G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

April 13, 2012

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 15, 2011, we issued our opinion on the U.S. Securities and Exchange Commission's (SEC) and its Investor Protection Fund's (IPF)[1] fiscal years 2011 and 2010 financial statements. We also issued our opinion on the effectiveness of SEC's internal controls over financial reporting as of September 30, 2011, and our evaluation of SEC's compliance with selected provisions of laws and regulations during fiscal year 2011.[2] In that report, we identified significant deficiencies in SEC's internal control over financial reporting.

The purpose of this report is to (1) present new recommendations related to the significant deficiencies we identified in our November 2011 report;[3] (2) communicate less significant internal control issues we identified during our fiscal year 2011 audit of SEC's internal controls and accounting procedures, along with our related recommended corrective actions; and (3) summarize information on the status of the recommendations reported as open in our March 29, 2011, management report[4] (see enc. I).

[1]IPF was established in 2010 to fund the activities of SEC's whistleblower award program and the SEC Office of Inspector General suggestion program for SEC employees. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 922, 124 Stat. 1376, 1841 (July 21, 2010) (*codified at* 15 U.S.C. § 78u-6). IPF is a separate fund within SEC and its financial statements present a segment of SEC financial activity. Accordingly, IPF's financial transactions are also included in SEC's financial statements. However, the significant deficiencies discussed in this report pertain to SEC's financial reporting but not that of IPF because of the nature of IPF's financial transactions during fiscal year 2011.

[2]GAO, *Financial Audit: Securities and Exchange Commission's Financial Statements for Fiscal Years 2011 and 2010*, GAO-12-219 (Washington, D.C.: Nov. 15, 2011).

[3]See enc. I for the list of open recommendations relating to continuing control deficiencies that contributed to the significant deficiencies over financial reporting discussed in our opinion report, GAO-12-219.

[4]GAO, *Management Report: Improvements Needed in SEC's Internal Controls and Accounting Procedures*, GAO-11-348R (Washington, D.C.: Mar. 29, 2011).

Results in Brief

In our audit of SEC's fiscal years 2011 and 2010 financial statements, we identified four significant deficiencies in internal control[5] as of September 30, 2011. These significant internal control deficiencies represent continuing deficiencies concerning controls over (1) information systems, (2) financial reporting and accounting processes, (3) budgetary resources, and (4) registrant deposits and filing fees.[6] These significant control deficiencies may adversely affect the accuracy and completeness of information used and reported by SEC's management. We are making a total of 10 new recommendations to address these continuing significant internal control deficiencies.

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

- payroll monitoring,
- implementation of post-judgment interest accounting procedures,
- accounting for disgorgement and penalty transactions, and
- the government purchase card program.

We are making a total of 9 new recommendations related to these other internal control deficiencies.

We are also providing summary information on the status of SEC's actions to address the recommendations from our prior audits as of the conclusion of our fiscal year 2011 audit. By the end of our fiscal year 2011 audit, we found that SEC took action to fully address 38 of the 66 recommendations from our prior audits, subsequent to our March 29, 2011, management report.[7]

Lastly, we found that SEC took action to address and resolve all four weaknesses in information systems controls that we identified in public and "Limited Official Use Only" reports issued in 2008 through 2009[8] that were reported as open at the time of our March 29, 2011, management report.

---

[5]A control deficiency exists when the design or operation of a control does not allow management or employees in the normal course of performing their assigned functions to prevent or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a 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. In contrast, a material weakness is a 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 and corrected on a timely basis.

[6]See enc. I for list of open recommendations related to registrant deposits and filing fees.

[7]GAO-11-348R.

[8]GAO, *LIMITED OFFICIAL USE ONLY Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program*, GAO-08-279SU (Washington, D.C.: Feb. 29, 2008), and *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).

In providing written comments on a draft of this report, the SEC Chairman stated that continued improvement in the agency's internal control structure, particularly in the areas of information security, financial reporting and accounting processes, budgetary resources, and registrant deposits and filing fees, is a top priority. The Chairman stated that the centerpiece of SEC's effort to strengthen financial controls is to migrate SEC's core financial system and transaction processing to a federal shared service provider. We will evaluate SEC's actions, strategies, and plans as part of our fiscal year 2012 audit. SEC's written comments are reprinted in enclosure II. SEC also provided technical comments, which we considered and incorporated as appropriate.

Scope and Methodology

As part of our audit of SEC's fiscal years 2011 and 2010 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. As part of our audit, we considered and evaluated the work performed and conclusions reached by SEC management in its internal control assessment.[9] Further details on our scope and methodology are included in our November 2011 report on our audit of SEC's fiscal years 2011 and 2010 financial statements and are summarized in enclosure III.

We conducted our audit of SEC's fiscal years 2011 and 2010 financial statements in accordance with U.S. generally accepted government auditing standards. We believe our audit provided a reasonable basis for our conclusions in this report.

Significant Deficiency over Information Security

As we reported in our report on our audit of SEC's fiscal years 2011 and 2010 financial statements,[10] SEC has made progress in strengthening internal control over its financial information systems. However, despite this progress, we identified new weaknesses in information security controls regarding (1) incomplete implementation of SEC's information security program and (2) inadequate review of service auditors' reports that jeopardized the confidentiality and integrity of SEC's financial information, as discussed below.

[9]Office of Management and Budget Circular No. A-123, *Management's Responsibility for Internal Control*, defines management's responsibility for internal control in federal agencies and establishes requirements for documenting, testing, and making an assessment on the effectiveness of internal controls.
[10]GAO-12-219.

Incomplete Implementation of SEC's Information Security Program

During our audit, we identified new deficiencies that limited the effectiveness of information security controls protecting the confidentiality and integrity of key financial systems and databases that support financial reporting. Specifically, SEC had not consistently or fully implemented controls for identifying and authenticating users, authorizing access to resources, ensuring that sensitive data are encrypted, or auditing actions taken on its systems. In addition, SEC had not installed patch updates on its software, exposing it to known vulnerabilities, which could jeopardize data integrity and confidentiality.

- **Controls were not consistently implemented for identifying and authenticating users.** A computer system needs to be able to identify and authenticate each user so that activities on the system can be linked and traced to a specific individual. An organization does this by assigning a unique user account to each user, and because of this, the system is able to distinguish one user from another—a process called identification. The system also needs to establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. The combination of identification and authentication—such as user account password combinations—provides the basis for establishing individual accountability and for controlling access to the system. SEC policy requires password controls such as complex passwords and account lockout after unsuccessful log-in attempts, as well as disabling inactive accounts. However, the commission had not enforced complex passwords or account lockout for certain servers supporting key financial applications, nor had it disabled inactive accounts on one server. As a result, SEC is at increased risk that accounts could be compromised and used by unauthorized individuals to access sensitive information.
- **Weaknesses in authorization controls limited their effectiveness.** Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic principle for securing computer resources and data that means that users are granted only those access rights and permissions that they need to perform their official duties. SEC policy requires that each user or process be assigned only those privileges or functions needed to perform authorized tasks. However, SEC did not always employ the principle of least privilege when authorizing access permissions. Specifically, it did not appropriately restrict security-related parameters and users' rights and privileges for certain network devices, databases, and servers supporting key financial applications. As a result, users have excessive levels of access that were not required to perform their jobs. This could lead to data being inappropriately modified, either inadvertently or deliberately.

