United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Federal Financial Management, Government Information, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EST
Wednesday, July 27, 2005

SECURITIES AND EXCHANGE COMMISSION

Results of Fiscal Year 2004 Financial Audit

Statement of David M. Walker
Comptroller General of the United States

May 2005

SECURITIES AND EXCHANGE COMMISSION

Results of Fiscal Year 2004 Financial Audit

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-05-880T, testimony before the Subcommittee on Federal Financial Management, Government Information, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Pursuant to the Accountability for Tax Dollars Act of 2002, the Securities and Exchange Commission (SEC) is required to prepare and submit to Congress and the Office of Management and Budget audited financial statements. GAO agreed, under its audit authority, to perform the initial audit of SEC's financial statements. GAO's audit was done to determine whether, in all material respects, (1) SEC's fiscal year 2004 financial statements were reliable, (2) SEC's management maintained effective internal control over financial reporting and compliance with laws and regulations, and (3) SEC's management complied with applicable laws and regulations.

Established in 1934 to enforce the securities laws and protect investors, the SEC plays an important role in maintaining the integrity of the U.S. securities markets.

GAO was asked by the Chairman of the Senate Subcommittee on Federal Financial Management, Government Information, and International Security, Committee on Homeland Security and Governmental Affairs, to present the results of its May 26, 2005, report, *Financial Audit: Securities and Exchange Commission's Financial Statements for Fiscal Year 2004* (GAO-05-244).

www.gao.gov/cgi-bin/getrpt?GAO-05-880T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jeanette M. Franzel at (202) 512-9471 or franzelj@gao.gov.

What GAO Found

The SEC's first ever financial audit was performed by GAO for fiscal year 2004. In reporting on the results of the audit, GAO issued an unqualified, or clean, opinion on the financial statements of the SEC. This means that SEC's financial statements presented fairly, in all material respects, its financial position as of September 30, 2004, and the results of operations for the year then ended. However, because of material internal control weaknesses in the areas of preparing financial statements and related disclosures, recording and reporting disgorgements and penalties, and information security, GAO issued an adverse opinion on internal controls, concluding that SEC did not maintain effective internal control over financial reporting as of September 30, 2004. However, SEC did maintain, in all material respects, effective internal control over compliance with laws and regulations material in relation to the financial statements as of September 30, 2004. In addition, GAO did not find reportable instances of noncompliance with laws and regulations it tested. It is important to remember that GAO's opinions on SEC's financial statements and internal controls reflect a point in time.

SEC prepared its first complete set of financial statements for fiscal year 2004 and made significant progress during the year in building a financial reporting structure for preparing financial statements for audit. However, GAO identified inadequate controls over SEC's financial statement preparation process including a lack of sufficient documented policies and procedures, support, and quality assurance reviews, increasing the risk that SEC management will not have reasonable assurance that the balances presented in the financial statements and related disclosures are supported by SEC's underlying accounting records. In addition, GAO identified inadequate controls over SEC's disgorgements and civil penalties activities, increasing the risk that such activities will not be completely, accurately, and properly recorded and reported for management's use in its decision making.

GAO also found that SEC has not effectively implemented information system controls to protect the integrity, confidentiality, and availability of its financial and sensitive data, increasing the risk of unauthorized disclosure, modification, or loss of the data, possibly without detection. The risks created by these information security weaknesses are compounded because the SEC does not have a comprehensive monitoring program to identify unusual or suspicious access activities.

SEC agreed with our findings and is currently working to improve controls in all these areas.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the results of our audit of the Securities and Exchange Commission's (SEC) fiscal year 2004 financial statements, the first complete set of financial statements SEC has prepared and has subjected to an independent audit.[1] Our recent report,[2] issued on May 26, 2005, presents the results of that audit. Today, I will discuss those results and the steps we believe SEC needs to take to improve its ability to produce timely and reliable financial statements, and to produce them efficiently and with reasonable assurance that they are fairly presented. These steps will also help SEC to produce complete and reliable information for internal management who make decisions about SEC operations and expenditures, and congressional stakeholders who provide oversight of SEC operations and make decisions about SEC funding.

