GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 31, 2010

The Honorable Mary L. Schapiro
Chairman
U.S. Securities and Exchange Commission

Subject: *Management Report: Improvements Needed in SEC's Internal Controls and Accounting Procedures*

Dear Ms. Schapiro:

On November 16, 2009, we issued our opinion on the U.S. Securities and Exchange Commission's (SEC) fiscal years 2009 and 2008 financial statements. We also issued our opinion on the effectiveness of SEC's internal controls over financial reporting as of September 30, 2009, and our evaluation of SEC's compliance with selected provisions of laws and regulations during fiscal year 2009.[1]

The purpose of this report is to present (1) our recommendations related to the significant deficiencies we reported and discussed in our opinion report;[2] (2) less significant internal control issues we identified during our fiscal year 2009 audit of SEC's internal controls and accounting procedures, along with our related recommended corrective actions; (3) the status of the recommendations reported as open in our April 2, 2009, management report[3] (see enclosure I), and (4) the status of the security weaknesses in information systems controls at SEC that we identified in public and "Limited Official Use Only" reports issued in 2005, 2007, 2008, and 2009,[4] (see enclosure II) that were unresolved at the time of our March 16, 2009, information security reports.[5]

---

[1]GAO, *Financial Audit: Securities and Exchange Commission's Financial Statements for Fiscal Years 2009 and 2008*, GAO-10-250 (Washington, D.C.: Nov. 16, 2009).
[2]The significant deficiencies are detailed in *Appendix I: Material Weaknesses of* GAO-10-250. These weaknesses collectively resulted in a material weakness over SEC's financial reporting.
[3]GAO, *Management Report: Improvements Needed in SEC's Internal Controls and Accounting Procedures*, GAO-09-376R (Washington, D.C.: Apr. 2, 2009).
[4]*GAO, Information Security: Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data*, GAO-05-262 (Washington, D.C.: Mar. 23, 2005); *GAO, LIMITED OFFICIAL USE ONLY Information Security: Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data*, GAO-05-263SU (Washington, D.C.: Mar. 23, 2005); *GAO, Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program*, GAO-06-408 (Washington, D.C.: Mar. 31, 2006); GAO, *LIMITED OFFICIAL USE ONLY Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program*, GAO-06-407SU (Washington, D.C.: Mar. 31, 2006); *GAO,*

Results in Brief

As part of our audit of SEC's fiscal years 2009 and 2008 financial statements, we identified a material weakness[6] in internal control over financial reporting that resulted from the cumulative effect of significant deficiencies we identified in six key areas of SEC's controls over financial reporting.[7] These significant deficiencies concerned controls over:

- information security,
- financial reporting process,
- fund balance with Treasury,
- registrant deposits,
- budgetary resources, and
- risk assessment and monitoring processes.

We discussed these significant deficiencies in detail in our audit opinion on the SEC's fiscal years 2009 and 2008 financial statements.[8] We are making a total of 25 new recommendations related to these six significant deficiencies that are presented, along with a brief description of the deficiency, in the following sections.

We also identified other internal control issues that although not considered material weaknesses or significant deficiencies, warrant SEC management's consideration. These issues concern:

- security over sensitive employee information,
- policies and procedures documents related to or affecting financial reporting,
- documentation of payroll controls,

Information Security: Sustained Progress LIMITED OFFICIAL USE ONLY Needed to Strengthen Controls at the Securities and Exchange Commission GAO-07-256, (Washington, D.C.: Mar. 27, 2007); GAO, *LIMITED OFFICIAL USE ONLY Information Security: Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission*, GAO-07-257SU, (Washington, D.C.: Mar. 27, 2007); GAO, *Information Security: SEC Needs to Continue to Improve Its Program*, GAO-08-280 (Washington, D.C.: Feb. 29, 2008); GAO, *LIMITED OFFICIAL USE ONLY Information Security: SEC Needs to Continue to Improve Its Program*, GAO-08-279SU (Washington, D.C.: Feb. 29, 2008); GAO, *Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls*, GAO-09-203 (Washington, D.C.: Mar. 16, 2009); GAO, *LIMITED OFFICIAL USE ONLY Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls*, GAO-09-204SU (Washington, D.C.: Mar. 16, 2009).

[5]GAO-09-203 *and* GAO-09-204SU.

[6]A material weakness is a significant deficiency or combination of deficiencies in internal control, such that, there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected.

[7]A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

[8]GAO-10-250.

- prior period corrections,
- preparation of labor surveys,
- Prompt Payment Act interest payments,
- excessive user access rights in SEC's time and attendance system,
- financial statement closing schedule: cutoffs and related activities,
- documentation of Contracting Officer's Technical Representative's review of contractor invoices prior to SEC payment, and
- notes to interim financial statements and pro-forma financial reporting.

We present a discussion of our findings and related recommendations for each of these less significant control deficiencies following the presentation of our recommendations to address SEC's significant financial reporting deficiencies. We are making a total of 18 new recommendations related to these less significant control deficiencies.

Enclosure I provides the status of the recommendations from our prior audits at the conclusion of our fiscal year 2009 audit. By the end of our fiscal year 2009 audit SEC took action to fully address 22 of the 43 recommendations from our prior audits that were open at the time of our April 2, 2009, management report.[9] We also closed 14 other recommendations for which SEC had substantially implemented the recommendations or had implemented alternative controls consistent with the intent of our recommendations. Seven of the 43 recommendations from our prior audits remained open as of the end of fiscal year 2009.

The 43 new recommendations made in this report include recommendations related to the alternative controls SEC implemented in response to our prior recommendations and recommendations that were substantially but not fully implemented. For example, SEC improved its recording of disgorgement and penalty transactions to the extent that it integrated the accounts receivable module with the general ledger. However, we continued to find deficiencies related to non-integrated processes for other types of disgorgement and penalty transactions. Consequently, we are issuing new recommendations that more specifically address the underlying weaknesses we found in those areas.

We did not identify any new weaknesses concerning information security controls during our fiscal year 2009 audit. However, of the 43 new recommendations, 2 relate to the continuing weaknesses in information security controls. Enclosure II presents a summary of the status of SEC's actions to address previously reported information system security weaknesses. Specifically, as shown in the table in enclosure II, during fiscal year 2009, SEC took action to fully address 21 of the 43 security weaknesses in information systems controls which GAO identified in previous reports, leaving 22 weaknesses which SEC had not taken actions to fully correct as of the end of fiscal year 2009.

[9]GAO-09-376R.

In providing written comments on a draft of this report, the SEC Chairman stated remediating the material weakness in internal control over financial reporting is a top priority. The Chairman discussed work to strengthen internal controls that SEC has already begun, including retaining the services of an independent consulting firm to assist SEC in its efforts. The Chairman also discussed SEC's longer-term effort to fully integrate its financial systems and that SEC is developing a formal remediation plan to fully address the identified significant deficiencies.

Scope and Methodology

As part of our audit of SEC's fiscal years 2009 and 2008 financial statements, we evaluated SEC's internal controls over financial reporting and tested its compliance with selected provisions of laws and regulations. We designed our audit procedures to test relevant controls over financial reporting, including those designed to provide reasonable assurance that transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in conformity with U.S. generally accepted accounting principles, and that assets are safeguarded against loss from unauthorized acquisition, use, or disposition.

We requested comments on a draft of this report from the SEC Chairman. SEC's written comments are reprinted in enclosure III. We conducted our audit in accordance with U.S. generally accepted government auditing standards. Further details on our scope and methodology are included in our November 2009 report on our audits of SEC's fiscal years 2009 and 2008 financial statements and are summarized in enclosure IV.

Recommendations Related to Significant Deficiencies Discussed in Our November 2009 Opinion Report

During our fiscal year 2009 audit of SEC's controls over financial reporting, we identified six significant deficiencies:

- information security,
- financial reporting process,
- fund balance with Treasury,
- registrant deposits,
- budgetary resources, and
- risk assessment and monitoring processes.

These deficiencies collectively represented a material weakness in internal control. Our findings related to each of these deficiencies are detailed in our opinion report and briefly highlighted in the following sections. Our related recommendations are also presented here.

Information Security

We identified weaknesses in SEC's information security controls over key financial reporting systems. Specifically, we found that SEC did not adequately:

- segregate computer-related duties and functions;
- restrict user privileges;
- implement patches and current software versions;
- use approved, secure means to transmit data;
- implement configuration management; and
- complete a certification and accreditation of its general ledger system and supporting processes during the fiscal year.

These control weaknesses jeopardize the confidentiality, availability, and integrity of automated information processed by SEC's financial reporting systems, thereby increasing the risk of material misstatement in financial reporting and the risk of unauthorized modification or destruction of data.

The information security weaknesses we found are similar to those found in our prior financial audits of SEC and relate to 22 of our prior weaknesses that remained unaddressed at the conclusion of our audit. The status of SEC's actions to address these information security control weaknesses is summarized in enclosure II.

Recommendations for Executive Action

In addition to completing actions to address the 22 outstanding previously reported automated system security-related weaknesses, we recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve automated information system security controls:

1. Reevaluate existing automated information system security controls in light of the risks identified in SEC's October 2009 certification and accreditation procedures for the general ledger system and supporting processes.
2. Establish and implement appropriate controls to mitigate any additional risks that were identified as a result of this reevaluation.

Financial Reporting Process

We identified deficiencies in SEC's general ledger system, configurations, and financial reporting processes that prevent management from generating accurate, complete, and timely transaction-level financial information needed to readily report reliable and useful financial information. In addition, as we also found SEC's controls did not always effectively detect misstatements that could occur as a result of SEC's extensive use of manual workarounds and data handling in its financial reporting processes. Specifically, we found (1) lack of capability for

generating useful financial reports, (2) lack of systems integration, (3) unconventional general ledger posting models, and (4) lack of reliability in SEC's accounting and reporting of contingent liabilities and intragovernmental liabilities. As a result, management placed continued reliance on manual compensating controls which are cumbersome, detective in nature, and prone to error. The following paragraphs present an overview of our findings we identified related to the financial reporting process and our related recommendations.