- **Certain sensitive data were transmitted unencrypted.** Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption, which is used to transform plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. According to the National Institute of Standards and Technology (NIST), employing encryption protects the confidentiality and integrity of transmitted data. However, SEC did not configure servers supporting key financial applications to use encryption when transmitting data. As a result, increased risk exists that transmitted data can be intercepted, viewed, and modified.
- **Certain systems were not configured to maintain audit trails of security-relevant events.** To establish individual accountability, monitor compliance with security policies, and investigate security violations, organizations need to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail—a log of system activity—that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security-relevant events. Accordingly, SEC requires the enforcement of auditing and accountability by configuring information systems to produce, store, and retain audit records of system, application, network, and user activity. However, SEC had not consistently configured certain servers supporting key financial applications to maintain audit trails for all security-relevant events. As a result, increased risk exists that the commission will be unable to determine (1) if certain malicious incidents have occurred and (2) who or what caused them.
- **Systems were not routinely and consistently patched.** Configuration management involves, among other things, (1) verifying the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) obtaining reasonable assurance that systems are configured and operating securely and as intended. Patch management, a component of configuration management, is an important element in mitigating the risks associated with software vulnerabilities. When a software vulnerability is discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. Without the patch, an attacker can exploit a software vulnerability to read, modify, or delete sensitive information; disrupt operations; or launch attacks against systems at another organization. SEC policy requires remediation efforts, such as patching, to be implemented within 7 days or less for those vulnerabilities deemed of high importance or critical. However, the commission did not routinely and consistently patch servers supporting key financial applications in a timely manner. Failing to apply critical patches increases the risk of exposing SEC systems to vulnerabilities that could be exploited.

An underlying reason for these deficiencies is that SEC has not fully implemented elements of its information security program. Specifically, SEC did not consistently take the following actions:

- **Develop baselines and guidance for securely configuring systems.** NIST guidance recommends developing, documenting, and maintaining a baseline configuration of information systems. In addition, the United States Government Configuration Baseline provides the baseline security settings that federal agencies are required by the Office of Management and Budget (OMB) to implement, for platforms such as Windows, to improve information security and reduce overall information technology (IT) operating costs. Also, SEC policy requires that it establish and maintain baseline configuration standards for its systems. However, SEC management did not develop or maintain baseline configurations of security settings or associated guides for configuring several of its systems and devices. In addition, in its fiscal year 2011 Federal Information Security Management Act of 2002 (FISMA) reporting,[11] the commission reported that it did not have an automated capability that provided visibility into the system configurations of any of its IT assets. As a result, SEC risks not being able to ensure that its systems are securely configured in accordance with federal and commission policies.
- **Document security requirements for an SEC subsystem in a system security plan.** According to NIST, organizations should document security requirements for information systems—and any subsystems they contain—as part of the process of certifying a system to operate. However, SEC did not document security requirements for its EDGAR/Fee Momentum subsystem[12] in its security plan for EDGAR. Without documenting these requirements, SEC risks not effectively securing the EDGAR/Fee Momentum subsystem.
- **Scan for vulnerabilities in all its systems and applications.** NIST recommends that organizations implement a vulnerability management program that includes (1) scanning for vulnerabilities, (2) employing scanning tools and techniques that promote interoperability and automation, (3) analyzing vulnerability reports and results, and (4) sharing information obtained from the scanning process and assessments with appropriate personnel throughout the organization. However, SEC had not developed a comprehensive vulnerability management strategy, including a scanning schedule; performed compliance and vulnerability scans on its

[11]FISMA requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of its information security policies, procedures, practices, and compliance with requirements. *See* FISMA, *codified, in part, at* 44 U.S.C. § 3544.
[12]SEC requires publicly traded entities to use EDGAR, a web-based system for all fee-bearing filings. *See* SEC's Regulation S-T, *General Rules and Regulations for Electronic Filings*, *codified at* 17 C.F.R. part 232. EDGAR is the system used by these companies to file registration statements, periodic reports, and other forms electronically with SEC. The EDGAR/Fee Momentum subsystem processes the data entered into EDGAR with a registrant's filing and matches this data with collection information received from depository banks, which is then extracted, summarized, and transferred to SEC's general ledger system.

applications, databases, and network devices; or provided evidence of analysis and actions taken based on scan results. By not implementing a comprehensive vulnerability management scanning program, SEC is at increased risk of not being able to detect vulnerabilities that could jeopardize the security of its systems.

SEC officials stated that they had taken actions to correct several of the weaknesses we identified in the agency's security controls, but we have not yet verified the extent or effectiveness of SEC's actions as they occurred subsequent to the completion of our fiscal year 2011 financial audit.

Nevertheless, although SEC has made progress in strengthening information security controls intended to protect key financial information, control weaknesses continue to jeopardize the confidentiality and integrity of that information. These include deficiencies in SEC's controls for identifying and authenticating users, authorizing access to resources, ensuring that sensitive data are encrypted, and monitoring actions taken on its systems, as well as inconsistent patching of software. These increase the risk that unauthorized individuals could gain access to critical systems and intentionally or inadvertently access, alter, or delete sensitive data or computer programs. Until SEC mitigates its control deficiencies and fully implements its information security program, it will continue to be at risk of ongoing deficiencies in the security controls over its financial and support systems and the information they contain.

Recommendations for Executive Action

To address the deficiencies in internal control over information security, we recommend that the Chairman direct the Chief Operating Officer (COO) and Chief Information Officer (CIO) to take the following specific actions:

1. Establish configuration baselines and related guidance for securing systems and monitoring system configuration baseline implementation.
2. Enhance the EDGAR security plan to document security requirements for the EDGAR/Fee Momentum subsystem.
3. Develop and implement a comprehensive vulnerability management strategy that includes routine scanning of SEC's systems and evaluation of such scanning to provide for any needed corrective actions.

In a separate report designated "Limited Official Use Only," we are also making 27 recommendations to enhance SEC's internal control over information security.

Inadequate Review of Service Auditors' Reports

During our audit, we found that SEC did not take appropriate action to address the audit reports of SEC's external service providers although a significant portion of SEC's collections, payroll, and investment transaction processing is performed by

U.S. Bancorp (for the Department of the Treasury's (Treasury) CA$HLINK[13] system), the Department of the Interior's National Business Center, and the Bureau of the Public Debt's Federal Investments Branch, respectively. As such, SEC places significant reliance on these service providers to determine whether its collections, payroll, and investment transactions are complete, valid, accurate, and timely.

In fiscal year 2011, each of these service providers contracted with an independent auditor to perform an audit of controls related to its service operations under Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization*. SSAE No. 16 provides authoritative guidance for service auditors to report on the design and operating effectiveness of controls at organizations that provide services to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting. The issuance of a service auditor's report prepared in accordance with SSAE No. 16 signifies that a service organization has had its control objectives and control activities examined by an independent auditing firm. The service auditor's report includes valuable information regarding the service organization's controls and the effectiveness of those controls and also identifies complementary user entity controls that should be implemented by the user entity to ensure that its control objectives are met.[14]

NIST recommends that organizations that authorize connections from systems outside of their authorization boundary[15] should monitor these connections on an ongoing basis to ensure that security measures are in place. In accordance with OMB Circular No. A-123 agency management should review the scope of the SSAE No. 16 service auditor's report (SSAE No. 16 report) in the context of the agency's overall internal control assessment and take timely and effective actions to address any deficiencies identified. Moreover, according to *Standards for Internal Control in the Federal Government*,[16] 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 levels.