The results of our audit were mixed—a clean opinion on the financial statements and an adverse opinion on internal control. Because we detected three material weaknesses in internal control, we concluded that SEC's internal control did not reduce to a relatively low level the risk of misstatements material to the financial statements. In other words, mistakes may occur and either go undetected by employees in the normal course of their work or be detected too late to prevent errors or fraud**.** The material weaknesses we found relate to SEC's internal control over (1) preparing financial statements and the related disclosures, (2) recording and reporting of disgorgements[3] and civil penalties,[4] and (3) information security. It is important to remember that our opinions on SEC's financial statements and internal controls reflect a point in time. SEC has stated its commitment to enhancing its financial and operational effectiveness. We and others have made recommendations, which if successfully implemented, would help SEC to generate timely, reliable, and useful financial information with which to make informed decisions, manage daily operations, and ensure accountability on an ongoing basis.

[1]The Accountability of Tax Dollars Act of 2002 requires certain agencies, including SEC, to prepare financial statements and have them audited.

[2]*Financial Audit: Securities and Exchange Commission's Financial Statements for Fiscal Year 2004*, GAO-05-244 (Washington, D.C.: May 26, 2005).

[3]Disgorgement is the repayment of illegally earned profits.

[4]A penalty is a monetary sum that is to be paid by the registrant to SEC as a result of a security law violation.

SEC has a very visible and prominent leadership role in promoting and enforcing accountability for corporations whose equity and debt securities are traded in the securities markets. Recently, this role has also encompassed helping to ensure the effective implementation of the Sarbanes-Oxley Act, with its emphasis on internal control and corporate governance for the companies it regulates. At a time when many corporations are striving to strengthen internal controls and improve financial reporting, SEC has the opportunity and responsibility to serve as a model of good practice. In that regard, SEC stated in its *2004 Performance and Accountability Report*, issued in May 2005, that SEC must lead by example with respect to the internal control requirements demanded of the private and federal sectors, and also articulated management's vision that SEC serve as the standard against which other federal agencies are measured. A higher standard of accountability is appropriate for SEC as a government regulatory agency; moreover, it is important to the success of SEC's programs, activities, and leadership in the business community and as a government regulator.

Audit Results

In our audit of the fiscal year 2004 financial statements for SEC, we found

- the financial statements as of and for the fiscal year ended September 30, 2004, including the accompanying notes, are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles;
- SEC did not have effective internal control over financial reporting (including safeguarding of assets), but had effective control over compliance with laws and regulations that could have a material effect on the financial statements as of September 30, 2004; and
- no reportable noncompliance with laws and regulations we tested.

We issued an unqualified, or clean, opinion on the SEC's financial statements. This means that the financial statements and accompanying notes present fairly, in all material respects, SEC's financial position as of September 30, 2004, and, as well, certain other financial information that the statements must provide: net cost, changes in net position, budgetary resources, financing, and custodial activities for the year then ended. We also found that the statements conform to U.S. generally accepted accounting principles. In order to reach our conclusions about the financial statements, we (1) tested evidence supporting the amounts and disclosures

in the financial statements, (2) assessed the accounting principles used and significant estimates made by management, and (3) evaluated the presentation of the financial statements.

We found three material weaknesses in internal control and thus issued an adverse opinion on internal control—stating that SEC management did not maintain effective internal control over financial reporting and the safeguarding of assets as of September 30, 2004. Internal control over financial reporting consists of an entity's policies and procedures that are designed and operated to provide reasonable assurance about the reliability of that entity's financial reporting and its process for preparing and fairly presenting financial statements in accordance with generally accepted accounting principles. It includes policies and procedures for maintaining accounting records, authorizing receipts and disbursements, and the safeguarding of assets. Because SEC makes extensive use of computer systems for recording and processing transactions, SEC's financial reporting controls also include controls over computer operations and access to data and computing resources.