Capability for Generating Useful Financial Reports

Office of Management and Budget (OMB) Circular No. A-127, *Financial Management Systems* (2004),[10] provides that the agency financial management system shall be able to provide financial information in a timely and useful fashion to (1) support management's fiduciary role; (2) support the legal, regulatory, and other special management requirements of the agency; (3) support budget formulation and execution functions; (4) support fiscal management of program delivery and program decision making; (5) comply with internal and external reporting requirements, including, as necessary, the requirements for financial statements prepared in accordance with the form and content prescribed by OMB and reporting requirements prescribed by Treasury; and (6) monitor the financial management system to ensure the integrity of financial data.

As we reported in fiscal year 2008,[11] SEC upgraded its general ledger system and implemented two new system modules to automate SEC's accounting for disgorgement and penalty[12] accounts receivable and property and equipment transactions. However, during our fiscal year 2009 audit, we found that SEC's general ledger system and sub-modules lacked the functionality and proper configuration to generate and report financial information necessary for the preparation of the financial statements and the management of day-to-day operations on an ongoing basis. Management was unable to produce standard reports at a point in time that reconcile to the related general ledger balances. For example:

- The general ledger system was unable to accurately generate a consolidated trial balance.[13] Consequently, monthly financial statements

[10]GAO tested SEC's financial management systems against the 2004 version of OMB Circular No. A-127, which was effective through the end of fiscal year 2009. SEC will be required to comply with the requirements in the 2009 version of A-127 during fiscal year 2010.
[11]GAO, *Financial Audit: SEC's Financial Statements for Fiscal Years 2008 and 2007*, GAO-09-173 (Washington, D.C.: Nov. 14, 2008).
[12]A disgorgement is the repayment of illegally gained profits (or avoided losses) for distribution to harmed investors whenever feasible. A penalty is a monetary payment from a violator of securities law that SEC obtains pursuant to statutory authority. A penalty is fundamentally a punitive measure, although penalties occasionally can be used to compensate harmed investors.
[13]A trial balance is a listing of proprietary and budgetary U.S. standard general ledger accounts and balances recorded as of a point in time (i.e., a specific date); the values for the proprietary and budgetary accounts are self-balancing; that is, the debits equal the credits for each type of account. A consolidated trial balance is an aggregation of trial balances for each type of account.

and trial balance reports were generated through a financial reporting database that lacks system controls necessary to preserve the integrity of financial data. As a result, SEC is at increased risk of material misstatement in financial reporting. For example, we identified a discrepancy between certain general ledger account balances obtained directly from the general ledger system reports and the related balances in SEC's financial reporting database resulting from the exclusion of a few manual payments in the general ledger system reports.

- The general ledger system could not produce an undelivered order aging report to identify outstanding obligations for potential deobligation.[14] Instead, SEC personnel manually extracted open obligations data from the general ledger and performed queries of the resulting file to identify outstanding obligations. During our fiscal year 2009 audit, we found that this process did not identify numerous outstanding travel obligations totaling over $1 million that should have been deobligated. As a result of this error, SEC's accounts payable accrual and obligated balances at June 30, 2009, were overstated.
- The general ledger could not produce an aging report of its disgorgement and penalties accounts receivables. As a result, SEC personnel manually prepared a spreadsheet to support the accounts receivable balance reported in the financial statements. The initial spreadsheet SEC prepared at September 30, 2009, contained inaccurate data and required multiple iterative corrections.
- The property module could not generate a property register readily supported balances reported on the financial statements. To compensate, management executed manual queries of property data to extract cost, accumulated depreciation, and other pertinent information to generate a property register that could be reconciled to the account balances.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions to improve period-end financial reporting process controls:

3. Reconfigure the general ledger system to produce reports necessary to both prepare the financial statements and support managing operations, such as a consolidated trial balance report and undelivered order aging report, respectively, on an ongoing basis.
4. Reconfigure the disgorgements and penalty accounts receivable module to enable production of an accounts receivable aging report.
5. Reconfigure the property and equipment module to enable production of a property register report.

[14]An obligation is a definite commitment that creates a legal liability of the government for the payment of goods and services ordered or received, or a legal duty on the part of the United States that could mature into a legal liability by virtue of actions on the part of the other party beyond the control of the United States. Deobligation refers to an agency's cancellation or downward adjustment of previously incurred obligations.

Lack of Systems Integration

OMB Circular No. A-127, *Financial Management Systems* (2004), provides that the agency financial management system shall be designed to provide for effective and efficient interrelationships between software, hardware, personnel, procedures, controls and data contained within the system. In doing so, the agency's financial management system shall eliminate unnecessary duplication of transaction entry, as appropriate. Data needed by the system to support financial functions shall be entered only once, and other parts of the system shall be updated through electronic means.

We found SEC's controls were not always effective in detecting misstatements that could occur as a result of SEC's extensive use of manual workarounds and data handling in its financial reporting processes due to certain key processes that were not integrated with the general ledger system. Investment activity related to collections of disgorgements and penalties were not captured in the general ledger at the enforcement case level and the recording of disgorgement and penalty information was entered twice because the two systems that capture the information are not integrated, specifically:

- SEC invests disgorgement funds in Treasury securities and managed such investments using spreadsheets. The general ledger did not capture detailed investment activity and disgorgement and penalty liability activity at the enforcement case level. SEC used a large unsecured spreadsheet, which was not integrated with the general ledger, to deconstruct the summary level disgorgement and penalty data in the general ledger to the case level. Use of this spreadsheet increases the risk of incomplete recording of investment and other data that would not be detected in a timely manner. During our fiscal year 2009 review of this spreadsheet, we noted numerous differences in the calculated balances and related balances maintained by Treasury. The ability to have detailed data at the case level is important in order to effectively manage the investments and cash amounts attributable to the individual enforcement cases.
- SEC has not developed an automated interface between its disgorgement and penalty accounts receivable module, which is integrated with its general ledger system, and Phoenix—the database that is the source of the disgorgement and penalty data. Instead, disgorgement and penalty information is first manually entered into Phoenix and then again manually entered into the accounts receivable module using weekly data extracts from Phoenix. Given the use of two manual entry points for similar information, significant analysis, reconciliation, and review are performed outside the system to ensure amounts were appropriately entered into the accounts receivable module. As a result, resources are unnecessarily wasted from this duplication of efforts and increase the risk of error with the second recording of the transaction.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions to improve period-end financial reporting process controls:

6. Develop and implement an automated sub-ledger that interfaces with the general ledger for investment and disgorgement and penalty liability transaction activity.
7. Until SEC is able to establish and implement procedures for fully integrating its detailed investment and disgorgement liability activity into its general ledger, establish and implement procedures for documenting data reliability checks at the enforcement case level for data extracted from non-integrated subsidiary systems to include appropriate supervisory reviews.
8. Develop and implement an automated solution that will eliminate the manual process of reentering disgorgement and penalties data from Phoenix into the general ledger system accounts receivable module.

Unconventional General Ledger Posting Models

OMB Circular No. A-127, *Financial Management Systems* (2004), states that the agencywide Financial Information Classification Structure shall be consistent with the U.S. Standard General Ledger (SGL). For the federal government, Treasury, through the Treasury Financial Manual (TFM), provides federal agencies the list of SGL accounts, their definition, and guidance regarding the use of SGL accounts in accounting transactions for events occurring throughout the federal government. These transactions document the basic standard posting logic for financial events across the federal government, which federal agencies should follow in order to comply with the SGL policy prescribed by both OMB and Treasury. Moreover, *Standards for Internal Control in the Federal Government*[15] states that financial transactions and events should be accurately and timely recorded to maintain their relevance and value to management in controlling operations and making decisions.

During our fiscal year 2009 audit, we found SEC's general ledger system had several unconventional posting models, not consistent with posting models prescribed in the TFM, that necessitated extensive research to identify and correct for through the posting of correction-type journal voucher (JV) and standard voucher (SV) transactions, for example:

- SEC's general ledger did not recognize and properly record payments made through the Department of the Interior (DOI)[16] for student loan payments,

[15]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).
[16]The DOI's National Business Center (NBC) is SEC's payroll service provider. Student loan payments and employee awards are typical transactions processed through SEC's payroll.

employee awards, and employee litigation settlements to the related obligation. When such payments occur, the automated entries from DOI result in, among others, (1) accounting entries that duplicate previously recorded expenses and allotments—realized resources, and (2) recording of an upward adjustment to prior year delivered orders—obligations unpaid when no such activity should be recorded. In addition, the related liability is not reduced when the payment is recorded. To compensate, SEC staff perform extensive ad-hoc queries to develop several correcting JV entries, including the recording of other transactions with no underlying financial activity, that are intended to link liquidation activity to the related obligation and correct the automated entry discussed above. As a result, SEC's general ledger routinely included many accounting entries that do not represent true financial transactions and is therefore inaccurate until the correcting entries have been made.

- SEC utilizes SV transactions to record a variety of adjustments in its general ledger system resulting from the improper posting of property and equipment transactions. According to SEC policy, an itemized receipt is processed in its general ledger system when property and equipment assets are received. If processed accordingly, an itemized receipt document should automatically capitalize the cost of the item to the related asset accounts. Our review found that because SEC personnel do not consistently process receipt documents as assets are received, the general ledger system is unable to record property transactions to the appropriate general ledger account. Consequently, SEC routinely used SVs to reclassify asset costs that were erroneously expensed. As a result of these improper postings, SEC relied upon a contractor's weekly analysis of expense account transactions to identify items that were erroneously expensed and reclassify such payment, as appropriate.
- Our audit work identified several obligation-related transactions that were recorded in fiscal year 2009 as a result of incorrect posting models for budget transactions. As a result of these improper postings, SEC routinely recorded correcting JV transactions.

As these examples show, SEC's general ledger contains numerous automated entries and subsequent corrections that do not represent actual activity that should be recorded in these respective accounts. Such posting obscure management's ability to discern true activity from erroneous, adjusted-for, transactions. During our audit, we found several instances of adjustment type entries that were indistinguishable from actual activity in account reconciliations that were provided for our review. Moreover, in fiscal year 2009, SEC has invested resources to standardize the recording of correcting accounting entries that were systemically posted incorrectly rather than correcting underlying systems configurations.