---

[13]CA$HLINK is an electronic cash concentration, financial information, and data warehouse system used to manage the collection of U.S. government funds and to provide deposit information to federal agencies. CA$HLINK links federal agencies, financial institutions, the Federal Reserve Banks, and Treasury fund managers through an electronic network. It receives deposit information, initiates fund transfers, and concentrates daily deposits made through Financial Management Service-managed collection mechanisms, such as Treasury's General Account, Lockbox, Pay.gov, Credit Card, Paper Check Conversion, and Fedwire Deposit Systems, into Treasury's account at the Federal Reserve Bank. It also provides federal agencies with information (via the Internet) to verify deposits, Automated Clearing House (if check disbursements) and Fedwire transfers, and voucher adjustments to reconcile their accounts with Treasury.

[14]AT Section 801, *Reporting on Controls at a Service Organization*, defines complementary user entity controls as controls that management of the service organization assumes, in the design of the service provided by the service organization, will be implemented by user entities, and that if necessary to achieve the control objectives stated in management's description of the service organization's system, are identified as such in that description.

[15]NIST SP 800-53 (rev. 3), *Recommended Security Controls for Federal Information Systems and Organizations*, states that "authorization boundary" refers to all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

[16]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

In fiscal year 2011, based on our review of SEC's risk assessment of internal controls over financial reporting and its SSAE No. 16 report review process, 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 and mitigate for any control deficiencies of its service provider that affected the integrity and availability of SEC's information. Specifically, we found that SEC did not do the following:

- Have a documented process in place to review SSAE No. 16 reports from its lockbox[17] service provider to determine whether the service organization's controls were suitably designed and operating effectively. The SSAE No.16 report we were provided noted exceptions in user access privileges and shared administrative user identification and passwords.
- Timely evaluate or test the effectiveness of complementary user entity controls identified by the SSAE No. 16 report from its payroll service provider. The service provider's processing of transactions and controls over the processing were designed under the assumption that these complementary user entity controls would be placed in operation by its clients to ensure that control objectives were met. As a result, we concluded that SEC was unable to fully consider these controls as part of its assessment of the effectiveness of its internal control over financial reporting as of September 30, 2011. SEC completed its assessment of complementary user controls from its payroll service provider after the end of fiscal year 2011 and did not review the SSAE No. 16 report from its investments service provider. Consequently, SEC did not evaluate and test the design and operating effectiveness of the complementary user controls the service providers' auditors recommended.

As a result, SEC is at risk that it may not be aware of deficiencies in security controls that could affect SEC data. Further, as a result of these weaknesses in SEC's risk assessment and control monitoring process, SEC did not consider the complete financial reporting control environment for the areas evaluated and management did not identify all risks or test all of the key controls that drive a significant portion of its cash collections; payroll, which accounts for over 69 percent of gross costs in its statement of net cost; and investment operations.

Recommendation for Executive Action

To address the deficiencies in internal control over review of service auditors' reports, we recommend that the Chairman direct the COO and Chief Financial Officer (CFO) to take the following action:

4. As part of the risk assessment process, include steps for reviewing the SSAE No. 16 reports from all service organizations key to SEC's financial reporting control environment in time to allow appropriate actions to be taken before the

[17]Lockbox service refers to services necessary for a federal agency to process remittance documents and update its internal accounts receivable system. The lockbox service provider has to meet specific requirements and is authorized by the Financial Management Service to perform "lockbox services" for federal government agencies.

end of the fiscal year to address any identified deficiencies in the design and operating effectiveness of service organization or user entity controls.

Significant Deficiency over Financial Reporting and Accounting Processes

During our fiscal year 2011 audit, we found that SEC continued to carry out its financial reporting during fiscal year 2011 using numerous spreadsheets, databases, and data processing practices that relied on significant manual analysis, reconciliation, work-arounds, and review to calculate amounts for the general ledger transaction postings. Such manual processes are resource intensive and prone to error and, coupled with the significant amount of data involved, increased the risk of materially misstated account balances in the general ledger. [18]

During fiscal year 2011, we also found that SEC's financial reporting procedures were not always effective at ensuring the completeness and accuracy of the financial data obtained from its various systems or at detecting any errors or omissions in financial reporting activities. Specifically, our 2011 audit found that SEC did not accurately and completely allocate leasing costs to regional offices, resulting in misstated activity costs being reported across various organizations in its statement of net cost at June 30, 2011. According to SEC, these differences were caused by new organization codes containing leasing cost data that were included in the general ledger summary file used to identify allocable leasing costs but not considered in the manual queries designed to identify the cumulative amount of leasing costs that needed to be allocated. Contributing to this error was a lack of procedures for (1) notifying responsible personnel when changes are made to organization codes containing allocable costs and (2) comparing the sum of all allocated costs to the total actual costs of the various organizations to ensure that all such costs are allocated.

Standards for Internal Control in the Federal Government[19] provides that management should establish specific control activities to ensure that all transactions are completely and accurately recorded. Without effective controls over its cost allocation process, SEC is at increased risk of incomplete or inaccurate financial reporting.

Recommendation for Executive Action

To address the deficiencies in internal control over the financial reporting and accounting processes, we recommend that the Chairman direct the COO and CFO to take the following specific action:

5. Document and implement quality assurance procedures over the preparation of the statement of net cost, including a procedure to compare the sum of all allocated costs to the total actual costs of the various organizations to ensure that all such costs are properly and fully allocated.

[18]See enc. I for the list of 11 open recommendations relating to the continuing deficiencies related to financial statement preparation and reporting at SEC.
[19]GAO/AIMD-00-21.3.1.

Significant Deficiency over Budgetary Resources

During our fiscal year 2011 audit, we reported that consistent with our prior audits, we continued to find deficiencies in SEC's (1) recording of new obligations[20] and (2) monitoring of open obligations. These deficiencies resulted in misstatements in SEC's accounting records, which could affect the reliability of information reported in its Statement of Budgetary Resources (SBR).[21]

Deficiencies in Recording of Obligations

Our testing of new obligations as part of our fiscal year 2011 audit identified several control deficiencies over SEC's recording of obligations. Specifically, we found that SEC's (1) process for recording obligations was not effective, (2) procedures for delegation of authority for obligating budgetary funds for the agency lacked sufficient guidance to ensure the proper authorization of obligations activity, and (3) process for recording obligations did not ensure timely recording of obligations, in accordance with SEC policy.[22]

- SEC's process for recording obligations did not ensure accurate and complete recording of obligation data in the general ledger system. For example, for 3 of 45 new obligations we statistically selected for testing internal control over the process for recording obligations, we found that they were recorded in the wrong budget object class. Prior supervisory reviews of contract and obligation information did not detect these errors. We also found that 1 of 84 obligation transactions we statistically selected for testing at June 30, 2011, was recorded in the financial system at an incorrect amount. Although supervisory review of contract data was performed by the contracting officer (CO) in the contract management system, SEC's procedures for recording obligations in its financial records did not require supervisory review of obligation transaction and related contract data prior to recording them in the general ledger. In addition, we found that more than 50 percent of obligation records we tested did not have obligation information necessary to adequately track the ongoing validity of obligations, such as the end of the period of performance (POP), recorded in the general ledger. POP is not always recorded because SEC's general ledger system does not require this information to be recorded as part of the process of recording an obligation transaction in the general ledger. Without reliable POP information, SEC could not effectively use its financial system to routinely review obligations for ongoing validity and instead relied on detective controls, such as review of

[20]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.
[21]See enc. I for the list of eight open recommendations relating to the continuing deficiencies in SEC's accounting for its budgetary resources.
[22]SEC Regulation 14-1, *Administrative Control of Funds* (Apr. 14, 2011), allows 7 days for recording obligations in the financial systems.

undelivered orders (UDO)[23] based on a defined period of inactivity, for reporting of related amounts in the SBR. *Standards for Internal Control in the Federal Government* states that internal control activities should include a wide range of diverse control activities, such as approvals, authorizations, and reviews and verifications, to ensure that all transactions are completely and accurately recorded, and the creation and maintenance of related records that provide evidence of execution of these activities as well as appropriate documentation.