Our opinion on SEC's internal control means that SEC's internal control did not reduce to a relatively low level the risk that misstatements material to the financial statements may occur and go undetected by employees in the normal course of their work**.** This conclusion on SEC's internal controls did not affect our opinion on SEC's financial statements. This is because during the audit process SEC made the adjustments identified during the audit as necessary for the fair presentation of its financial statements. However, the weaknesses we found could affect other, unaudited information used by SEC for decision making. Our evaluation of internal control covered SEC's financial reporting controls which also cover certain operational activities that result in SEC's financial transactions, such as activities pertaining to stock exchange transaction fees, public-filing fees, maintaining disgorgements and penalties receivable, payroll-related transactions, and others.

We also tested SEC's compliance with selected provisions of laws and regulations that have a direct and material impact on the financial statements. For example, we tested for compliance with sections of the Securities Exchange Act of 1934, as amended, that requires SEC to collect fees from the national securities exchanges and the National Association of Securities Dealers based on volume of stock transactions, and sections of the Securities Act of 1933, as amended, that requires SEC to collect fees from registrants for public filings. Our tests found no instances of

noncompliance that are reportable. We also found that SEC maintained, in all material respects, effective internal control over compliance.

I would now like to discuss in detail the three material internal control weaknesses we found during our audit.

Material Internal Control Weaknesses

SEC Needs to Improve Its Controls over Financial Statement Preparation and Reporting

We found that SEC did not have formalized processes or documentation for the procedures, systems, analysis of accounts, and personnel involved in developing key balances and preparing the financial statements and related disclosures. As I will discuss later, this issue is compounded by SEC's limitations with its financial management system. Also, SEC did not have formalized quality control or review procedures. As a result, we identified errors in the beginning asset and liability balances and in the September 30, 2004, draft financial statements prepared by SEC management, that if had not been corrected, would have resulted in materially misleading operating results for fiscal year 2004.

SEC's lack of formalized processes, documented procedures, and quality assurance checks, significantly delayed the reporting of fiscal year 2004 financial results, consumed significant staff resources, caused audit inefficiencies, and resulted in higher financial statement preparation and audit costs. I would like to highlight the following items we found:

- SEC did not have documentation providing an explanation or a crosswalk between the financial statements and the source systems, general ledger accounts, account queries, and account analyses.
- SEC did not maintain a subsidiary ledger for certain activities, such as customer deposit amounts pertaining to filing fees.
- Accounting staff had difficulty in retrieving support for certain account balances, such as undelivered-order amounts, and for certain property and equipment leases.
- Reconciliations of detail and summary account balances were not prepared for certain financial statement line items, such as for the

customer deposit liability relating to filing fees and the associated earned filing fee revenue; the accounts receivable related to exchange fees and the related amount of earned exchange fee revenue; and the budgetary accounts related to undelivered and delivered orders, thus requiring SEC staff to create an audit trail after the fact.

- There also was no consistent evidence of supervisory review of journal entries, including closing and adjusting journal entries made in connection with preparing quarterly and year-end financial statements.

- Comprehensive accounting policies and procedures were still in draft or had not yet been developed for several major areas related to financial statements, including disgorgements and penalties, filing fees, exchange fees, and fixed asset capitalization.

GAO's *Standards for Internal Control in the Federal Government*[5] requires that controls over the financial statement preparation process be designed to provide reasonable assurance regarding the reliability of the balances and disclosures reported in the financial statements and related notes in conformity with generally accepted accounting principles, including the maintenance of detailed support that accurately and fairly reflect the transactions making up the balances in the financial statements and disclosures. In addition, an effective financial management system includes policies and procedures related to the processing of accounting entries.

SEC's difficulties in the area of financial statement preparation are exacerbated because SEC's financial management system is not set up to generate the user reports needed to perform analyses of accounts and activity on a real-time basis leading to SEC's staff-intensive and time-consuming efforts to prepare financial statements. Because SEC does not maintain standard schedules for producing certain basic reports of account detail for analysis, users have to request reports generated on an ad hoc basis by a software application whose operations are known only to some SEC staff. Also, as I will discuss in more detail later, not all of SEC's systems used for tracking and recording financial data are integrated with the accounting system.