Because its general ledger accounting system cannot readily produce relevant financial reports and subsidiary systems are not fully integrated with the general ledger, SEC and contractor personnel perform labor-intensive efforts to produce

reliable financial reports within mandated timeframes. In addition, the system reporting deficiencies discussed above result in SEC personnel performing significant manipulation of data using unsecured spreadsheets so that the data can be reconciled, managed, and reported accurately. Moreover, these conditions result in delays in the recording of the true accounting events. Such reliance on manual controls, which are largely detective in nature, increases the risk that material misstatement may occur in the financial statements.

To help address the significant deficiency in internal control over the financial reporting process, specifically unconventional general ledger posting models for budget transactions, we reaffirm our open recommendation from our prior audits related to correcting general ledger system configurations for upward and downward adjustments. The status of our open recommendation is summarized in enclosure I.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions to improve period-end financial reporting process controls:

9. In coordination with the DOI's National Business Center (NBC), establish and implement a cost effective procedure for accurately recording student loan payments and employee awards in the general ledger.
10. Establish and implement procedures to properly record property and equipment receipt transactions using capitalizable project and budget object class codes within the general ledger system.
11. Establish and implement procedures for performing a comprehensive review of all posting configurations and recurring correcting journal entries to identify and address any additional departures from Treasury's prescribed posting models.

Accounting and Reporting of Contingent and Intragovernmental Liabilities

We also found that SEC did not have an effective process for recording and disclosing contingent liabilities and accruing certain intragovernmental accounts payable. Both control weaknesses adversely affected the reliability of SEC's financial statements during fiscal year 2009.

OMB Circular No. A-136, *Financial Reporting Requirements* (rev. 2009), provides that agency management must make an assessment as to whether pending, threatened litigation or unasserted claims should be reported or disclosed in the financial statements. This determination extends to cases in which legal counsel has classified the likelihood of loss as "unknown." In addition, according to Statement of Federal Financial Accounting Standards (SFFAS) No. 5, *Accounting for Liabilities of the Federal Government*, an estimated liability may be a specific amount or a range of amounts. If some amount within the range is a better estimate than any other amount within the range, that amount is recognized. If no

amount within the range is a better estimate than any other amount, the minimum amount in the range is recognized and a description of the nature of the contingency should be disclosed. In addition, disclosure of a contingency should include the nature of the contingency and an estimate of the possible liability, an estimate of the range of the possible liability, or a statement that such an estimate cannot be made.

During our audit, we found that SEC did not report $9.5 million of contingent liabilities from two cases in its interim financial statements and appropriately disclose contingent liabilities in the related note at June 30, 2009. Of this amount, SEC's general counsel had already determined a $500,000 probable loss to the SEC. Moreover, we found that an adverse ruling had been issued the previous fiscal year on a related case. However, despite that adverse ruling, we found that applicable divisions in SEC had not initiated actions to estimate the additional contingent liability that may result from the adverse ruling in preparing the June 30, 2009, interim financial statements. As a result, certain amounts in SEC's interim financial statements were significantly misstated. Based on the adverse ruling, SEC later calculated the estimated range of loss and recorded $9.5 million of contingent liabilities, which included the $500,000 probable loss discussed above, for its yearend financial statements. We also found that SEC's period-end financial reporting process did not detect unrecorded liabilities of about $5 million from the settlement of certain cases detailed in the lawyers' final updated legal representation letter to GAO.

SEC did not timely and accurately report and disclose contingent liabilities in its financial statements because it did not have a documented process for identifying, evaluating, and accounting for litigation, claims, and assessments as part of its process for preparing its financial statements. SEC officials stated that in preparing the management schedule, management relies on the information contained in the legal representation letter and only updates the contingency note on an annual basis.[17] Until effective procedures for identifying, evaluating, and accounting for litigation, claims, and assessments have been developed and implemented, ongoing reliability of SEC's financial statements and related note disclosures may not be assured.

During our fiscal year 2009 audit, we also found that SEC's period-end financial reporting process did not appropriately account for certain intragovernmental accruals in accordance with its own guidance and generally accepted accounting principles (GAAP). Our review of SEC's accrual of intragovernmental expense and

[17]OMB Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements, (as amended)* describes the management schedule as the schedule the CFO prepares to document how the information contained in the legal counsel's response was considered in preparing the financial statements to satisfy management's responsibilities under SFFAS No. 5, *Accounting for Liabilities of the Federal Government*, as amended, related to contingent liabilities arising from litigation. Specifically, the schedule should reflect management's conclusion as to the likelihood of loss about each case to determine whether an amount should be recorded in the financial statements and/or if note disclosure is necessary for the financial statements to conform with U.S. GAAP.

payable amounts with the General Services Administration (GSA) at September 30, 2009, found that SEC allocated an unsupported payable amount of approximately $7.7 million to contracts with GSA. Specifically, SEC recorded the GSA-stated receivable balance without reconciling such data to internal records. Further, because the intragovernmental balance provided by GSA was a net total and did not identify the related contracts numbers, SEC chose to allocate GSA's stated balance amongst the contracts with the highest amount of unliquidated obligations until the amount was absorbed.

According to SEC's *Accounts Payable Accrual As-Is Process* documentation,[18] accounts payable accruals should be made for items where a good or service has been received in the current month but will not be paid for prior to month-end. The process document also provides, among other things, that accruals are based on actual invoices for goods and services received and the corresponding period of performance. All unliquidated obligations greater than $400,000, are individually tracked for accrual purposes. Under SEC administrative regulations, the Contracting Officer's Technical Representative (COTR) is responsible for the review and processing of all invoices and ensuring that supplies are delivered and/or services are performed according to the provisions of the contract. COTRs are to document and maintain records that sufficiently describe all actions.

According to SFFAS No. 5, *Accounting for Liabilities of the Federal Government*, a liability for federal accounting purposes is a probable future outflow or other sacrifice of resources as a result of past transactions or events, such as receipt of goods and services.

Because SEC did not follow its own documented process and lacked COTR review in accruing certain of its intragovernmental liabilities, its accrual of amounts payable to GSA lacked the detailed support to determine (1) whether the recorded accounts payable balances provided by GSA are related to SEC, (2) the proper accounting of the related expenses and reporting of related costs in its Statement of Net Cost, (3) whether the related goods or services have been received, and (4) if expenses may have been recorded twice. As a result, the ongoing reliability of SEC's financial statements may not be assured.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions to improve period-end financial reporting process controls related to contingent and intragovernmental liabilities:

12. Develop and implement policies and procedures to identify, evaluate, and account for contingencies related to any litigation, claims, and assessments against SEC as part of the routine preparation of financial statements in conformity with generally accepted accounting principles.

[18]OFM-09-02-AIP, dated May 14, 2009.

13. Develop or update and implement policies and procedures for reconciling any SEC intragovernmental expense and payable amounts reported by GSA to internal SEC data records prior to recording an accrual in SEC's general ledger for financial statement reporting.
14. Develop and implement control and verification procedures to ensure all of SEC's contingency and intragovernmental liability transactions comply with SEC's *Accounts Payable Accrual As-Is Process* documentation.

Fund Balance with Treasury

During our audit of SEC's fiscal year 2009 financial statements, we identified a significant deficiency concerning SEC's inability to perform the required monthly reconciliations of its Fund Balance with Treasury (FBWT) accounts and adequately resolve differences in disbursements between SEC's and Treasury's records of such disbursements. *The Treasury Financial Manual*, *Part 2 Chapter 5100 Supplement*, provides that all agencies must complete and fully document a reconciliation of FBWT monthly. The reconciliation should be approved by an authorized agency official as evidences that the reconciliation was properly completed and reviewed. Federal agencies are also required to research and resolve differences reported on the monthly Statement of Differences (Treasury's Financial Management Service 6652).As a result of this weakness, SEC is at an increased risk (1) that the accuracy and timeliness of deposit and disbursement data reflected in SEC's FBWT and related accounts are misstated and (2) of fraud, violations of appropriations laws, and mismanagement of funds.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve period-end FBWT financial reporting process controls:

15. Develop and implement procedures for timely performing, reviewing, and documenting reconciliation of SEC's FBWT accounts with balances reported by Treasury.
16. Develop and implement procedures for timely resolving any identified differences in FBWT activity reported by Treasury and FBWT activity recorded by SEC.

Registrant Deposits

Section 202.3a(e) of Title 17, *Code of Federal Regulations*, provides that funds held in any filing fee account in which there has not been a deposit, withdrawal or other adjustment for more than 180 calendar days will be returned to the account holder, and account statements will not be sent again until a deposit, withdrawal or other adjustment is made with respect to the account. Further, SEC's documented internal policy for the processing of registrant deposits requires a review of registrant account balances over $500 prior to issuance of a refund.

Registrant deposits represent collections from registrants for securities registration, tender offer, merger, and other fees (filing fees). SEC recorded filing fee collections in a registrant deposit liability account until earned by SEC from a future filing. These collections, when earned, provide the resources SEC used to fund its own operations. Our review of SEC's liability for registrant deposits as of September 30, 2009, identified approximately $27 million in deposit accounts that were dormant for six months or more, but were not returned to registrants. We also noted that there were no readily and routinely available reports for effectively managing the deposit operations. Our audit also identified amounts in the registrant deposit liability account that SEC earned in prior years and therefore should have been recognized as revenue in those years.

SEC's practice for managing deposit operations is inconsistent with its own documented process. As a result, a significant balance in dormant accounts remained as of the end of fiscal year 2009, and SEC's ability to effectively comply with applicable federal regulations was significantly impaired. SEC management attributed the significant balance in dormant accounts to a lack of dedicated resources assigned to perform the labor intensive reviews of deposit account activity prior to the disbursement of refunds. In order to determine whether a full refund is owed to the registrants or if a portion is earned fee revenue that should be recognized, SEC policy included a review of all accounts with balances above $500. However, the passage of time increases the difficulty in performing the review procedures and ultimately returning the funds to their rightful owners. Some of the businesses involved may have already ceased operations. Until such time that registrant deposit liability accounts are timely reviewed and excess registrants' deposit balances resolved, SEC is at risk of overstating cash and liability balances for amounts that should have been refunded and understating revenue for amounts that have been earned but not recorded. Moreover, SEC's internal control for ensuring compliance with federal regulations regarding timely issuance of refunds for dormant deposits remains weak.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve internal control over its registrant deposit account monitoring process and compliance with applicable federal regulations:

17. Design and implement controls to ensure registrant filings and deposits are consistently matched timely on an ongoing basis.
18. Allocate sufficient resources to fully resolve current registrants' deposits liability balances in accordance with SEC policy and with federal regulations.
19. Develop and implement procedures to include the use of periodic (i.e., weekly or monthly) system generated reports to facilitate oversight of

registrant deposits accounts, such as developing and using exception reports of registrant account activity.