- SEC's guidance for recording obligations increased the risk of unauthorized commitments. In our testing of internal controls over the process for recording obligations, we found that 1 of the 45 transactions we tested was not approved by a warranted CO. This was due to a lack of clearly defined delegation of obligation authority for noncontractual obligations in SEC's Regulation (SECR) 14-1 *Administrative Control of Funds*, which is an internal regulation followed by all agency personnel. SECR 14-1 provided that the CO[24] is responsible for entering contractual obligations in the core financial management system. However, we noted that SEC's practice for recording obligations did not always reflect the stated agency regulation. SEC routinely incurred noncontractual obligations for agency expenditures such as training and small purchases that were not approved by a CO.[25] SEC's Office of Financial Management (OFM) developed certain standard operating procedures (SOP) and business process procedures documents (BPP) that authorized processing of obligation transactions that were approved by agency personnel other than a CO. *Standards for Internal Control in the Federal Government* provides that internal control should be clearly documented in management directives, administrative policies, or operating manuals.
- SEC's process for recording obligations did not ensure timely recording of obligations in the general ledger system. SEC's internal regulation allows 7 days after the obligation document was signed for recording of obligations in the financial systems.[26] However, we found that 2 of the 45 new obligations we tested for evaluating internal control over the process for recording obligations were not recorded within 7 days of when the obligation documents were approved. For both of these obligations, the delays occurred because while the

[23]UDOs represent the value of goods and services ordered and obligated that have not been received. This amount includes any orders for which advance payment has been made but for which delivery or performance has not yet occurred.

[24]COs are personnel delegated authority to enter into, administer, or terminate contracts by the agency head. COs shall be appointed in writing on a certificate of appointment, which shall state any limitations on the scope of authority to be exercised, other than limitations contained in applicable law or regulation. The Federal Acquisition Regulation (FAR) provides that COs may bind the government only to the extent of the authority delegated to them and that no contract shall be entered into by an agency unless the CO ensures that all requirements of law, executive orders, regulations, and all other applicable procedures, including clearances and approvals, have been met. *See* FAR, 48 C.F.R. subpart 1.6.

[25]Section 1.603-3(b) of the FAR states that agency heads are encouraged to delegate micro-purchase authority to individuals who are employees of the agency that will be using the supplies or services being purchased. Further, it states that individuals delegated this authority shall be appointed in writing in accordance with agency procedures. Section 2.101 of the FAR states that "micro-purchase" means an acquisition of supplies or services using simplified acquisition procedures, the aggregate amount of which does not exceed the micro-purchase threshold, which is generally $3,000.

[26]SECR 14-1, *Administrative Control of Funds.*

obligation document was signed by responsible personnel, indicating approval of the obligation, verification needed to record the obligation in the financial system had not been completed. As a result, obligation transactions were not always recorded promptly. *Standards for Internal Control in the Federal Government* states that transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions.[27]

Recommendations for Executive Action

To address the deficiencies in internal control over the accounting and reporting of budgetary resources, we recommend that the Chairman direct the COO and CFO to take the following specific actions:

6. Enhance current procedures for supervisory review to include required steps for ensuring (a) the accuracy and completeness of the obligation transaction and contract information prior to recording the obligation in the general ledger records and (b) timely recording of obligation transactions in the general ledger.
7. Implement system controls to ensure that all applicable information (such as POP) is recorded in the financial system and can be associated with its obligation record.
8. Implement system controls to provide for the review and approval of all obligation transactions and all related contract information by appropriate officials prior to posting the information in the general ledger records.
9. Revise agency regulation SECR 14-1 to clearly delineate circumstances under which authority for obligating agency budgetary resources can be delegated to appropriate personnel other than the CO, compare current SOPs and BPPs with SECR 14-1, and make any necessary conforming changes.

Deficiencies in the Monitoring of Open Obligations for Ongoing Validity

Our fiscal year 2011 audit found that SEC does not have key controls in place for timely reviewing open obligations for ongoing validity to facilitate complete and timely recording of downward adjustments[28] and contract closeout of open obligations that are no longer valid. Instead, SEC relies on detective controls, such as its UDO review and UDO accrual processes, for the proper financial reporting of certain of its budget activities in its SBR. However, we found that these detective controls were also not fully effective in ensuring the accurate status of recorded obligations.

[27]GAO/AIMD-00-21.3.1.

[28]A deobligation refers to an agency's cancellation or recording of downward adjustments of previously recorded obligations. OMB Circular No. A-11, § 20.5, provides that the deobligation should occur at the time there is documentary evidence that the contract price that was previously obligated is reduced.

According to an SEC SOP,[29] a UDO is to be identified for review for deobligation and closeout when there has been no activity for at least 6 months or 180 days. This SOP also specifies that SEC is to perform this UDO review twice a year, in February and August. As part of the UDO accrual process, SEC staff evaluate the results from this UDO review process, and then estimate and record any necessary accrual adjustments for downward adjustments relating to UDOs that were no longer valid for financial reporting purposes.[30] Because the UDO review is only performed twice a year, the accrual adjustment may not result in accurate obligation reporting on a quarterly basis.[31] Specifically, during our audit, we found that 1 of the 23 statistically selected obligations we tested for ongoing validity should have been deobligated but was not, nor was it included in SEC's accrual adjustment for recording downward adjustments for financial reporting. In addition, we found that 28 of the 45 recorded deobligations we tested were not deobligated timely, and for these 28, the contract closeout process or recording of the downward accrual adjustment took from 3 months to more than 3 years to complete after the end of the POP or completion of the contract. We also found that SEC does not routinely or consistently reconcile its obligation records with its vendors throughout the contract performance period, which contributed to the delays in the deobligation and contract closeout process that we found during our audit. Such reconciliations, if performed, could result in more timely (1) identification of recording errors, (2) deobligation of obligations that are no longer valid, and (3) contract closeout.

Standards for Internal Control in the Federal Government states that internal control activities occur at all levels and functions of the entity. They include a wide range of diverse control activities that management should establish, such as approvals, reconciliations, authorizations, and verifications, to ensure that all transactions are completely and accurately recorded, and the creation and maintenance of related records that provide evidence of execution of these activities as well as appropriate documentation. In addition, it states that transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. Without effective controls over monitoring open obligations for ongoing validity, SEC is at increased risk of inaccurately reporting of its budgetary resources.

Recommendation for Executive Action

To address the deficiencies in internal control over the accounting for obligation activity, we recommend that the Chairman direct the COO and CFO to take the following specific action:

10. Develop and implement procedures for ongoing monitoring of open obligations for validity and timely closeout of any open obligations that are no longer valid. These should include (a) quarterly review of open obligations for ongoing validity based on end of POP or contract completion dates and (b)

[29]SEC OFM, *Procurement: Unliquidated Obligation Review Process*, OFM Reference Guide 12-02 (Aug. 16, 2011).
[30]A UDO accrual is recorded as an adjustment, if contracts have not been closed out administratively.
[31]OMB Circular No. A-136, *Financial Reporting Requirements*, requires federal agencies to prepare quarterly unaudited interim financial statements.

reconciling SEC's records of contract activity and balances with its key vendors at least annually.