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

Federal agencies preparing financial statements are required to develop a financial management system to prepare a complete set of statements on a timely basis in accordance with generally accepted accounting principles. The financial statements should be the product of an accounting system that is an integral part of an overall financial management system with structure, internal control, and reliable data. Office of Management and Budget Circular No. A-127, *Financial Management Systems*, requires that each agency establish and maintain a single integrated financial management system—basically a unified set of financial systems electronically linked for agencywide support. Integration means that the user is able to obtain needed information efficiently and effectively from any level of use or access point. (This does not necessarily mean having only one software application covering all financial management system needs or storing all information in the same database.) Interfaces between systems are acceptable as long as the information needed to enable reconciliation between the systems is accessible to managers. Interface linkages should be electronic unless the number of transactions is so small that it is not cost beneficial to automate the interface. Reconciliations between systems, where interface linkages are appropriate, should be maintained to ensure data accuracy.

To support its financial management functions, SEC relies on several different systems to process and track financial transactions that include filing and exchange fees, disgorgements and penalties, property and equipment, administrative items pertaining to payroll and travel, and others. Not all of these systems are integrated with the accounting system. For example, the case-tracking system and the spreadsheet application used to account for significant disgorgement and penalty transactions and the system used to account for property and equipment are not integrated with the accounting system. Without a fully integrated financial management system, SEC decision makers run the risk of delays in attaining relevant data or using inaccurate information inadvertently while at the same time dedicating scarce resources toward the basic collection of information.

A properly designed and implemented financial statement preparation and reporting process (which encompasses the financial management system) should provide SEC management with reasonable assurance that the balances presented in the financial statements and related disclosures are materially correct and supported by the underlying accounting records. To address the issues related to SEC's financial statement preparation and

reporting processes, we recommended that SEC take the following 13 actions to improve controls over the process.

1. Develop written policies and procedures that provide sufficient guidance for the year-end closing of the general ledger as well as the preparation and analysis of quarterly and annual financial statements.

2. Establish clearly defined roles and responsibilities for the staff involved in financial reporting and the preparation of interim and year-end financial statements.

3. Prepare a crosswalk between the financial statements and the source systems, general ledger accounts, and the various account queries and analyses that make up key balances in the financial statements.

4. Maintain subsidiary records or ledgers for all significant accounts and disclosures so that the amounts presented in the financial statements and footnotes can be supported by the collective transactions making up the balances.

5. Perform monthly or periodic reconciliations of subsidiary records and summary account balances.

6. Perform a formal closing of all accounts at an interim date or dates to reduce the level of accounting activity and analysis required at year-end. The formal closing entails procedures to ensure that all transactions are recorded in the proper period through the closing date, and then closing the accounting records so that no new entries can be posted during that period.

7. Distinguish common closing and adjusting entries in a formal listing, which is used in the general ledger closing process and in preparing financial statements.

8. Require supervisory review for all entries posted to the general ledger and financial statements, including closing entries. A supervisor should review revisions to previously approved entries and revised financial statements and footnotes. All entries and review should be documented.

9. Establish milestones for preparing and reviewing the financial statements by setting dates for critical phases such as closing the

general ledger; preparing financial statements, footnotes, and the performance and accountability report; and performing specific quality control review procedures.

10. Use established tools (i.e., checklists and implementation guides) available for assistance in compiling and reviewing financial statements.

11. Maintain documentation supporting all information included in the financial statements and footnotes. This documentation should be more self-explanatory than what has been retained in the past. The documentation should be at a level of detail to enable a third party, such as an auditor, to use the documentation for substantiating reported data without extensive explanation or re-creation by the original preparer.

12. Take advantage of in-house resources and expertise in establishing financial reporting policies, internal controls, and business practices, as well as in review of financial statement and footnote presentation.

13. Develop or acquire an integrated financial management system to provide timely and accurate recording of financial data for financial reporting and management decision making.

In response to our audit findings, SEC plans to increase its financial reporting staff this fiscal year, formalize its policies and procedures, and solicit advice from corporate financial reporting experts within SEC. SEC senior management has reviewed and endorsed certain initial policies applied in the first year of financial reporting, and has modified or recommended others for further review. In addition, SEC plans to establish a formal audit committee to provide for regular review by key management officials and advise on policies and controls. SEC is undertaking a multiyear project to replace the existing case-tracking system with a system that is better designed for financial reporting purposes.