Budgetary Resources

During our fiscal year 2009 audit, we continued to find the same types of problems in SEC's controls over budgetary resources transactions that we reported in prior fiscal years. Specifically, we noted many instances in which SEC (1) recorded invalid obligation-related transactions due to incorrect posting configurations in SEC's general ledger, (2) did not maintain documentation of authorizations for downward adjustments to prior-year undelivered orders, and (3) recorded obligations without a previously approved purchase requisition.

The continued existence of these control deficiencies in SEC's budgetary activities, which result in significant manual workarounds and the posting of a large number of general ledger adjustments, increases the risk of processing errors and misstatements related to budgetary activities in SEC's Statement of Budgetary Resources. Further, inadequate documentation of downward adjustments to prior-year undelivered orders hinders management's ability to adequately determine (1) whether budget activity transactions were approved for deobligation, (2) the officials authorizing deobligation transactions, or (3) the date the transaction was approved.

In addition to the continued weaknesses noted above, our testing of obligations transactions in fiscal year 2009 identified that key system controls, such as use of properly approved purchase requisitions and the linking of obligations to these approved purchase requisitions—both critical to helping prevent obligations from exceeding budget authority—were not consistently applied to all types of obligation documents. According to SEC's procedures, a budget analyst must certify the availability of funds through the approval of purchase requisitions to reserve funding within the general ledger system for the specified use and that all obligations must be linked to an approved purchase requisition within the general ledger system. However, in testing these key controls, we found that obligations made using the miscellaneous purchase order document (MO) were not linked to an approved purchase requisition. Instead, MOs were generally approved by the budget analyst at the time of obligation. In fiscal year 2009, SEC obligated material budgetary resources, approximately $58 million, through 257 MO transactions.

Particularly because obligations incurred using MOs represent material amounts of SEC's budgetary resources, the ability for personnel to record obligations without a previously approved purchase requisition significantly increases the risk that obligations entered into the general ledger system may exceed the apportioned levels.

To help address the significant deficiency in control over budgetary resources, we reaffirm three open recommendations from our prior audits related to

(1) correcting general ledger system configurations for upward and downward adjustments, (2) clarifying administrative control of funds guidance, and (3) establishing and implementing controls related to the recording statute. The status of these open recommendations is summarized in enclosure I.

Recommendations for Executive Action

We also recommend that the Chairman take the following specific action as part of SEC's planned corrective measures to strengthen internal control over the management of its budgetary resources:

20. Strengthen existing control procedures for recording miscellaneous purchase order documents by requiring an approved purchase requisition before certifying fund availability.

Risk Assessment and Monitoring Process

According to *Standards for Internal Control in the Federal Government*, management should comprehensively identify risks and consider all significant interactions between the entity and other parties as well as internal factors at both the entitywide and activity level. Risk identification methods may include the consideration of findings from audits and other assessments. Once risks have been identified, they should be analyzed for their possible effect on the financial statements and what actions should be taken.

Based on our review of SEC's risk assessment of internal controls over financial reporting, we found that management did not develop an understanding of its complete financial reporting control environment sufficient to identify all relevant risks and effectively plan and test controls, for example:

- SEC did not initially evaluate or test information systems internally identified as "critical" to the financial reporting environment. This risk is heightened given SEC's continued weaknesses over information security which has consistently been reported as a control deficiency since fiscal year 2004.
- A significant portion of SEC's payroll processing relies on the Department of the Interior's National Business Center (NBC), a payroll service provider. As such, SEC places significant reliance on reports generated by NBC to determine whether its payroll disbursements were complete, valid, accurate, and timely. Specifically, in processing payroll disbursements, SEC management relies on exception reports generated by NBC as a basis for adjusting internal payroll records. Despite such reliance, management's risk assessment of payroll controls did not initially consider SEC's internal control environment related to NBC's processing of its payroll. The servicer's auditor's report, Statement on Auditing Standards (SAS) 70

report,[19] related to its payroll servicing operations listed user controls that should be in place at SEC, as a user organization, in order for SEC to rely on the specified internal controls at NBC.

- In several cases, SEC's entity-level risk assessment did not specifically include the internal risks over financial reporting; rather, the risks identified were solely external risks associated with SEC's task of regulating the markets. As such, SEC's risk assessment for certain areas did not appropriately highlight internal risks relating to internal control over financial reporting, such as use of spreadsheets and use of contractors to perform key controls.
- We also identified weaknesses in SEC's monitoring and oversight of controls. For example, SEC's monitoring procedures did not address all identified risks. Further we found that management did not consistently follow documented test plans or maintain sufficient documentation for control activities.

As a result of weaknesses in SEC's risk assessment and control oversight monitoring process, SEC did not consider the complete financial reporting control environment for the areas evaluated and management did not identify all risks, effectively implement monitoring controls in high risk areas, as well as test many of the key controls that drive operations. Moreover, SEC did not document its evaluation of the design of the key controls that were identified as part of the risk assessment process.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve risk assessment and monitoring process controls:

21. Reevaluate the risk assessment and monitoring processes to ensure they consider all key elements of SEC's financial reporting control environment, including information systems and service providers.
22. Establish and implement procedures for performing and documenting risk assessment and monitoring processes in a timely manner throughout the year, based on the frequency and sensitivity of certain control activities.
23. As part of the risk assessment process, document the evaluation of the design effectiveness of key controls.

[19]SAS No. 70, *Service Organizations*, is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. The issuance of a service auditor's report prepared in accordance with SAS No. 70 signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. The service auditor's report includes valuable information regarding the service organization's controls and the effectiveness of those controls.

24. Establish procedures to comprehensively identify and assess risk related to SEC's payroll-related control activities, including risk associated with user controls identified by its payroll service provider in SAS 70 reports.
25. Enhance risk assessment and mitigation control procedures to include maintaining a list of any internally identified control breakdowns that occur during the year, documenting an evaluation of financial reporting impact as a result of any such control breakdown, and any corrective actions taken.

Other Less Significant Internal Control Issues

In addition to the recommended actions related to the six significant deficiencies we identified in our opinion report, we also identified less significant deficiencies warranting management's attention. Although not considered to be significant deficiencies, the following sections present the other internal control weaknesses identified in our fiscal year 2009 audit and our related recommendation for corrective action.

Security Over Sensitive Information

OMB Memorandum No. 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007, provides that agencies should identify and eliminate the unnecessary collection or use of social security numbers in agency systems and programs. Further, agencies are directed to participate in governmentwide efforts to explore alternatives to agency use of social security numbers as a personal identifier for federal employees.

Our review of unliquidated obligations at June 30, 2009, found that SEC used employees' social security numbers as the vendor codes within its general ledger system in processing its employees' travel authorizations. The excess circulation and use of personally identifiable information, such as social security numbers, increases susceptibility to identity theft or other fraudulent use of the information in the agency systems which may result in substantial harm, embarrassment, and inconvenience to individuals.

SEC management concurred that it should limit the use of social security numbers in agency systems and has indicated that the Office of Financial Management (OFM) will be working with the Office of Information Technology, Human Resources, and the Department of the Interior to eliminate the use of social security numbers.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to reduce the availability of personally identifiable information:

26. Review current usage of social security numbers as a personal identifier for federal employees in agency systems and programs and establish and implement alternative procedures to eliminate any such usage.

Policies and Procedures Documents

According to *Standards for Internal Control in the Federal Government*, an agency's internal control and all transactions and other significant events should be clearly documented, and the documentation should be readily available for examination.

During our fiscal year 2009 audit, we found that SEC's policies and procedures for several financial reporting processes were still in draft form or contained incomplete, incorrect, or outdated information. For example we found:

- SEC's procurement and purchases process document[20] contained multiple recommendations for internal process improvements that were not acted upon or reviewed by appropriate departments. Consequently, this process document is in draft form and had not been finalized at of the time of our audit.
- SEC's travel expenses policies and procedures document[21] contained several instances of references to incorrect or outdated information.
- SEC's *Standard Voucher (SV) Creation and Modification Standard Operating Procedure* document[22] primarily described the process to design and approve SV configurations in the system. However, it did not discuss the definition and purpose of using SVs. In fiscal year 2009, we found that SVs were used to record original transactions and correct recurring errors either due to incorrect posting logic or system modules not operating as intended, as discussed previously in the Financial Reporting Process section of this report. In addition, the document omitted procedures regarding the creation, review, and approval of actual SV entries of posted transactions. As a result, SEC management lacked assurance that all SVs were properly posted. During our audit, we found several SV transactions in the general ledger system were in an incomplete status (i.e. pending approval or held) for up to six months without resolution. It is unclear whether such transactions would have been captured through SEC's normal business process given the lack of finalized documented procedures concerning how to monitor and resolve SV entries that remain in SEC's financial system in an incomplete status.
- SEC's process document for securities transaction fees paid by self-regulatory organizations (Section 31 Fees)[23] remained in draft form at September 30, 2009.

[20]OFM-08-10-CAP, dated May 19, 2008, and labeled "Draft".
[21]OFM-08-09-CAP, dated May 19, 2008, and labeled "Draft".
[22]Document number UM-GL-0001-09-00.
[23]OFM-08-07-CAP, Draft Version 1.1 dated June 25, 2008.

SEC's incomplete, incorrect, and outdated policies and procedures hinder management's ability to identify the key risks and corresponding controls over financial reporting in all of its key business processes. In addition, without documented policies and procedures, staff may not consistently implement control activities as designed.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve financial reporting process controls:

27. Finalize the policies and procedures for the procurement and purchases and Section 31 revenue processing to include incorporating any changes needed to resolve all recommendations or deficiencies identified during the development of these draft documents.
28. Revise the SV Creation and Modification process document to clearly define
    - the purpose and use of SV transactions;
    - the process for entering SV transactions into the general ledger system, including the performance and documentation of supervisory review; and
    - monitoring procedures to ensure that SV transactions post to the general ledger system as intended.
29. Establish and implement procedures to monitor and update policy and procedure documents in a timely manner to ensure key risks and corresponding controls are documented for each key process.