Other Less Significant Control Issues

In addition to the significant deficiencies we identified in our fiscal year 2011 audit report and discussed above, we identified other deficiencies in SEC's internal control that warrant management's attention. These control deficiencies identified in our fiscal year 2011 audit and our related recommendations for corrective action are discussed below.

Payroll Monitoring

During our audit, we found that certain SEC payroll controls intended to prevent or detect improper payroll disbursements were not operating as intended throughout the fiscal year. For example:

- SEC's policies and procedures for time and attendance administration provide that the primary certifying official may designate backup certifying officials to assume his or her responsibilities. Backup certifying officials must be at the same organizational level or above and have direct knowledge of the employees' time and attendance. Through our review of 45 payroll expenditures, we identified 1 for which an administrative officer certified the time card of an employee because the designated certifier did not have an alternate assigned within SEC's time and attendance system. GAO's guidance on controls over time and attendance reporting[32] provides that the integrity of the information in a time and attendance reporting system depends largely on the approval by a supervisor (or other official) with an appropriate basis for such approval.
- According to SEC policy, the division directors and office heads must review and certify the validity of employees listed in personnel on board listings (POL)[33] within 30 days of the end of each quarter to ensure that only active employees are receiving compensation. Any issues identified are to be communicated to SEC's Office of Human Resources for subsequent corrective action. During our audit, we found that on two occasions during the fiscal year, the division directors and office heads did not submit the POL certifications within the 30-day requirement.
- During our testing of 45 payroll disbursements, we found 3 for which leave, compensatory time, or both[34] were taken without prior management approval. SEC's policies and procedures for time and attendance administration provide

[32]GAO, *Maintaining Effective Control over Employee Time and Attendance Reporting*, GAO-03-352G (Washington, D.C.: January 2003). Under 31 U.S.C. § 3512(c), (d), commonly known as the Federal Managers' Financial Integrity Act of 1982, GAO is responsible for issuing standards and guidance on internal control for the federal government and has issued this guidance related to controls over employee time and attendance reporting.

[33]The POL report lists active SEC employees maintained by SEC's payroll service provider.

[34]Compensatory time off is time off with pay in lieu of overtime pay for irregular or occasional overtime work, or when permitted under agency flexible work schedule programs.

that all requested leave and compensatory time must be recorded officially in SEC's time and attendance system. Each employee is responsible for submitting requests for leave and compensatory time before submitting his or her time card. In undergoing validation, the employee's timekeeper is to ensure that all leave and extra hours recorded on the employee's time card are supported by appropriate documentation.

- We identified two employees who routinely did not verify their own time within SEC's time and attendance system. SEC's policies and procedures for time and attendance administration provide that each SEC employee is responsible for recording and submitting his or her own time card in a timely and accurate manner. Designated timekeepers are responsible for submitting a time card on behalf of an employee in rare instances when an employee is unable to enter and submit his or her own time card based on input from either the employee or the employee's certifier. In such instances, timekeepers must document the reason they are submitting on behalf of another employee and maintain this documentation with their time and attendance records. Certifying officials should monitor instances in which employees are not submitting their own time cards and work with those employees and timekeepers to limit such instances.

These deficiencies increase the risk that improper payroll disbursements or erroneous reporting of time and attendance will not be timely detected or corrected and impair the effectiveness of management's oversight of employees' time and attendance.

Recommendations for Executive Action

We recommend that the Chairman direct the COO and CFO to take the following specific actions:

11. Perform a review of roles within SEC's time and attendance system to ensure that all supervisors or managers designated as certifiers have an alternate responsible for reviewing the accuracy of time cards in their absence.
12. Develop and implement monitoring procedures to ensure that responsible management officials submit POL within the 30-day SEC policy requirement.
13. Develop procedures to provide for documented evidence of a certifying official's approval of leave and compensatory time before recording such transactions in the time and attendance system.
14. Develop and implement monitoring procedures to ensure that all time and attendance sheets recorded and submitted on behalf of another employee are supported by documented input from either the employee or the employee's certifier and include a valid reason for why a designated timekeeper is submitting a time and attendance sheet on behalf of another employee.

Implementation of Post-Judgment Interest Accounting Procedures

In fiscal year 2011, SEC implemented new policies and procedures for accruing monthly post-judgment interest amounts on outstanding disgorgement and penalty receivables[35] and the related liability balances.[36] However, our testing of collections on disgorgement and penalties receivables during the year found that these new procedures were not operating as intended, which resulted in misstatements in SEC's liability balances. For example:

- We identified instances in which a receivable[37] for post-judgment interest was recorded even though SEC did not have a claim to cash or other assets. In each of these instances, amounts were remitted by defendants in excess of their total outstanding principal and interest. Consistent with SEC's practices prior to the new procedures,[38] these collections were recorded as collections of post-judgment interest, which resulted in an overstatement of balances reported under SEC's Liability for Non-Entity Assets - Intragovernmental.
- SEC erroneously reported the compounded and noncompounded portions of post-judgment interest receivable under two separate liability line items, which was not in accordance with its policy. Specifically, under SEC's revised procedures,[39] post-judgment interest receivables were to be accounted for under Miscellaneous Receipts Fund 1435, *General Fund Proprietary Interest - Not Otherwise Classified*, and reported under SEC's Liability for Non-Entity Assets - Intragovernmental line item on the balance sheet. However, our testing identified that an error in SEC's posting configurations within its general ledger resulted in the compounded amounts of post-judgment interest being recorded in Deposit Fund 6563 and reported as a liability with the public even though such amounts should be treated as payable into the general fund of Treasury under SEC's policy.

[35]Under 28 U.S.C. § 1961, post-judgment interest accrues automatically on federal money judgments entered in a civil suit in federal court. Unless otherwise provided, post-judgment interest also accrues on SEC orders requiring the payment of disgorgement or penalties that the commission issues in administrative proceedings. *See* 17 C.F.R. § 201.601, 31 U.S.C. § 3717, and 31 C.F.R. § 901.9.

[36]A liability for disgorgement and penalties arises when an order is issued for SEC to collect disgorgement, penalties, and interest from securities law violators. When the commission or a court issues such an order, SEC establishes an accounts receivable due to SEC offset by a liability. The presentation of this liability on the balance sheet depends on several factors. If the court or commission order indicates that collections are to be retained by the federal government, the liabilities are classified as custodial and intragovernmental. If the order indicates that the funds are eligible for distribution to harmed investors, SEC will recognize a governmental liability. SEC does not record a receivable or liability on its financial statements for disgorgement and penalty amounts that another government entity, such as a court, or a nongovernmental entity, such as a receiver, has collected or will collect.

[37]Statement of Federal Financial Accounting Standards No. 1, *Accounting for Selected Assets and Liabilities*, provides that a receivable should be recognized when a federal entity establishes a claim to cash or other assets against other entities, either based on legal provisions, such as a payment due date (e.g., taxes not received by the date they are due) or goods or services provided. If the exact amount is unknown, a reasonable estimate should be made.

[38]Prior to April 30, 2011, SEC did not accrue post-judgment interest on disgorgement and penalties receivable in its general ledger system. Amounts remitted by defendants were applied to the principal with any remainder being recorded as post-judgment interest.