Now I would like to shift to the second material internal control weakness.

SEC Has Control Weaknesses over Disgorgements and Civil Penalties

As part of its enforcement responsibilities, SEC issues and administers judgments that order disgorgements and civil penalties against violators of federal securities laws. The resulting transactions for fiscal year 2004 involved collections of about $945 million, and recording and reporting of fiduciary and custodial balances on the financial statements.[6] SEC records and tracks information on over 12,000 parties in SEC enforcement cases involving disgorgements and penalties through a case-tracking system. However, the case-tracking system is not designed for financial reporting and is not integrated with SEC's general ledger accounting system, which accumulates, tracks, and summarizes SEC's financial transactions.

To compensate for limitations in the system, SEC staff compiles quarterly subsidiary ledgers using extensive and time-consuming procedures. After downloading financial information on disgorgements and penalties from the case-tracking system to a spreadsheet with thousands of cases and defendants with a magnitude of approximately 1 million data elements, SEC staff performs numerous calculations using the data in the spreadsheet to compile the disgorgement and penalty balances as of the end of each quarter. Such a process is inherently inefficient and prone to error. Further, since the source of the data included on the spreadsheet is from the case-tracking system, whose data reliability has been reported as a problem by SEC for the past three years,[7] it is imperative that specific control procedures be put in place to provide reasonable assurance over the completeness and reliability of the data in the case-tracking system. In addition, control procedures are needed to reduce the risk of errors in the spreadsheet and ultimately the reported financial statement information. Finally, when reviewing case files we noted instances in which the supporting documentation in the files contained notations by the case managers indicating that potential activities or transactions related to the case had occurred. However, there was not adequate supporting

[6]Fiduciary activities represent the moneys collected from federal securities law violators and maintained by SEC to be distributed to harmed investors. Custodial activities represent the moneys collected by SEC from violators of federal securities laws that are returned to the General Fund of the Treasury, as nonfederal individuals or entities do not have an ownership interest in these revenues.

[7]The Federal Managers' Financial Integrity Act (FMFIA) of 1982 (31 U.S.C. § 3512 (c)(d)) requires the head of each agency to annually prepare a statement that identifies material weaknesses in the agency's systems of internal accounting and administrative control and its plans and schedule for correcting them. SEC reported material weaknesses and related system nonconformance issues concerning data integrity and financial reporting for disgorgements and penalties in its 2002, 2003, and 2004 FMFIA reports.

documentation to support an entry to the case-tracking system. These instances raised questions about whether SEC's accounting and financial reporting information related to penalties and disgorgements was potentially incomplete or out-of-date.

As a result of the issues I have described, we concluded that SEC did not have adequate control procedures in place to provide adequate assurance over the reliability of financial information related to this area. Thus, our auditors performed additional testing over SEC's financial statement balances related to penalties and disgorgements. GAO's *Standards for Internal Control in the Federal Government* requires that agencies establish controls to ensure that transactions are recorded in a complete, accurate, and timely manner. Although SEC has a draft policy that covers certain aspects of accounting for disgorgements and penalties, it is not comprehensive. For example, the policy does not define who is responsible for recording disgorgement and penalty data or the documentation that should be maintained to support the amounts recorded. Of even greater importance, the policy does not identify controls that are critical for determining the amounts to be recorded and for reviewing entries for completeness and accuracy, including the specific types of controls needed for the quarterly downloading of data and use of the spreadsheets for arriving at the accounting entries. Nor does the policy address supervisory review necessary to ensure consistent application of the procedures.

A lack of comprehensive policies and controls over disgorgement and penalty transactions increases the risk that the transactions will not be completely, accurately, and consistently recorded and reported. In our audit of the estimated net amounts receivable from disgorgements and penalties, we did find errors in the recorded balances for the related gross accounts receivable and allowance for loss. Specifically, we noted errors where SEC had made entries to the accounting system that conflicted with information in the files. We also noted inconsistent treatment in recording judgments, interest amounts, terminated debts, and collection fees imposed by Treasury. We believe that these errors and inconsistencies occurred because of the control weaknesses we found. While, in most cases, these errors and inconsistencies were offsetting, such errors raise concern about the reliability of the $1.673 billion gross accounts receivable for disgorgements and penalties and the related allowance amounts of $1.394 billion reported in footnote 3 to SEC's financial statements.