Documentation of Payroll Controls

According to *Standards for Internal Control in the Federal Government*, an agency's internal control and all transactions and other significant events should be clearly documented, and the documentation should be readily available for examination. Further, the documentation requirements should appear in management directives or policy and procedures manuals.

During our audit, we noted that SEC did not consistently document evidence of payroll-related internal control procedures. Specifically, we noted SEC did not have documentation supporting the Office of Human Resources' (OHR) resolution of biweekly payroll exception reports and division certifications of personnel on-board listing (POL) reports. Timely resolution of payroll exception reports is a complementary user control specified in the SAS 70 report that should be in place at SEC to ensure related controls are operating effectively at NBC. The POL report lists SEC employees paid through NBC's payroll system, which responsible SEC managers are to review and certify as representing current active employees. These controls are intended to prevent improper payroll disbursements.

Each pay period, timesheet data is transmitted from SEC's time and attendance system to NBC's Federal Personnel and Payroll System. As payroll data is transmitted between the two systems, NBC generated exception reports which are then transmitted to OHR. SEC personnel are to review exception reports and resolve issues in the time and attendance system to ensure that payroll transactions are processed timely. This process was repeated over the course of several consecutive days as timesheet transmissions were updated and personnel data issues were resolved. Although OHR provided evidence of resolution on the exception reports, we found that documentation of such resolution was unavailable for 11 of the 17 pay periods that we reviewed. Specifically, SEC was unable to provide clear documented evidence for the resolution of 10 exception reports we reviewed. In addition, OHR could not produce the report for one pay period because under existing SEC practices, exception reports are generally not retained for greater than 6 months.

Management's lack of a documented policy and procedure to retain reports for the entire period under audit and consistently provide evidence for resolution of exceptions raises uncertainty as to whether key personnel actions that affect staff employment and salaries have been accomplished accurately and timely. Moreover, as discussed in the Risk Assessment and Monitoring section of this report, SEC did not have a policy to link the complementary user controls identified in the SAS 70 report on NBC's payroll servicing operation to ensure related controls at NBC are operating effectively.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve internal controls over payroll transactions:

30. Develop and implement written procedures that (a) standardize required documentation related to resolution of NBC's biweekly payroll exception reports and (b) extend the retention period for supporting documentation long enough to facilitate internal and external audit or review, such as a period of 18 months after payment.

Prior Period Corrections

The *Standards for Internal Control in the Federal Government* provide that an agency's transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. In addition, an agency's control activities should be established to ensure that all transactions are completely and accurately recorded.

During our fiscal year 2009 audit, we identified yearend cutoff problems resulting in prior period corrections recorded in the current fiscal year related to SEC's

improper recognition of filing fee revenue and capitalization of property, plant, and equipment. Specifically, we identified

- equipment additions exceeding $1 million, that were expensed and placed into service in the prior year, but capitalized in fiscal year 2009;
- software placed in production in December 2007, but not recorded as placed in service until December 2008; and
- $3.6 million in filing fee revenue that was earned in prior fiscal years but recorded during the first 9 months of fiscal year 2009.

Upon inquiry with management concerning the cumulative effect of all prior period corrections on the financial statements, we found that management did not have a process to evaluate the impact of all corrections affecting prior years on the current and prior year financial statements as a whole or to quantify likely errors existing in the financial statements, such as the likelihood that some portion of the registrant deposit liability relates to prior year revenue.

The lack of effective processes for evaluating the cumulative effect of prior period corrections increases the risk that management is unaware of the impact of misstatements on the reliability of SEC's financial information.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve period-end financial reporting process controls:

31. Develop and implement procedures to provide for a review of all transactions resulting in prior period corrections, including filing fee revenue and property and equipment transactions, and to quantify the cumulative effect of known and likely prior period corrections in the current fiscal year.

Preparation of Labor Surveys

The Government Performance and Results Act of 1993 (GPRA) requires federal agencies to prepare performance plans describing resources required to achieve expected results.[24] In addition, SFFAS No. 4, *Managerial Cost Accounting Concepts and Standards for the Federal Government*, provides that cost assignments should be performed by directly tracing costs wherever feasible and economically practicable.

In fiscal year 2008, SEC implemented an automated time and attendance system to among other things, enhance the level of data collected in relation to its activity based costing model. Although the time and attendance system contains

[24]GPRA, *codified, as amended, in part at* 31 U.S.C. § 1115(a).

functionalities that allow for employees to record work hours under preset activity codes on their biweekly time and attendance report, SEC did not utilize this feature. According to SEC management, in fiscal year 2009, only 54 percent of hours reported in the time and attendance system were associated with an activity code. As such, management relied on quarterly data calls (labor surveys) to allocate labor costs to the four strategic goals[25] presented in SEC's Statement of Net Cost.

Based on our review of SEC's labor survey process, we found that the accumulation of cost data is inherently subjective and that the procedures used to compile such information varied greatly from one unit to another. One unit we interviewed allocated cost information based on the supervisor's estimates of the hours spent on each activity, without any supporting analysis or data. In another unit, an employee was designated to track the hours each staff person spent on activities using a spreadsheet. As a result of this variation, SEC did not have consistent documentation supporting cost allocation or appropriately link resources used to performance results as presented in the management discussion and analysis.

Without the full utilization of activity codes in the time and attendance system or a formalized procedure for consistently supporting labor survey estimates, SEC's program costs by strategic goals presented on the Statement of Net Cost are potentially at risk of misstatement. As of September 30, 2009, the only control procedure over management's quarterly time estimates was verification that labor survey estimates provided by the various units sum to 100 percent. However, this procedure does not ensure that costs were accurately allocated among the four strategic goals.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve controls over the Statement of Net Cost preparation:

32. Update the time and attendance system to establish preset active activity and project codes for all activities used by SEC in its process for allocating gross costs to program costs by the strategic goals presented in its Statement of Net Cost.
33. Modify existing policy and procedures to require all employees to report labor hours using preset activity and project codes within the time and attendance system and establish and implement applicable controls to ensure compliance.

[25]The four strategic goals reported in SEC's Statement of Net Cost are (1) enforce compliance with federal securities laws, (2) promote healthy capital markets through an effective and flexible regulatory environment, (3) foster informed investment decision making, and (4) minimize the use of SEC resources.

34. Revise and implement procedures over the preparation of the Statement of Net Cost to utilize actual data reported by employees on their biweekly time and attendance reports.

Prompt Payment Act Interest Payments

Under the Prompt Payment Act, SEC must pay interest penalties to its vendors when it fails to timely pay its vendors in full.[26] According to implementing regulations, each agency head is responsible for ensuring: timely payments, and payment of interest penalties where required; and that internal procedures will include provisions for monitoring the causes of late payments and any interest penalties incurred, and taking necessary corrective action.[27]

More specifically, the Prompt Payment Act requires that if payment for property or services from a vendor is not made by the required due date, an interest penalty shall be paid for the period beginning on the day after the required payment date.[28] During our fiscal year 2009 audit, our testing of disbursement transactions found that SEC routinely did not meet payment due dates when processing vendor payments. Of 78 disbursement transactions we randomly selected for the 9-month period ended June 30, 2009, 27 (35 percent) included additional interest penalty charges because SEC did not submit a payment in a timely manner.

Although SEC's current policies and procedures require tracking invoices from the time of receipt until the payment is processed, they did not specify procedures to ensure that payments are processed in a timely manner and to evaluate the causes for any untimely payments. Until such controls are developed, SEC will likely continue to use a significant of amount of resources paying interest penalty charges.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve controls over disbursements transactions:

35. Investigate the causes of late payments and any interest penalties incurred and develop and implement any necessary corrective actions.

[26]31 U.S.C. § 3902(a). The Prompt Payment Act is codified, as amended, at 31 U.S.C. ch. 39, and OMB has prescribed implementing regulations, which are codified, as amended, at 5 C.F.R. pt. 1315.
[27]5 C.F.R. § 1315.3.
[28]31 U.S.C § 3902. OMB implementing regulations on determining the due date generally provide that the required payment date is **(A)** the date payment is due under the contract for the item of property or service provided; or **(B)** 30 days after a proper invoice for the amount due is received if a specific payment date is not established by contract. 5 C.F.R. § 1315.4(g).

Excessive User Access Rights in SEC's Time and Attendance System

According to the National Institute of Standards and Technology,[29] the most fundamental means of carrying out logical access controls are with policy and personnel. Logical access controls are the technical implementation of system-specific and organizational policy, which stipulates who should be able to access what kinds of information, applications, and functions. These access controls are normally based on the principles of separation of duties and least privilege. In addition, *Standards for Internal Control in the Federal Government* identifies the need for appropriate segregation of duties. Key duties and responsibilities should be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event.

During our fiscal year 2009 audit, we found that the SEC had not implemented a monitoring control to periodically assess the access rights granted to users within SEC's time and attendance system. Because SEC lacked such controls, our review of user rights within the time and attendance system identified instances in which individuals were assigned levels of access that were excessive relative to their job functions. For example, we identified one user assigned the incompatible roles of administrator, certifier, and timekeeper within the system. This broad level of access in the time and attendance system was unnecessary given that the user's job was to extract payroll and timesheet data for use in other financial reporting activities.

Until an effective monitoring control over access rights granted to persons within the SEC's time and attendance system is implemented, additional instances of excessive access resulting in possible inadvertent or deliberate misuse, fraudulent use, or improper disclosure of payroll data may occur and not be detected.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve access control within the time and attendance system:

36. Develop and implement controls over access rights in the time and attendance system to prevent or timely correct any excessive access in the system.

[29](NIST SP800-12, NIST Handbook).

Financial Statement Closing Schedule: Cutoffs and Related Activities

The *Standards for Internal Control in the Federal Government* provides that internal control and all transactions and other significant events should be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form and provide reasonable assurance that the objectives of the agency are being achieved with respect to effectiveness and efficiency of operations. Further, all transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions.