[39]SEC OFM, *Initial Accrual of Interest on Disgorgement and Penalty Accounts Receivable*, OFM Reference Guide B-05 (Apr. 30, 2011).

Consistent with *Standards for Internal Control in the Federal Government*,[40] SEC should have controls in place to provide reasonable assurance that its financial transactions are accurately recorded. Until users are adequately trained in using the new policies and procedures for accruing monthly post-judgment interest amounts on outstanding disgorgement and penalty receivables, and oversight and review processes over such transactions are strengthened, SEC does not have sufficient assurance that post-judgment interest will be consistently or accurately recorded or reported.

Recommendations for Executive Action

We recommend that the Chairman direct the COO and CFO to take the following specific actions:

15. Develop an oversight mechanism to ensure that disgorgement and penalty collections are processed and reported in accordance with existing SEC policies and procedures.
16. Revise existing posting configurations to account for liability balances related to compounded post-judgment interest amounts in accordance with SEC policy.

Accounting for Disgorgement and Penalty Transactions

As part of its enforcement responsibilities, SEC issues orders and administers judgments ordering, among other things, disgorgement, civil monetary penalties, and interest against violators of federal securities laws.[41] SEC is to recognize a receivable when it is designated in an order or a final judgment to collect the assessed disgorgement, penalties, and interest. SEC is also party to court orders directing violators of federal securities laws to pay amounts assessed to a federal court or to a nonfederal receiver acting on behalf of harmed investors. These court orders are not recognized as accounts receivable by SEC because the debts are payable to, and collected by, another party.

During our audit of SEC's fiscal year 2011 financial statements, we identified deficiencies concerning SEC's accounting for disgorgement and penalty transactions. Although these errors did not materially affect the financial statements, such deficiencies present a risk that errors could occur and not be detected. For example:

- As discussed above, SEC is party to court orders directing violators of federal securities laws to pay amounts to other federal entities. In this capacity, under federal law, SEC is responsible for referring delinquent debts owed to SEC, the

[40]GAO/AIMD-00-21.3.1.

[41]A disgorgement is the repayment of illegally gained profits (or avoided losses), which SEC has authority to distribute 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.

courts, and other federal agencies to Treasury for collection, regardless of the payee. Any amounts collected by Treasury are transmitted to SEC. We found that SEC's procedures provided for accounting for disgorgement and penalty collections that were payable to other federal entities but were remitted to SEC, as governmental liabilities, which is not in accordance with generally accepted accounting principles[42] and which resulted in SEC overstating its Liability for Disgorgement and Penalties line item on its balance sheet.

- We identified one instance in which the receipt of moneys remitted to an SEC field office was not timely communicated to OFM or deposited in accordance with SEC policy and the Miscellaneous Receipts Statute. Unless an exception applies, the Miscellaneous Receipts Statute and related implementing Treasury regulations require all executive agencies to achieve same-day or next-day deposit of all collections of federal moneys into the U.S. Treasury.[43] Under SEC's existing procedures for recording collections, OFM has responsibility for depositing check receipts and recording collections of disgorgement and penalty amounts received by SEC in the general ledger. Any checks received by other divisions and offices are to be immediately forwarded to OFM for processing. In this instance, the check was not forwarded to OFM for deposit until April 2011, 9 months after the check issue date and days before the check expiration date.

Recommendations for Executive Action

We recommend that the Chairman direct the COO and CFO to take the following specific actions:

17. Revise existing procedures to account for amounts collected on behalf of other federal entities as intragovernmental liabilities.
18. Augment existing policies and procedures for check collections to include specific required steps for handling amounts remitted to SEC field offices to ensure compliance with the Miscellaneous Receipts Statute and related Treasury regulation.

The Government Purchase Card Program

Appendix B of OMB Circular No. A-123, *Improving the Management of Government Charge Card Programs*, prescribes that managers should mitigate the risk of misuse, delinquency, or both in agency charge card programs by (1) performing periodic reviews of the number of charge card accounts in use for the appropriateness of number and continued necessity as well as evaluating the span of control for approving officials (AO) and (2) establishing a control to ensure that

[42]Statement of Federal Financial Accounting Standards No. 1, *Accounting for Selected Assets and Liabilities*, provides that agencies should distinguish between intragovernmental and governmental liabilities. Intragovernmental liabilities are amounts that a federal entity owes to other federal entities. Governmental liabilities are amounts that the federal government or an entity within the federal government owes to nonfederal entities. SEC reports intragovernmental and governmental liabilities related to disgorgement and penalties under its Custodial Liability and Liability for Disgorgement and Penalties line items, respectively.

[43]*See* Miscellaneous Receipts Statute, 31 U.S.C. § 3302(b),(c), and Treasury Regulation on Collection and Deposit Timeframe Requirements, 31 C.F.R. § 206.5.

card accounts are canceled when employees retire or leave the agency. SEC's internal regulations[44] designated the Agency Program Coordinator (APC) responsible for overseeing the issuance and retention of purchase cards. Under these regulations, the APC is responsible for ensuring that purchase cards are limited to employees with a continuing, bona fide need. Moreover, SEC internal regulations require that when cardholders become aware of their reassignment or departure from the agency, or no longer require a purchase card, they are to immediately notify their designated AO[45] so that he or she can coordinate with the APC to suspend the cardholder's account prior to the cardholder's reassignment or departure.

Our review of purchase card accounts active as of June 30, 2011, found that SEC did not implement fully effective controls over its purchase card accounts. Specifically, our review identified two active accounts for employees who separated from SEC in fiscal year 2010, and several accounts in which the designated AO no longer worked at SEC. These control deficiencies over active purchase card accounts increase the risk of fraud, waste, and error in government charge card programs.

Recommendation for Executive Action

We recommend that the Chairman direct the COO and CFO to take the following specific action:

19. Establish an oversight monitoring mechanism to ensure that periodic reviews of cardholder and AO accounts are being performed in accordance with Appendix B of OMB Circular No. A-123.

Status of Prior Audit Recommendations

During our audit of SEC's fiscal year 2011 financial statements, we found that SEC took action to address many of the recommendations from our prior audits. Specifically, as summarized in enclosure I, SEC took action to fully address 38 of the 66 recommendations reported as open in our March 29, 2011, management report.[46] The 28 recommendations that remained open as of the end of our fiscal year 2011 financial statement audit relate to information system security controls, financial statement preparation and reporting, accounting for budgetary resources, registrant deposits, disgorgement and penalties and investments, nonpayroll disbursement and accrual transactions, and property and equipment.

[44]SECR 10-6, *Government Purchase Card Program* (Aug. 31, 2009).
[45]In purchase card programs, the AO ensures that the purchase card is used properly. The AO also authorizes cardholder purchases (for official use only) and ensures that the statements are reconciled and submitted to the designated billing office in a timely manner. Under SEC policy, an AO is assigned to a purchase card account when it is first established.
[46]GAO-11-348R.

Agency Comments

In her April 2, 2012 written comments on a draft of this report, the SEC Chairman stated that continued improvement in the agency's internal control structure, particularly in the areas of information security, financial reporting and accounting processes, budgetary resources, and registrant deposits and filing fees, is a top priority. The Chairman stated that the centerpiece of SEC's effort to strengthen financial controls is to migrate SEC's core financial system and transaction processing to a federal shared service provider. The Chairman also cited a number of additional interim steps the agency has underway to address the deficiencies in our draft report, including: tightening controls over spreadsheets and other user-developed applications used in financial reporting; strengthening the process for de-obligating funds from completed contracts; and reevaluating its processes for reviewing filing fees paid by registrants, and addressing the SEC's backlog of inactive registrant deposit accounts. We will evaluate SEC's actions, strategies, and plans as part of our fiscal year 2012 audit. SEC's written comments are reprinted in enclosure II. SEC also provided technical comments, which we considered and incorporated as appropriate.

