation to address new accounting system.
FY 2007 condition related to Controls over Capital Leases: We recommend that OCFO review and revise procedures in place over recording and disposing of capital leases to ensure that all capital assets are properly recorded in FAS and that supporting documentation for all transactions posted is maintained and is readily available for review.	Unresolved. Modified repeat condition in FY 2008.
FY 2007 condition related to Improper Revenue Recognition: We recommend that OCFO coordinate with the Director of RFD to establish procedures to recognize revenue on a full accrual basis consistent with generally accepted accounting principles. We recommend that training service revenue be recognized when earned, regardless of when the cash payment takes place. Customer payments received in advance should be recorded as deferred revenue to recognize a liability for the future provision of services.	Unresolved. Repeat condition. Included in FY 2008 internal control report.
FY 2005 through 2007 conditions related to Outstanding Accounts Payable and Undelivered Order (UDO) Balances: a. We recommend that the Chief Financial Officer (CFO) continue to refine the accounts payable and UDO review process implemented during FY 2007 to ensure that all recorded balances at year end are valid.	Unresolved. Repeat condition in FY 2008.
b. We recommend that the OCFO implement procedures requiring EEOC personnel to contact vendors to obtain invoices for accounts payable that are over 3 months old to ensure timely liquidation of recorded payables.	Unresolved. Repeat condition in FY 2008.
FY 2006 and 2007 conditions related to Quality Assurance Procedures over the Financial Statements: We recommend that the OCFO improve quality control procedures for	Unresolved. Repeat condition in FY 2008.

reviewing final versions of the financial statements and related footnotes to ensure that financial information to be reported in the PAR is complete, accurate, consistent, and timely.	
FY 2006 and 2007 conditions related to Physical Inventory of Accountable Property: a. We recommend that EEOC establish policies and procedures requiring the OCFO to notify the Division Director responsible for any office not submitting "property certifications." Upon notification from the OCFO, the Division Director should be given 30 days to either provide the property certification or provide a written explanation as to why the property certification cannot be completed. We recommend that EEOC implement policies and procedures to ensure that all Forms 629 (Report of Loss, Theft or Incident) are provided to the Security Specialist in a timely manner to ensure that all losses are promptly reported and investigated.	Unresolved. Repeat Condition in FY 2008. Completed.
FY 2007 condition related to Internal-Use Software: We recommend that OCFO coordinate with OIT to improve communication among divisions to ensure that requested information is received in a timely manner. We also recommend that OCFO and OIT coordinate to ensure that documentation supporting inquiries made and costs incurred is maintained and is readily available for review.	Completed.
FY 2007 condition related to Segregation of Duties over Cash Receipts: We recommend that OCFO coordinate with the Director of the Revolving Fund Division (RFD) to segregate potentially incompatible functions at the contractor office assigned to handle cash receipts by making assignments to prevent a single individual from opening mail, entering transactions in the general ledger, and processing bank deposits.	Completed.
FY 2007 condition related to Background Investigations: We recommended that EEOC complete background investigations for all employees and contractors, as appropriate, in accordance with federal guidelines and recommendations, as well as EEOC department guidelines and document, record, and maintain evidence of these investigations.	Unresolved.
FY 2007 condition related to Outsourced System Account Administration: We recommended that EEOC develop, document, and implement policies and procedures for reviewing user accounts on FPPS. We also recommended that EEOC review user listings against terminated and	Unresolved.

separated employee listings on a continual basis to ensure that only appropriate users have active accounts.	
FY 2006 and 2007 conditions related to Network Password Weaknesses: We recommend that OIT revise its policy for password minimum length, expiration/change interval, and account lockout to adhere to industry best practices. We also recommended that EEOC implement the strengthened password policies in the system and ensure that they comply with industry best practices. We recommended the following changes to strengthen network password controls: • Password minimum length = 6 to 18 (18 for administrative accounts) • Password expiration = 30 to 90 days (30 for administrative accounts) User lockout = minimum of 12 hours or until reset	Completed.
FY 2006 and 2007 conditions related to Removal of System Access for Terminated Employees and Inactive Accounts: We recommended that OIT develop and implement procedures to guide the review of network accounts for inactivity. The procedures should define an allowable number of days before the account is removed or disabled. The allowable time period should be based on industry standards.	Completed.
FY 2006 and 2007 conditions related to Internal Penetration Results: We recommended that OIT develop full standard configurations for the platforms in use and ensure that these configurations meet recommendations of industry best practices, NIST, and NSA and are applied to all machines sitting on the network. We also recommended that OIT ensure that users and administrators are properly trained on the use of strong password for all accounts.	Completed.
FY 2006 and 2007 condition related to Vulnerability Assessment Results: We recommended that OIT ensure that the necessary software patches and security hot-fixes are installed on the network in a timely manner. We recommended that OIT update its baseline configuration document for the network and ensure that these configurations comply with the industry best practices, NIST, and NSA. The strengthened configurations should then be applied to all machines sitting on the EEOC network.	Completed.
FY 2007 condition related to Security Program Plan: We recommended that EEOC update the IT security program plan to include the following key areas:	Completed.

• Personnel Security • Technical Security System Interconnection/Information Sharing	
FY 2007 condition related to Certification and Accreditation: We recommended that EEOC conduct risk assessments and ST&Es for outsourced-system-control areas for which EEOC is responsible as part of a comprehensive C&A process.	Completed.
FY 2007 condition related to Whole Disk Encryption: We recommended that EEOC implement whole disk encryption for all mobile devices/computers in accordance with federal regulations and guidelines. If data are determined to be non-sensitive, the agency deputy secretary or designee must verify this in writing.	Completed.
FY 2007 condition related to Access Authorization Documentation: We recommended that EEOC develop, document, and implement policies and procedures to collect access request forms from all users, including users located in field offices. We also recommended that EEOC revise its current policies for reviewing account access to require that these forms be maintained on file for future reference.	Completed.