Our fiscal year 2009 audit identified instances of delay in SEC's finalizing the financial statement closing schedule,[30] delays in the proper closing of the accounting period, failures to reverse prior period accrual entries and accrue current period transactions, and lack of documented protocols for the reopening of closed accounting periods, for example:

- SEC was not able to finalize the June 2009 accounting period (3rd quarter closing) financial statement closing schedule in a timely manner because several staff were on leave and unable to attend the meeting for establishing target dates. As a result, the due dates for key closing activities were not communicated to key accounting personnel until June 29, 2009. Similarly, the yearend financial statement closing schedule was not finalized until September 25, 2009.
- Several closing journal vouchers prepared as part of the November 2008 monthly closing process were never posted to the general ledger. In addition, several accrual transactions recorded in one period were not appropriately reversed in the succeeding fiscal month. Specifically, accrual entries from fiscal year 2008 were not reversed in October 2008, the first accounting period in fiscal year 2009; these were ultimately reversed in December 2008.
- SEC routinely reopened closed accounting periods. SEC's financial statement closing schedule reflected a period closing date for closing each accounting period in its general ledger system, but did not establish cutoff dates for the recording of transactions from key activities to occur prior to the closing of the accounting period. Many key activities were performed subsequent to the accounting period closing date to allow for the recording of key transactions. Further, the responsibility for the reopening of a closed accounting period was not restricted to management personnel. Certain staff accountants from two branches within the OFM, Financial Operations Branch and Financial Statements and Policy Branch, routinely performed this task.

[30]SEC's monthly financial statement closing schedule lists key activities relative to the closing of an accounting period and preparation of monthly financial statements, the staff's performing each of the activities, and the date when such activities will be completed or performed.

Such delays resulted from the lack of control procedures establishing a standardized timeline with cutoff dates for the completion and recording of key month-end accounting transactions prior to closing of an accounting period and preparation of the financial statements and footnotes. As a result, OFM staff and contractors met monthly to review and establish due dates for the financial statement closing schedule. Consequently, completion of the financial statement closing schedule was delayed for certain accounting periods and transactions; transactions were not recorded in the appropriate accounting periods; and closed accounting periods were routinely reopened to allow for key transactions to be posted. In addition, SEC was unable to timely and accurately prepare its interim financial statements for the first two months of fiscal year 2009. SEC did not have documented policies and procedures for reopening a closed accounting period, including formal assignment of authority and responsibility for reopening a closed accounting period. As a result, risks of potential misstatements existed, potentially adversely affecting management's ability to accurately and timely prepare interim financial statements.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions as part of SEC's planned corrective measures to improve period-end financial reporting closing process:

37. Develop and implement a standardized financial statement closing schedule with cutoff dates for key month-end accounting transactions that should be completed prior to the closing of an accounting period.
38. Develop and implement control procedures to ensure prior period accrual accounting entries are reversed in the following accounting period and current period accrual accounting entries are recorded prior to the accounting period closing date.
39. Develop and implement policies and procedures to ensure that only designated senior staff and management (such as branch chief level and above) have the authority to reopen previous accounting periods. Such procedures should provide for (a) documenting the required protocols to follow for requesting to reopen a closed accounting period and approval of such request, (b) specifying required documentation for situations that caused a closed accounting period to be reopened, and (c) as applicable, documenting any corrective actions that were taken to preclude such circumstances from reoccurring.

Documentation of Contracting Officer's Technical Representative's (COTR) Review

SEC regulation SECR 10-15 *Contracting Officer's Technical Representative (COTR), Inspection and Acceptance Official (IAO), and Point of Contact (POC)* provides that COTRs must review and process all invoices and vouchers to ensure

that payment is made in accordance with the contract payment schedule. In addition, for cost-reimbursable contracts, SEC regulations provide that COTRs must ensure that vouchers are consistent with the contractor's proposal or negotiated amounts, commensurate with the rate of expenditure, and that any recommendations by the COTR to change a voucher should be made in writing. Furthermore, according to *Standards for Internal Control in the Federal Government*, internal control and all transactions and other significant events should be clearly documented, and the documentation should be readily available for examination.

During our testing of non-payroll expenses for the 9-month period ended June 30, 2009, we identified two instances in which evidence of the COTR's review of the invoice was not clearly documented. In both instances, we noted that the billing rates and unit prices on the invoices were different than the rates and prices contained in the contract documentation. In each of these cases, we found the COTRs relied upon the delegated authority of project managers to review and authorize invoices for payment; however, the review and authorization were not documented.

The lack of a documented conclusion by COTRs or other delegated authority when there are apparent differences between the invoice and contract or other obligating document raises questions as to whether vendors have billed SEC in error and if the proper amount were properly approved for payment. Without a consistent and documented COTR review, errors in amounts billed to SEC may not be detected and incorrect amounts may be disbursed.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions to improve internal control over vendor invoice payments:

40. Develop and implement procedures to provide for appropriately documented COTR review of all vendor invoices prior to payment in compliance with SEC regulation.
41. Establish and implement procedures to provide periodic training to COTRs and project managers regarding their responsibilities for reviewing and approving invoices.

Notes to Interim Financial Statements and Pro-Forma Financial Reporting

OMB Circular No. A-136 (rev. 2009) provides that beginning with the third quarter of fiscal year 2008, agencies may submit unaudited notes (and other required disclosure information as deemed relevant and useful) along with unaudited interim financial statements. Under A-136, participating agencies should complete key notes, such as those notes that present a greater risk of failing to meet the prescribed disclosure requirements, to allow agencies to receive comments from OMB well in advance of the yearend, so that the agencies will have sufficient time

to improve the accuracy and conformity of these notes for the yearend submission of the Performance and Accountability Report (PAR). For certain notes, the data may not be available or it may not be cost-efficient to obtain the interim data. In these cases, A-136 provides that agencies should provide pro-forma notes without the amount and/or data information.

Further, SFFAS No. 15, *Management's Discussion and Analysis (MD&A)*, requires federal agencies to include as "required supplementary information" an MD&A with its financial statements. The MD&A is supposed to provide among others a concise description of its activities and program, financial, and performance highlights during the year. As such certain information reported in the MD&A could relate to information reported in the financial statements and/or related notes.

As discussed previously in the Financial Reporting Process section of this report, SEC did not always properly account for and report material contingent liabilities in its June 30, 2009, interim financial statements and related notes. In addition, SEC's MD&A reported certain information that was inconsistent with related information in its financial statements and/or notes. For example, the MD&A initially reported disbursements to harmed investors from the Fair Funds[31] account of $2.1 billion, which differed from the related information in a note to its financial statements, which reported approximately $1.1 billion of such disbursements. After we pointed out this difference, SEC later adjusted its final MD&A to report the amount as disbursements to harmed investors, which included funds from the Fair Funds account. Nonetheless, we concluded that SEC did not have procedures in place to ensure disbursements information reported in the MD&A was reviewed for consistency prior to our review. In another example, before we pointed out the differences, SEC's draft reporting showed offsetting collections of $1.016 billion in the Financial and Performance Highlights section of the MD&A, which differed from the related amounts in its Statement of Budgetary Resources, which showed approximately $1.018 billion of such collections. We noted other inconsistencies, though not material, which were not adjusted due to time constraints and management's concern that other unintended inconsistencies may arise and not be detected.

SEC officials stated that several of the notes that were provided with its June 30, 2009 financial statements and submitted to OMB are only updated at yearend. As a result, SEC's contingent liability was materially misstated in its interim financial statements. In addition, SEC's yearend financial statements contained instances of inconsistent information. Although individually, or in the aggregate, the inconsistencies we identified were not significant, they nevertheless obscure the information presented in SEC's financial statements and the related MD&A. Until

[31]When an SEC enforcement action results in both disgorgement orders and civil money penalties imposed on the same violator, SEC has discretionary authority to move to combine both amounts for payment into a fund for distribution to harmed investors, which is called a Fair Fund, instead of into the General Fund of the U.S. Treasury. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 308, 116 Stat. 745, 784 (July 30, 2002) (*codified at* 15 U.S.C. § 7246).

such time that SEC develops a process for preparing pro-forma financial statements and MD&A, and routinely updating the notes[32] at interim periods, the ongoing reliability of its financial statements and notes are at risk of material misstatements. Further, SEC is at risk of reporting information in its MD&A that is inconsistent with related information reported in the financial statements.

Recommendations for Executive Action

We recommend that the Chairman take the following specific actions to improve internal control over its financial statement preparation process:

42. Develop and implement a process for reliably preparing accurate pro forma financial statements and updating the notes that accompany financial statements prior to yearend, preferably with the third quarter reporting.
43. Augment current procedures to provide specific steps for ensuring the consistency of related information reported in the MD&A and the financial statements and related notes.

Agency Comments

In providing written comments on a draft of this report, the SEC Chairman stated that remediating the material weakness in internal control over financial reporting is one of her top priorities and expressed her commitment to improving the integrity of SEC's reporting systems. The Chairman cited short-term work to strengthen internal controls that has already begun including building a robust, fully documented program for evaluating internal controls over financial reporting; enhancing and documenting SEC's processes with respect to the FBWT and shifting responsibility for this area to dedicated staff within a new branch; adding new staff and contractor support to the registrant deposits function to enhance compliance with SEC policies and return funds in dormant accounts to their owners; bringing the posting models in the core financial system into compliance with the SGL; improving process and system documentation and formalizing tighter controls over key areas we identified; and bolstering SEC's security policies and monitoring the core financial system and fee system. To assist SEC in these efforts, the SEC Chairman stated that SEC has retained the services of an independent consulting firm.

The Chairman also discussed SEC's goal to build a fully integrated, secure suite of financial systems and eliminate manual processes that can lead to errors. The SEC Chairman stated that SEC's longer-term effort to fully integrate its financial systems will include procuring a new financial reporting tool; deploying a module to track agency investments; replacing the manual process by which disgorgement and penalties data are reentered into the core financial system with an automated system; creating a robust program for documenting and managing system

[32]SEC's financial statements disclose that the accompanying notes are an integral part of their financial statements. Standard notes are an integral part of the financial statements.

configurations; and building a separate, secure network for the financial systems. The Chairman also stated that SEC is developing a formal remediation plan to fully address the significant deficiencies we identified. We will evaluate the effectiveness of SEC's actions, strategies, and plans during our fiscal year 2010 audit.

SEC's written comments are reprinted in enclosure III of this report.