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.

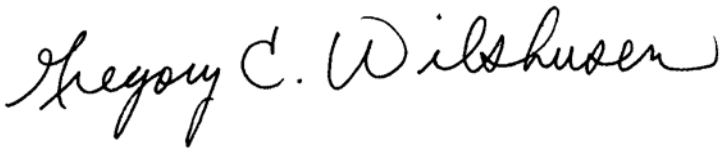
This report is intended for use by SEC management. We are sending copies of this report to the Chairmen and Ranking Members of the Senate Committee on Banking, Housing, and Urban Affairs; the Senate Committee on Homeland Security and Governmental Affairs; the House Committee on Financial Services; and 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 the GAO website 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 2011 and 2010 financial statements. If you have any questions about this report or need assistance in addressing these issues, please contact Jim Dalkin at (202) 512-3133 or dalkinj@gao.gov or Greg Wilshusen at (202) 512-6244 or

wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in enclosure IV.

Sincerely yours,

James R. Dalkin
Director, Financial Management and Assurance



Gregory C. Wilshusen
Director, Information Security Issues

Enclosures - 4

Enclosure I: Status of Recommendations from Prior Audits Reported as Open in GAO's 2010 Management Report

Table 1 presents GAO's assessment of the status of the 66 recommendations to the Securities and Exchange Commission (SEC) reported as open in GAO's March 29, 2011, management report. The weaknesses are grouped according to the deficiency area.

Table 1: Status of Recommendations from Prior Audits Reported as Open in GAO's 2010 Management Report (as of the End of GAO's Audit of SEC's Fiscal Year 2011 Financial Statements)

Audit area	Year initially reported	Status of corrective action	
		Completed	In progress
Information system security controls			
1. Establish and implement appropriate controls to mitigate any additional risks that were identified as a result of SEC's reevaluation of 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.	2010		X
2. Conduct an analysis of the cost and benefits of relocating the ADC to a different geographical area in comparison with the cost of re-creating data if a major disaster compromised data at both OPC and ADC locations.	2011	X	
3. Establish a mechanism to ensure current procedures for audit logging and audit log monitoring activities are followed for all financial systems.	2011	X	
4. Establish a mechanism to ensure current procedures for implementing all elements of an entitywide information security program for general support systems (GSS) are followed, consistent with FISMA requirements and NIST guidance.	2011	X	
5. Establish a mechanism to ensure current procedures to ensure timely follow-up on outstanding GSS POA&M items are followed, consistent with SEC policy.	2011	X	
6. Establish a mechanism to ensure current procedures to periodically review the information system access and roles of all SEC personnel for suitability and compliance with authorized security forms are followed, consistent with SEC policy.	2011	X	
7. Perform and document a BIA for the GSS in accordance with SEC policy.	2011	X	
Financial statement preparation and reporting			
8. 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.	2010		X
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.	2010	X	
10. 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.	2010		X
11. 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.	2010		X

Audit area	Year initially reported	Status of corrective action: Completed	Status of corrective action: In progress
12. 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.	2010		X
13. 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.	2010		X
14. 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.	2010		X
15. Develop and implement a process for reliably preparing accurate pro forma financial statements and updating the notes that accompany financial statements prior to year-end, preferably with the third quarter reporting.	2010		X
16. 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.	2010		X
17. 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.	2010		X
18. Augment policies and procedures concerning supervisory review of key spreadsheets used for financial disclosures to provide assurance that calculations within the spreadsheets are accurate.	2011		X
19. Augment existing control procedures over the processing of JV transactions to provide assurance that JVs processed into the general ledger reflect transactions approved by management. Such procedures should provide for accurate JV transaction posting at the account, fund, organization, and budget object class levels.	2011		X
20. Augment procedures concerning SEC's review of its financial statements to specify review steps necessary to ensure that all applicable financial statements, related notes, and required supplementary information required under OMB Circular No. A-136 are presented.	2011	X	
21. Augment policies and procedures to ensure the completeness of the GL Summary file used to prepare monthly trial balance reports, including procedures for identifying and notifying management and key users of any errors or omissions detected in the report.	2011	X	
22. Augment existing control procedures over the GL Summary file by requiring documented approval by SEC management before making the file available to key users to calculate manual adjustments.	2011	X	
23. Develop and implement procedures over the preparation of the monthly accounts payable accrual calculation and entry to provide assurance that all organization codes are included in the calculation.	2011	X	
24. Augment policies and procedures concerning SEC's monthly review and recalculation of securities transaction fee assessments to include procedures to ensure that the appropriate fee rate is used in the calculation of accounts receivable.	2011	X	
Accounting for budgetary resources			
25. 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
26. Establish and implement controls to ensure that SEC staff adheres to existing policies and procedures to prevent violations of the recording statute.	2008		X
27. Strengthen existing control procedures for recording miscellaneous purchase order documents by requiring an approved purchase requisition before certifying fund availability.	2010	X	

Audit area	Year initially reported	Status of corrective action: Completed	Status of corrective action: In progress
28. Develop and implement reconciliation, validation, and analytical procedures to ensure the reliability of the Open Obligations Review Reports used by the various SEC divisions and offices in their review of unliquidated obligations.	2011		X
29. Augment existing policies and procedures for recording obligations to include, at a minimum, (a) backup procedures for the recording of obligations in the event that responsible employees are unable to perform their assigned duties and (b) controls designed to ensure that SEC offices submit obligating documents to OFM for processing as obligations are incurred.	2011		X
30. Augment guidance in SEC's *Unliquidated Obligation Review Process* to provide, at a minimum, (a) clarifying and communicating the responsibilities for recording deobligations and (b) clarifying when to deobligate unliquidated obligations with no recent activity for financial reporting purposes and for contract closeout purposes for completed contracts to be consistent with applicable federal financial reporting guidance and OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*.	2011	X	
31. Develop and implement documented control procedures to ensure liquidation and/or deobligation of remaining travel obligations after the completion of the travel.	2011		X
32. Until such time that SEC is able to correct configuration limitations of its general ledger system, implement procedures to prepare and post correcting budgetary transactions prior to the close of the monthly accounting period.	2011		X
33. Augment existing policies and procedures to provide for supporting documentation for MOs consistent with applicable guidance provided in OMB Circular No. A-11.	2011		X
34. Develop and implement policies and procedures detailing the steps and documentation required to effectively control and monitor travel expenses paid through the central billing account (CBA), including steps required to ensure documented receipt of refunds or credits for travel/tickets that were previously paid for by SEC but subsequently canceled.	2011		X
Registrant deposits and filing fees			
35. Allocate sufficient resources to fully resolve current registrations' deposits liability balances in accordance with SEC policy and with federal regulations.	2010		X
36. Design and implement controls to ensure registrant filings and deposits are consistently matched timely on an ongoing basis.	2010	X	
37. Develop and implement procedures to include the use of periodic (i.e., weekly and monthly) system-generated reports to facilitate oversight of registrant deposits accounts, such as developing and using exception reports of registrant account activity.	2010	X	
Disgorgement and penalties and investments			
38. 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.	2010		X
39. Reconfigure the disgorgements and penalty accounts receivable module to enable production of an accounts receivable aging report.	2010		X
40. Develop and implement an automated subledger that interfaces with the general ledger for investment and disgorgement and penalty liability transaction activity.	2010		X
41. 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 nonintegrated subsidiary systems to include appropriate supervisory reviews.	2010	X	
42. Augment current procedures to require that Enforcement's reviews of disgorgement and penalty data in the case-management system be completed prior to closing the accounting period.	2011		X

Audit area	Year initially reported	Status of corrective action: Completed	Status of corrective action: In progress
43. Develop and implement policies and procedures to calculate and accrue for post-judgment interest amounts collectible prior to closing the accounting period in accordance with generally accepted accounting principles.	2011	X	
44. Develop and implement policies and procedures to identify and post receivable transactions for court orders initiating the transfer of moneys to the SEC after a distribution has occurred in accordance with generally accepted accounting principles.	2011	X	
45. Develop and implement procedures to provide for footnote disclosures concerning post-judgment interest amounts accrued on uncollectible accounts receivable in accordance with generally accepted accounting principles.	2011	X	
46. Develop and implement policies and procedures to reconcile investment balances reported by BPD to SEC records of investment purchase and withdrawal transactions processed during the reporting period.	2011	X	
47. Develop and implement policies and procedures to reconcile SEC's calculated interest receivable to interest receivable amounts reported by BPD.	2011	X	
48. Develop and implement policies and procedures to record investment activity in the general ledger using investment purchase and withdrawal requests submitted to BPD.	2011	X	
49. Establish and implement procedures for recording all check collections in the general ledger in the same fiscal period they are received in accordance with generally accepted accounting principles.	2011	X	
50. Revise existing posting configurations to account for amounts disbursed from SEC's Deposit Suspense Liability accounts in accordance with the USSGL.	2011		X
51. Until posting configurations for amounts disbursed from SEC's Deposit Suspense Liability accounts are corrected, establish and implement interim procedures to evaluate balances residing in SEC's Deposit Suspense Liability accounts and adjust related accounts for amounts that have already been disbursed prior to the close of each accounting period.	2011	X	
Nonpayroll disbursement and accrual transactions			
52. Develop and implement procedures to provide for appropriately documented COTR review of all vendor invoices prior to payment in compliance with SEC regulation.	2010		X
53. 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.	2010	X	
54. Investigate the causes of late payments and any interest penalties incurred and develop and implement any necessary corrective actions.	2010	X	
55. Augment procedures over the preparation of the monthly accounts payable accrual entry to provide for identification of all instances in which a good or service has been received and accepted but has not yet been paid prior to month-end.	2011	X	
56. Establish a mechanism to monitor compliance with the documentation requirements under SECR 10-15 to ensure proper, consistent approval of invoices by COTRs and IAOs and retention of their appointment letters.	2011	X	
Payroll processing and reporting			
57. Establish and implement procedures for documenting evidence of monitoring of time card certifications and include procedures to document any identified exceptions.	2008	X	
58. Develop procedures for implementing management's policy on the authorization and validation of personnel actions and the timely processing of such actions.	2009	X	
59. Develop and implement controls over access rights in the time and attendance system to prevent or timely correct any excessive access in the system.	2010	X	

Audit area	Year initially reported	Status of corrective action: Completed	Status of corrective action: In progress
60. 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.	2010	X	
61. 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.	2010	X	
62. Establish and implement procedures requiring review of the payroll service provider SAS 70 report to include consideration of whether compensating controls are needed to address any open exceptions in the report that affect SEC's payroll processing.	2011	X	
Property and equipment			
63. 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.	2010		X
Risk assessment and monitoring processes			
64. 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.	2010	X	
65. 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.	2010	X	
66. 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.	2010	X	

Source: GAO analysis of SEC data.

Enclosure II: Comments from the Securities and Exchange Commission

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

THE CHAIRMAN

April 2, 2012

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

Dear Mr. Dalkin:

Thank you for the opportunity to respond to the draft report entitled *Management Report: Improvements Needed in SEC's Internal Controls and Accounting Procedures* (GAO-12-424R). The report contains a number of helpful recommendations to strengthen the SEC's internal controls over financial reporting.

I am extremely pleased that the GAO found the SEC had no material weaknesses in its financial controls audit for FY 2011. I am gratified that the agency staff's hard work and dedication to building a strong internal control environment have yielded such significant results. As your draft report noted, our internal control structure continues to warrant additional improvements, particularly in the four significant deficiency areas of information security, financial reporting and accounting processes, budgetary resources, and registrant deposits and filing fees. Continued improvement in the aforementioned areas is a top priority of the SEC.

As you know, the centerpiece of our effort to strengthen further our financial controls is to migrate our core financial system and transaction processing to a Federal Shared Service Provider, the Department of Transportation's Enterprise Services Center (ESC). We expect this initiative to improve long-term sustainability by enhancing system functionality, automating certain manual processes, and further enhancing financial management and reporting.

While the SEC works to ensure a successful system migration, the agency continues to take additional steps aimed to address deficiencies identified in your report. These efforts include:

- Tightening controls over spreadsheets and other user-developed applications used in financial reporting, based on risk;
- Strengthening our process for de-obligating funds from completed contracts, and ensuring we incorporate appropriate accounting adjustments for these amounts;
- Reevaluating our processes for reviewing filing fees paid by registrants, and addressing our backlog of inactive registrant deposit accounts;

- Further enhancing the policies and procedures around accounting for disgorgement, post judgment interest, and penalty transactions;
- Enhancing controls around the monitoring of payroll activities; and
- Standardizing Information Technology controls and applying them more consistently across the environment.

The SEC is committed to investing the time and resources to put its internal controls over financial reporting on a strong, sustainable path. I look forward to continuing to work with you in the coming months as our financial system migration and other internal control enhancements continue to unfold.

If you have any questions, please do not hesitate to contact Kenneth A. Johnson, the SEC's Chief Financial Officer, at (202) 551-4306.

Sincerely,

Mary L. Schapiro
Chairman

Enclosure III: 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:[47]

- 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. § 3512(c), (d), commonly known as the Federal Managers' Financial Integrity Act of 1982.
- 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.
- Evaluated the design and operating effectiveness of internal control over financial reporting based on the assessed risk.
- Tested relevant internal control over financial reporting.
- Evaluated SEC's assessment of its 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; the Prompt Payment Act; the Federal Employees' Retirement System Act of 1986; Full-Year Continuing Appropriations Act, 2011, which incorporates, by reference, certain provisions of the Financial Services and General Government Appropriations Act, 2010; and the Dodd-Frank Wall Street Reform and Consumer Protection Act.

We conducted our audit of SEC's fiscal years 2011 and 2010 financial statements in accordance with U.S. generally accepted government auditing standards. We believe our audit provided a reasonable basis for our conclusions in this report.

[47]For a further, more detailed explanation of our audit scope and methodology, see the discussion in our related financial audit report (GAO-12-219).

Enclosure IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

James R. Dalkin, (202) 512-3133 or dalkinj@gao.gov
Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contacts named above, the following individuals made key contributions to this report: Kristen A. Kociolek, Lead Assistant Director; Cheryl E. Clark; Lauren S. Fassler; Michael W. Gilmore; Meafelia P. Gusukuma; Nicole N. Jarvis; Jeffrey L. Knott; David E. Ramirez; Omyra M. Ramsingh; and Henry I. Sutanto.

(194875)