To address internal control weaknesses over disgorgements and penalties, we recommended that SEC

1. implement a system that is integrated with the accounting system or that provides the necessary input to the accounting system to facilitate timely, accurate, and efficient recording and reporting of disgorgement and penalty activity;

2. review the disgorgement and penalty judgments and subsequent activities documented in each case file by defendant to determine whether individual amounts recorded in the case-tracking system are accurate and reliable;

3. implement controls so that the ongoing activity involving disgorgements and penalties is properly, accurately, and timely recorded in the case-tracking system and the accounting system;

4. strengthen coordination, communication, and data flow among staff of SEC's Division of Enforcement and Office of Financial Management who share responsibility for recording and maintaining disgorgement and penalty data; and

5. 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.

SEC agrees with our findings in this area and has begun efforts to strengthen internal controls. For example, SEC plans to complete a comprehensive review of files and data and review and strengthen policies and procedures for recording and updating amounts receivable for disgorgements and penalties. SEC anticipates that consistent application of strengthened internal controls and potentially some limited redesign of the existing management information system will be adequate to resolve the material weaknesses in fiscal year 2006. However, SEC acknowledges that a replacement of the current case-tracking system and a more thorough reexamination of the relevant business process would provide more effective assurance. Accordingly, in fiscal year 2006, SEC plans to complete a requirements analysis as the first phase of the multiyear project to replace the case-tracking system.

Now I would like to shift to the discussion of the material internal control weakness pertaining to information security.

SEC Needs to Address Weak Controls over Financial and Sensitive Data

Information system controls are essential for any organization that depends on computer systems and networks to carry out its mission or business and maintain key records and accountability information. Without proper safeguards, organizations run the risk that intruders may obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

SEC—which relies extensively on computer systems to support its operations—needs a comprehensive program of general controls[8] to monitor and manage information security risks. Our review[9] of SEC's information system general controls found that the commission did not effectively implement controls to protect the integrity, confidentiality, and availability of its financial and sensitive information.

In March 2005, we reported weaknesses in electronic access controls, including controls designed to prevent, limit, and detect access to SEC's critical financial and sensitive systems.[10] We found these weaknesses in user accounts and passwords, access rights and permissions, network security, and the audit and monitoring of security-related events. These weaknesses were heightened because SEC had not fully established a comprehensive monitoring program.

We identified the following electronic access control weaknesses:

- SEC operating personnel did not consistently set password parameters—such as a minimum of six digits including both numbers and letters—to ensure a level of difficulty for an intruder trying to guess a password, and users sometimes did create easy-to-guess passwords.

[8]Information system general controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. These controls include security management, operating procedures, software security features, and physical protection designed to ensure that access to data is appropriately restricted, computer security functions are segregated, only authorized changes to computer programs are made, and back-up and recovery plans are adequate to ensure the continuity of essential operations.

[9]GAO-05-244.

[10]See GAO, *Information Security: Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data*, GAO-05-262 (Washington, D.C.: March 23, 2005).

- All 4,100 network users were inadvertently granted access that would allow them to circumvent the audit controls in the commission's main financial systems.

- Key network devices were not configured to prevent unauthorized individuals from gaining access to detailed network system policy settings and lists of users or user groups.

- SEC did not have a comprehensive monitoring program for routine review, audit, or monitoring of system user-access activities. For example, audit logging, which is typically used to track certain types of activity on a system, was not consistently implemented on network services and there was no real-time capability to target unusual or suspicious network events for review. In addition, SEC had not fully implemented a network intrusion-detection system. The commission did, however, have several initiatives under way to monitor user access activity.

We also identified weaknesses in other information system controls—including physical security, segregation of computer functions, application change controls, and service continuity. For instance:

- At the time of our review, 300 employees and contractors had physical access to SEC's data center. Persons with access included an undetermined number of application programmers, budget analysts, administrative staff, and customer support staff. Typically, persons serving these functions do not need access to the data center for their work.

- SEC had not sufficiently separated incompatible[11] system administration and security administration functions on its key financial applications.

- Although a change control board at SEC was responsible for authorizing all application changes, none of the software modifications reviewed had documentation to show that such authorizations had been obtained.

[11]Incompatible functions are those that cause a conflict or risk if they are under the responsibility of the same person. For example, authorizing access and using that access are incompatible functions.

- SEC had not implemented a service-continuity plan to ensure that the system and its major applications could continue to function after a major disruption, such as a loss of electricity.

As a result of these weaknesses, sensitive SEC data—including payroll and financial transactions, personnel data, regulatory, and other mission-critical information—were at increased risk of unauthorized disclosure, modification, or loss.

A key reason for weaknesses in SEC's information system general controls is that the commission has not fully developed and implemented a comprehensive agency information security program. The Federal Information Security Management Act (FISMA) requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and systems that support the operations and assets of the agency. Agencies are required to use a risk-based approach to information security management. FISMA also requires an agency's information security program to include these key elements:

- periodic assessments of risk and the magnitude of harm that could result from unauthorized access, use, or disruption of information systems;

- policies and procedures that are based on risk assessments and risk reductions to ensure that information security is addressed throughout the life cycle of each system and that applicable requirements are met;

- security awareness training to inform all users of information security risks and users' responsibilities in complying with information security policies and procedures; and

- periodic tests and evaluations of the effectiveness of information security policies, procedures, and practices related to management, operational, and technical controls of every major system.

Although SEC has taken some actions to improve security management—including establishing a central security management group and appointing a senior information security officer to manage the information security program—further efforts are needed. For example, we found that the commission had not clearly defined roles and responsibilities for the central security group it had established. In addition, SEC had not fully (1) assessed its risks, (2) established or implemented security policies,

(3) promoted security awareness, or (4) tested and evaluated the effectiveness of its information system controls.

SEC and its Office of Inspector General (OIG) have recognized weaknesses in the commission's information security program. Since 2002, SEC has reported information security as a material weakness in its FMFIA reports. In its fiscal year 2004 FISMA report, SEC's OIG reported that the commission had several weaknesses in information security and was not substantially in compliance with information security requirements contained in FISMA.

Without proper safeguards for its information systems, SEC is at risk from malicious intruders entering inadequately protected systems. It is at risk that intruders will use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. We believe the primary cause of these weaknesses has been the lack of a fully developed and implemented entitywide information security program. In our March 2005 report,[12] we recommended 6 actions to fully develop and implement an effective security program. In addition, we made 52 recommendations to correct specific information security weaknesses related to electronic access control and other information system controls. Due to their sensitivity, these recommendations were included in a separate report designated for "Limited Official Use Only." A fully developed, documented, and implemented agency information security program would provide the commission with a solid foundation for resolving its information security problems and for ongoing management of its information security risks.

We believe that if our recommendations and SEC's planned actions are carried out effectively, SEC can make considerable progress toward its declared vision as "the standard against which federal agencies are measured"[13] and will be in a stronger position to manage its daily operations and accomplish its mission.

This testimony is based on our recent audit of SEC's fiscal year 2004 financial statements, which was conducted in accordance with U.S. generally accepted government auditing standards.

[12]GAO-05-262.

[13]U.S. Securities and Exchange Commission, *2004 Performance and Accountability Report*.

Mr. Chairman, this concludes my prepared statement. I would be pleased to respond to any questions that you or the other members of the Subcommittee may have.

Contacts and Staff Acknowledgements

For further information on this testimony, please contact Jeanette Franzel at (202) 512-9471 or at franzelj@gao.gov. and Greg Wilshusen at (202) 512-6244 or at wilshuseng@gao.gov. Individuals making key contributions to this testimony include Cheryl Clark, Kim McGatlin, Charles Vrabel, Estelle Tsay, Kristi Dorsey, and Maxine Hattery.

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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548