This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. § 720 to submit a written statement on actions taken on the recommendations to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Government Reform not later than 60 days from the date of this report. A written statement also must be sent to the House and Senate Committees on Appropriations with your agency's first request for appropriations made more than 60 days after the date of this report.

This report is intended for use by SEC management. We are sending copies of this report to the Chairman and Ranking Members of the Senate Committee on Banking, Housing, and Urban Affairs; the Senate Committee on Homeland Security and Governmental Affairs; the House Committee on Financial Services; and the House Committee on Oversight and Government Reform. We are also sending copies to the Secretary of the Treasury, the Director of the Office of Management and Budget, and other interested parties. In addition, this report is available at no charge on GAO's Web site at http://www.gao.gov.

We acknowledge and appreciate the cooperation and assistance provided by SEC management and staff during our audit of SEC's fiscal years 2009 and 2008 financial statements. If you have any questions about this report or need assistance in addressing these issues, please contact me at (202) 512-3133 or dalkinj@gao.gov.

Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

Sincerely yours,

James R. Dalkin
Director
Financial Management and Assurance

Enclosure I: Status of Recommendations from Prior Audits Reported as Open in GAO's 2008 Management Report

This enclosure presents the status of the 43 recommendations reported as open in GAO's April 2, 2009, management report. The weaknesses are grouped according to deficiency areas specified in our prior audit reports.

Table 1: Status of Recommendations from Prior Audits Reported as Open in GAO's 2008 Management Report at the end of GAO's Audit of SEC's Fiscal Year 2009 Financial Statements.

Audit Area	Year initially reported	Status of corrective action	
		Completed	In progress
Disgorgement and penalties			
1. Implement controls so that the ongoing activities involving disgorgements and penalties are properly, accurately, and timely recorded in the accounting system.	2005	X	
2. Develop and implement written policies covering the procedures, documentation, systems, and responsible personnel involved in recording and reporting disgorgement and penalty financial information. The written procedures should also address quality control and managerial review responsibilities and documentation of such a review.	2005	X	
3. Develop, document in writing, and implement comprehensive policies, procedures, and controls over disgorgement and penalty transactions that include: The recording of activity by case for liabilities for fiduciary balances, including monthly reconciliations and management review, to ensure that balances by case are accurate.	2006	X	
4. Develop, document in writing, and implement comprehensive policies, procedures, and controls over disgorgement and penalty transactions that include: The initiation, recording, and monitoring of investments, including the monthly reconciliation of investment activity, to provide assurance that these fiduciary amounts are accurate and complete.	2006	X	
5. Develop and implement controls over the calculation of disgorgement and penalties accounts receivable, including the reliability of data downloaded from Phoenix and the accuracy of spreadsheet cell formulas and related methodologies.	2008	X	
6. Develop procedures for including in the footnotes to the financial statements disclosure and explanations about the source and disposition of SEC's disgorgement and penalty activities.	2009	X	
7. Develop and implement procedures specifying how the collectability assessments provided by Enforcement will be used by OFM, to include documentation requirements for instances in which an allowance amount other than Enforcement's assessment is recorded.	2009	X	
8. Reevaluate the reasonableness of the methodology used for calculating the allowance for loss on disgorgement and penalty accounts receivable, specifically evaluating whether the methodology should be revised to separate debts into risk-based groups when calculating the historical collection percentage and considering the effect of debts moving in and out of the top 25 debt list.	2009	X	

Enclosure I: Status of Recommendations from Prior Audits Reported as Open in GAO's 2008 Management Report

Table 1: Status of Recommendations from Prior Audits Reported as Open in GAO's 2008 Management Report at the end of GAO's Audit of SEC's Fiscal Year 2009 Financial Statements.

Audit Area	Year initially reported	Status of corrective action	
		Completed	In progress
9. Develop and implement improved safeguarding procedures within SEC's Operations Center for checks received or establish a lockbox for the submission of checks to OFM and instruct defendants to mail checks to the lockbox.	2009		X
10. Provide training to staff on the proper use of the new system module and the proper procedures for recording disgorgement and penalty transactions in Momentum.	2009	X	
11. Modify existing guidance to provide for a timely and documented supervisory review of all disgorgement and penalty transactions entered in Momentum to ensure that transactions are entered completely and accurately.	2009	X	
Financial statement preparation and reporting			
12. Develop or acquire an integrated financial management system to provide timely and accurate recording of financial data for financial reporting and management decision making.	2005	X	
13. Integrate subsystems that process significant accounting data with the general ledger.	2008	X	
14. Until subsystems are fully integrated, develop and implement documented data reliability checks for data extracted from nonintegrated subsidiary systems, including spreadsheets. These data reliability checks should include supervisory review.	2008	X	
15. Develop and implement procedures to account for the receipt of FOIA fees in accordance with GAAP and federal financial reporting requirements.	2009	X	
16. Develop and implement a desktop procedures manual that provides detailed instructions for performing each key accounting process preceding the general ledger closing process; the associated internal control to be followed for each step, as applicable; and the manner for documenting compliance with these controls.	2009		X
17. Develop and implement written procedures for the preparation and review of accounting entries to include descriptions of the steps to be performed and the documentation required for supervisory-level review of all supporting documentation.	2009	X	
18. Develop and implement written procedures providing guidance for when to use JV or SV entries.	2009	X	
Property and equipment			
19. Review all existing leases for property and equipment to determine if they should be capitalized or expensed and make any necessary adjustments to the related general ledger balances.	2005	X	
20. Implement procedures requiring periodic comparisons of related details in disbursement and property/equipment subsidiary records to identify any unrecorded purchases that satisfy established capitalization criteria.	2007	X	

Enclosure I: Status of Recommendations from Prior Audits Reported as Open in GAO's 2008 Management Report

Table 1: Status of Recommendations from Prior Audits Reported as Open in GAO's 2008 Management Report at the end of GAO's Audit of SEC's Fiscal Year 2009 Financial Statements.

Audit Area	Year initially reported	Status of corrective action	
		Completed	In progress
21. Implement procedures to ensure that internal use software project managers have a complete and consistent understanding of the requirements that should govern compilation of cost data submitted for capitalization, including consideration of joint Office of Information Technology and Office of Financial Management (OFM) training to software project managers on the requirements of applicable generally accepted accounting principles.	2007	X	
22. Implement procedures whereby OFM staff routinely review capitalized amounts for software projects against supporting documentation to provide additional assurance that the recorded amounts are accurate and complete.	2007	X	
23. Establish and implement controls over invoiced property costs and dates to ensure that property and equipment acquisitions are accurately recorded in the relevant subsidiary ledgers for personal property, leasehold improvement, and software.	2008	X	
24. Provide training for all appropriate employees on entering and processing transactions related to property and equipment purchases in the new property and equipment system.	2009	X	
25. Develop and implement procedures for performing and documenting oversight and review processes over property and equipment transactions.	2009	X	
26. Develop and implement procedures for the use of project codes in SEC's time and attendance system to automate the calculation of federal employee costs related to capitalized software amounts.	2009	X	
Closing of recommendations to address Federal Managers' Financial Integrity Act weaknesses			
27. Require documented support and review of SEC's corrective actions to provide evidence that actions taken in response to audit recommendations fully correct identified deficiencies prior to closing out the audit issues in the tracking system.	2005	X	
Responsibilities of contracting officer's technical representative (COTR)			
28. Clarify guidance regarding policies and procedures (as described in SECR 10-8 and SECR 10-15) for the COTR's responsibilities and take actions to help ensure existing policies and procedures are being followed consistently.	2006	X	
Internal review of filing fee calculations			
29. Take action to help ensure that its policy on recalculating fee-bearing filing amounts is consistently followed.	2006	X	
30. Take action to help ensure that the recalculation of the required filing fees is clearly documented.	2006	X	
Processing personnel actions and certifying employees' time cards			
31. Evaluate the overall effectiveness of its actions taken in response to our findings regarding payroll and personnel action processing, when fully implemented, to determine whether any modifications, additional actions, or both are needed.	2007	X	
32. Establish and implement procedures for documenting evidence of monitoring of time card certifications and include procedures to document any identified exceptions.	2008		X

Enclosure I: Status of Recommendations from Prior Audits Reported as Open in GAO's 2008 Management Report

Table 1: Status of Recommendations from Prior Audits Reported as Open in GAO's 2008 Management Report at the end of GAO's Audit of SEC's Fiscal Year 2009 Financial Statements.

Audit Area	Year initially reported	Status of corrective action	
		Completed	In progress
33. Segregate key responsibilities over the approval of personnel actions so that no one individual approves his own personnel action.	2008	X	
34. Develop procedures for implementing management's policy on the authorization and validation of personnel actions and the timely processing of such actions.	2009		X
35. Configure SEC's time and attendance system to preclude lower-level employees from approving higher-level employees' time cards.	2009	X	
Accounting for budgetary resources			
36. Correct general ledger system configurations to properly account for upward and downward adjustments of prior-years' undelivered orders in accordance with the *U.S. Standard General Ledger*.	2008		X
37. Establish and implement controls over obligation-related entries (including original obligations, corrections, and deobligations) to ensure the use of correct U.S. Standard General Ledger accounts and the recording of correct amounts.	2008	X	
38. Clarify administrative control of funds guidance and document the responsibilities of the staff performing obligation-related activities with regard to recording obligations in accordance with the recording statute.	2008		X
39. Establish and implement controls to ensure that SEC staff adheres to existing policies and procedures to prevent violations of the recording statute.	2008		X
40. Develop and implement formal operating procedures for monitoring undelivered orders to include guidance for documenting review and approval of downward adjustment transactions.	2009	X	
41. Correct general ledger configurations to properly record offsetting collections as these transactions occur.	2009	X	
42. Update the written guidance for funds management to include correct accounting entries and use of correct general ledger accounts for recording offsetting collections transactions.	2009	X	
Considering OCIE inspection results			
43. Develop and implement procedures for the review and consideration of OCIE inspection results by OFM as part of its process for recording Section 31 fees.	2009	X	

Source: GAO analysis of SEC data.

Enclosure II: Status of Previously Reported Information Security

This Enclosure presents the status of the 43 security weaknesses in information system controls at SEC that we identified in public and "Limited Official Use Only" reports issued in 2005, 2007, 2008, and 2009 that were still unresolved at the time of our March 16, 2009, reports. The weaknesses are grouped according to control areas—access controls, configuration management, and security management—specified by our Federal Information System Controls Audit Manual.

Table 1: Status of Prior Weaknesses Reported as Unresolved in our March 16, 2009, Reports at the end of GAO's Audit of SEC's Fiscal Year 2009 Financial Statements.

Control area	Year initially reported	Status of corrective action	
		Completed	In progress
Access controls			
Identification and authentication			
1. SEC did not always enforce strong password settings on its enterprise database servers.	2008		X
2. SEC did not always sufficiently protect passwords.	2008	X	
3. SEC did not use a strong authentication method for sharing files.	2008	X	
4. SEC did not securely configure the snmp community string used to monitor and manage network devices.	2009	X	
5. SEC did not remove a default vendor account from a remote copy protocol installed on network devices.	2009	X	
6. Multiple database administrators shared the same log-on application identification (ID) to a powerful database account called OPENFss.	2009	X	
7. SEC did not uniquely identify individual accounts on network switches for Hypertext Transfer Protocol Secure (https) log-in.	2009	X	
Authorization			
8. SEC did not adequately document access privileges for the EDGAR application.	2007		X
9. SEC allowed unnecessary database links.	2008	X	
10. SEC did not properly document or maintain approval of user access privileges to the Momentum system.	2009		X
11. SEC did not adequately restrict user privileges to two of its database systems.	2009		X
12. SEC did not sufficiently restrict remote access to the EDGAR and Fee Momentum database servers.	2009		X
13. SEC did not sufficiently prevent users from running long reports during critical times of the day, thus monopolizing database system resources.	2009		X
Cryptography			
14. SEC did not always provide approved, secure transmission of data over its network.	2008		X
15. SEC did not always ensure that information transmitted over the network was adequately encrypted.	2009	X	
Audit and monitoring			
16. SEC had not conducted a network baseline assessment for the general support system network.	2008	X	
17. SEC did not always produce, review, and document reviews of Momentum security reports in a timely manner.	2008		X
18. SEC did not keep an adequate audit trail record of user activities in the enterprise database environment.	2008		X

Enclosure II: Status of Previously Reported Information Security

Table 1: Status of Prior Weaknesses Reported as Unresolved in our March 16, 2009, Reports at the end of GAO's Audit of SEC's Fiscal Year 2009 Financial Statements.

Control area	Year initially reported	Status of corrective action	
		Completed	In progress
19. SEC did not adequately configure several databases' systems to enable auditing and monitoring of security-relevant events.	2009	X	
Segregation of duties			
20. SEC did not adequately segregate computer-related duties and functions.	2009		X
21. SEC it did not always adequately separate network management traffic from general network traffic.	2009		X
Physical security			
22. SEC did not adequately restrict physical access to SEC resources from publicly accessible areas.	2008	X	
23. SEC's physical security awareness program was not always effective. SEC policy requires that employees use their badges in order to access restricted information system facilities.	2009	X	
24. SEC's physical security standards were still in draft.	2009	X	
Configuration management			
25. SEC did not effectively implement patch management on certain Unix servers.	2005		X
26. SEC lacked procedures to periodically review application code to ensure that only authorized changes were made to production.	2005		X
27. SEC did not always implement patches on vulnerable workstations and enterprise database servers.	2008	X	
28. SEC did not always protect its major enterprise database applications from command injection attacks.	2008		X
29. SEC did not consistently apply patches or upgrade its database servers to the current software versions to support the processing of financial data.	2009		X
30. SEC did not adequately document the test plans associated with the Momentum scripts.	2009		X
31. SEC did not adequately document or approve changes to the requirements, design, and scripts associated with the upgrade to Momentum.	2009		X
32. SEC did not establish or maintain a configuration baseline for Momentum.	2009		X
33. SEC did not develop status reports for Momentum.	2009	X	
34. SEC did not periodically conduct configuration audits to verify and validate the extent to which the actual configuration items for the Momentum upgrade reflect the required physical and functional characteristics specified by requirements.	2009		X
35. SEC did not have a detailed configuration management plan associated with the Momentum upgrade.	2009		X
36. SEC did not assign a configuration manager or team responsibility for the Momentum upgrade.	2009	X	
37. SEC did not adequately implement tools to manage configuration items for the Momentum upgrade.	2009		X
Security management			
38. SEC did not complete the annual testing of security controls for its general ledger application and general support system.	2008	X	
39. SEC did not adequately back up critical accounting data files on key workstations.	2008	X	
40. Although SEC appointed an acting senior agency information security officer from April to July 2008, the position has been vacant for the past 8 months.	2009	X	
41. SEC did not provide full information for management oversight of risks associated with the Momentum application.	2009	X	

Enclosure II: Status of Previously Reported Information Security

Table 1: Status of Prior Weaknesses Reported as Unresolved in our March 16, 2009, Reports at the end of GAO's Audit of SEC's Fiscal Year 2009 Financial Statements.

Control area	Year initially reported	Status of corrective action	
		Completed	In progress
42. SEC did not sufficiently conduct periodic testing and evaluation of controls.	2009	X	
43. SEC did not certify and accredit a key intermediary subsystem that supports the production of its financial statements.	2009		X

Source: GAO analysis of SEC data.

Enclosure III: Comments from the U.S. Securities and Exchange Commission

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

THE CHAIRMAN

March 19, 2010

Mr. James Dalkin
Director
Financial Management and Assurance
Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Dalkin:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO's) draft *Management Report: Improvements Needed in SEC's Internal Controls and Accounting Procedures* (GAO-10-443R). In the report, you present the GAO's recommendations for correcting the deficiencies in internal control that the GAO identified during its financial statement audit of the Securities and Exchange Commission (SEC) for fiscal years 2008 and 2009.

During the audit, the GAO found that the SEC's financial statements for 2008 and 2009 were presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles. However, as a result of the cumulative effect of six significant deficiencies, the GAO identified a material weakness in internal control over financial reporting. As the agency responsible for enforcing the public company disclosure and financial statement requirements, the SEC must maintain strong internal controls over financial reporting. Remediating our material weakness swiftly is one of my top priorities.

We have already begun our work to strengthen our internal controls. In the short-term, we are actively working to:

- Build a robust, fully documented program for evaluating internal controls over financial reporting;
- Enhance and document our processes with respect to the Fund Balance With Treasury and shift responsibility for this area to dedicated staff within a new branch;
- Add new staff and contractor support to our registrant deposits function to enhance compliance with our policies and return funds in dormant accounts to their owners;
- Bring the posting models in our core financial system into compliance with the Standard General Ledger (USSGL);

Enclosure III: Comments from the U.S. Securities and Exchange Commission

- Improve our process and system documentation and formalize tighter controls over key areas identified by GAO; and

- Bolster our security policies and our monitoring of our core financial system and Fee Momentum system.

To assist us in these aggressive efforts, we have recently retained an independent consulting firm, Protiviti Government Services. We have tasked Protiviti to provide three types of services:

1) *Provide an independent review of the agency's plan for remediating the material weakness in internal controls over financial reporting.*

2) *Conduct business process reviews of key agency processes that are implicated by the material weakness.*

3) *Assist with the management assessment of internal control.* This will include assisting in the assessment of risks; documenting relevant processes and procedures; assessing the design and testing the effectiveness of relevant controls; documenting and reporting test results; assisting in developing remediation plans; and assisting in implementing a sustainable model for periodic evaluation.

Our goal is to build a fully integrated, secure suite of financial systems and eliminate manual processes that can lead to errors. As part of our longer-term effort to fully integrate our financial systems, we will:

- Procure a new financial reporting tool;

- Deploy a module to track agency investments;

- Replace the manual process by which disgorgements and penalties data is reentered into the core financial system with an automated system;

- Create a robust program for documenting and managing our system configurations; and

- Build a separate, secure network for our financial systems.

We are developing a formal remediation plan to fully address the significant deficiencies you have identified. I look forward to sharing this plan with you during your audit of our 2009 and 2010 financial statements, and would welcome any input that you would like to offer.

I am committed to improving the integrity of the SEC's reporting systems and establishing the SEC as a model of effective internal control over financial reporting. We are investing significant additional resources in this effort and I will closely monitor our progress.

Enclosure III: Comments from the U.S. Securities and Exchange Commission

Thank you again for the opportunity to comment on this report. If you have any questions relating to our response, please contact our Acting Chief Financial Officer, Kenneth A. Johnson, at (202) 551-4306.

Sincerely,

Mary L. Schapiro
Chairman

cc: Diego Ruiz
Kenneth Johnson

Enclosure IV: Summary of Audit Scope and Methodology

To fulfill our responsibilities as auditor of the financial statements of the Securities and Exchange Commission (SEC), we did the following:[1]

- Examined, on a test basis, evidence supporting the amounts and disclosures in the financial statements.
- Assessed the accounting principles used and significant estimates made by SEC management.
- Evaluated the overall presentation of the financial statements.
- Obtained an understanding of SEC and its operations, including its internal control over financial reporting.
- Considered SEC's process for evaluating and reporting on internal control over financial reporting based on criteria established under 31 U.S.C. sec. 3512(c), (d), commonly known as the Federal Managers' Financial Integrity Act of 1982.
- Tested relevant internal controls over financial reporting.
- Evaluated the design and operating effectiveness of internal control over financial reporting based on the assessed risk.
- Assessed the risk that a material misstatement exists in the financial statements and the risk that a material weakness exists in internal control over financial reporting.
- Tested compliance with selected provisions of the following laws and regulations: the Securities Exchange Act of 1934, as amended; the Securities Act of 1933, as amended; the Antideficiency Act; laws governing the pay and allowance system for SEC employees; the Debt Collection Improvement Act of 1996; the Prompt Payment Act; the Federal Employees' Retirement System Act of 1986; the Continuing Appropriations Resolution, 2009, as amended; the Financial Services and General Government Appropriations Act, 2009; and the Supplemental Appropriations Act of 2009.

We requested comments on a draft of this report from the SEC Chairman. We received written comments from SEC and summarized the comments in our report. We conducted our audit in accordance with U.S. generally accepted government auditing standards.

(194822)

[1]For a further, more detailed explanation of our audit scope and methodology, see the discussion in our related financial audit report (GAO-10-250).

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper