



THE CHAIRMAN

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

December 31, 2001

The Honorable George W. Bush
President of the United States
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear Mr. President:

I am pleased to report that the management controls of the Securities and Exchange Commission for the fiscal year ending September 30, 2001 are in compliance with the standards prescribed by the Comptroller General. This letter fulfills the reporting requirements of the Federal Managers' Financial Integrity Act of 1982 as they apply to the SEC. It has been prepared in conformity with the guidance provided by the Office of Management and Budget. A detailed discussion of the evaluation and review process supporting this conclusion is at Enclosure A.

I can provide assurance, based on the evaluations conducted by the staff, assurances by appropriate SEC officials, and other information provided that, taken as a whole, the agency's internal accounting and administrative systems comply with Section 2 of the Act.

The following material weakness was corrected during the year:

- The management controls for safeguarding sensitive, non-public information need to be strengthened to significantly enhance their effectiveness.

Safeguarding sensitive information is a critical activity at the SEC. To enhance the effectiveness of our controls over sensitive information, the Commission established a task force of senior staff to implement corrective actions, hired a security consultant to assist in a more comprehensive review of overall security, enhanced building access procedures, and issued an agency-wide policy that addresses employees' responsibilities to safeguard non-public information. The Commission has implemented the consultant's most significant recommendations and is continuing to monitor this area.

The agency continues to work aggressively on correcting the following material weakness that was identified previously and remains pending.

The Honorable George W. Bush

Page 2

- ADP security controls should be enhanced, strengthened, and communicated to all SEC staff. Many of the security administration processes performed by the SEC are not standardized or formalized. The lack of formalized policies and communication of adequate ADP security policies and procedures has the potential to impair the mission of the agency.

The IT Security Program has substantially completed its mission, which is to protect the SEC's sensitive information. The SEC's public website and electronic filing systems have remained secure and available; our perimeter security has detected and repelled countless probes, scans, and scripted attacks; and our intranet e-mail and critical applications have remained safe and available during numerous virus scares, major software upgrades, infrastructure changes, planned and unscheduled disaster recovery tests and failures, and other potentially catastrophic events. However, the IT Security Program, while robust and effective, still has some work ahead to grow into a mature program that is well documented and meets all federal guidelines. Under the direction of the agency's new IT Security Officer, the IT Security Group is finalizing a series of technical bulletins to support the SEC's IT security policy and developing a rigorous set of procedures for security certification and accreditation of agency systems. These critical milestones are expected to be completed during fiscal 2002 and 2003, respectively.

Additionally, the agency's financial management systems in use during 2001 were reviewed as required by Section 4 of the Act. The review was based on the principles and standards developed by the Comptroller General and implemented through OMB Circular A-127.

The results of limited reviews conducted of all of the agency's financial management systems, assurances given by agency officials, and other information provided indicate that the accounting systems, taken as a whole, are generally in conformance with the principles and standards developed by the Comptroller General and implemented through OMB Circular A-127.

The following material non-conformance was corrected during the year:

- The SEC needs to track the receipt and allocation of filing fee and account data and provide on-line inquiry, on a real-time basis, of specific filing fee information. A new agency system (Entity, Filing and Fees (EFFS)) was implemented in late fiscal 1992. However, since implementation, problems have been identified that inhibit the agency from maintaining real-time, accurate data.

The Honorable George W. Bush
Page 3

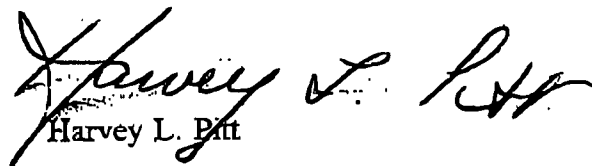
Through the efforts of a Commission task force assembled in November 1994, the agency improved significantly several features of the system and the reliability of EFFS financial data. However, the task force and an audit conducted by the SEC's Office of the Inspector General identified insufficient internal controls, lack of documentation, and difficulties maintaining the system such that a determination was made to redesign the system.

From fiscal 1995 to 1998, the task force worked on identifying EFFS system requirements and preparing a contract solicitation to replace the existing system. The EFFS redesign requirements were included with the EDGAR modernization initiative, which was awarded in July 1998. The EFFS replacement was implemented in September 2001. The design of the new system contains adequate financial controls.

Additional information regarding the agency's compliance with the Act and proposed corrective actions is contained in Enclosures B through D to this letter.

I would like to emphasize that the SEC is committed to the effective and efficient management of the resources entrusted to the agency.

Yours truly,



Harvey L. Pitt

Enclosures

Enclosure A

SECURITIES AND EXCHANGE COMMISSION
REVIEW PROCESSDescription of Organization and Structure of Review Process

The Office of the Executive Director is responsible for coordinating and overseeing the management control review process (OMB Circular A-123) and evaluations of financial management systems (OMB Circular A-127). The evaluation process is carried out by the management control officer assigned in each component, based upon instructions provided by the Executive Director. The Office of the Executive Director monitors correction of material weaknesses.

Twenty-six divisions and offices are designated as components. The components range in size from 9 to 489 positions with an average of 122 positions within a component at the end of fiscal 2001. Agency components were identified by evaluating the organization and budgetary allocations of the SEC and its activities. This segmentation ensures comprehensive coverage of all components.

2001 Statistical Data for Review Process

| | <u>Planned</u> | <u>Conducted</u> |
|----------------------------|----------------|------------------|
| Management Control Reviews | 0 | 0 |
| Alternative Reviews | 22 | 22 |

Percentage of Assessable Components Reviewed: 62%

Comment on Results Versus Plan

Twenty-two alternative reviews were completed in 2001. These reviews are conducted by the Commission's Office of Inspector General. The components reviewed consisted of five field offices; the Offices of General Counsel, the Secretary, the Executive Director, Investor Education and Assistance, Information Technology, Administrative and Personnel Management, Filings and Information Services, and Compliance Inspections and Examinations; and the Divisions of Corporation Finance, Market Regulation, and Enforcement. Some components underwent multiple reviews, and some not included in the above list were reviewed as part of audits that were not completed by the end of the fiscal year.

Enclosure B

SECURITIES AND EXCHANGE COMMISSION
STATISTICAL SUMMARY OF PERFORMANCESection 2. Management Control System

Overall Compliance Yes No Year Achieved
1983
(and all subsequent years)

Number of Material Weaknesses

| <u>Period Reported</u> | <u>Reported</u> | <u>Corrected</u> | <u>Pending at Year-End</u> |
|------------------------|-----------------|------------------|----------------------------|
| Prior Years | 31 | 28 | 3 |
| 1991 | 0 | 0 | 3 |
| 1992 | 0 | 0 | 3 |
| 1993 | 0 | 0 | 3 |
| 1994 | 1 | 2 | 2 |
| 1995 | 1 | 0 | 3 |
| 1996 | 0 | 1 | 2 |
| 1997 | 0 | 0 | 2 |
| 1998 | 0 | 0 | 2 |
| 1999 | 1 | 1 | 2 |
| 2000 | 0 | 0 | 2 |
| 2001 | 0 | 1 | 1 |

Pending Material Weaknesses

| <u>Category</u> | <u>Number</u> |
|--------------------------------------|---------------|
| Program Management: | |
| Program Execution | 0 |
| Systems Development & Implementation | 0 |
| Asset Disposition | 0 |
| Environmental Impact | 0 |
| Safety, Health-Related | 0 |
| Other (Specify) | 0 |

Enclosure B

Page 2

Functional Management:

| | |
|---------------------------------------|---|
| Procurement | 0 |
| Grant Management | 0 |
| Personnel & Organizational Management | 0 |
| ADP Security | 1 |
| Payment Systems & Cash Management | 0 |
| Loan Management & Debt Collection | 0 |
| Document Management | 0 |
| Total | 1 |

Section 4. Financial Management SystemsCompliance Assurance

| Overall Compliance with Section 4 | <u>Yes</u> | <u>No</u> | <u>Year Achieved</u> |
|--|------------|-----------|----------------------|
| • Conformance with Financial Information Standards | X | | 1989 |
| • Conformance with Systems Functional Standards | X | | 1989 |

Number of Material Non-conformances

| <u>Period Reported</u> | <u>Reported</u> | <u>Corrected</u> | <u>Pending at Year-End</u> |
|------------------------|-----------------|------------------|----------------------------|
| Prior Years | 3 | 3 | 0 |
| 1991 | 0 | 0 | 0 |
| 1992 | 1 | 0 | 1 |
| 1993 | 1 | 0 | 2 |
| 1994 | 0 | 0 | 2 |
| 1995 | 1 | 0 | 3 |
| 1996 | 0 | 1 | 2 |
| 1997 | 0 | 0 | 2 |
| 1998 | 0 | 0 | 2 |
| 1999 | 0 | 1 | 1 |
| 2000 | 0 | 0 | 1 |
| 2001 | 0 | 1 | 0 |

Enclosure C

SECURITIES AND EXCHANGE COMMISSION
MATERIAL WEAKNESSES/CORRECTIVE ACTION

1. ADP Security

Functional Category in Statistical Summary: ADP Security

Bureau/Appropriation/Account Number: Office of Information Technology

Administrative Activity/Program Activity: Data Processing--Nationwide

Pace of Corrective Action:

Year Identified: 1989

Original Targeted Correction Date: 1990

Targeted Correction Date in Last Year's Report: 2000

Current Target Date: 2003

Reason for Change of Date(s): Key members of the IT Security Group left the agency for the private sector in FY 2000, including the IT Security Officer. The new Security Officer is working aggressively to complete the two remaining critical milestones.

Description of Agency Impact: ADP security controls should be enhanced, strengthened, and communicated to all SEC staff. Many of the security administration processes performed by the SEC are not standardized or formalized. The agency also needs to ensure compliance with the revised OMB Circular A-130 requirements for ADP security administration and system certification. The lack of formalized policies and standards for security administration leaves the SEC vulnerable to fraud, mismanagement, and abuse of government resources. In addition, failure to certify sensitive application systems may result in loss of government resources if a problem goes undetected due to lack of timely review.

Source of Discovery of Material Weakness: The weakness was identified by the office head during the 1989 annual certification process and in a 1995 review by an outside auditor.

Critical Milestones in Corrective Action:

| <u>Critical Milestone</u> | <u>Original Plan</u> | <u>Current Plan</u> | <u>Actual</u> |
|---|----------------------|---------------------|---------------|
| Final ADP Security Policy | 5/92 | 1998 | 12/98 |
| Final Automated Information Security Manual (Technical Bulletins) | 6/92 | 2002 | -- |
| ADP Security Review Program | 6/92 | 1998 | 1998 |
| Certification and Accreditation Reviews | 6/92 | 2003 | -- |

Enclosure C

Page 2

A. Completed actions/events: Significant progress has been made in the ADP security area. Some examples of the more significant accomplishments to date follow.

- Restructured the Office of Information Technology.
- Established a Security Group in the Office of Information Technology.
- Issued an agency-wide IT security policy.
- Implemented an extensive security audit program.
- Developed a web-based application for system security plans.
- Conducted regular security posture assessments to identify system and network vulnerabilities.
- Drafted technical bulletins on a variety of security issues.
- Continued training SEC staff on security issues.
- Developed an internal website that is dedicated to security issues.
- Reviewed and approved all SEC operating system deployment and end user applications.
- Conducted inspections for password security, patch levels, service packs and hot fixes, anti-virus software, suid programs, permissions on files and directories, adequate logging levels, and security tool deployment.
- Periodically hired outside security experts to review the work conducted by the OIT Security Group.
- Developed a custom Intruder Detection System that actively monitors over 70 firewalls, servers, and general support hosts throughout the SEC.
- Implemented a new guideline that requires all new SEC applications to use certain encryption mechanisms.
- Isolated all external network connections behind firewalls.

B. Planned actions/events (short-term, *i.e.*, next 12 months): A series of technical bulletins will be issued to assist in implementing the IT Security Program. One-fourth of the agency's sensitive systems will be formally certified and accredited with contractor support.

C. Planned actions/events (long-term): The remaining sensitive systems will be certified and accredited. We will continue to improve the IT security program.

Enclosure C
Page 3

2. Sensitive Information

Functional Category in Statistical Summary: Document Management

Bureau/Appropriation/Account Number: Office of the Executive Director

Administrative Activity/Program Activity: Safeguarding Sensitive Information

Pace of Corrective Action:

Year Identified: 1999

Original Targeted Correction Date: 2000

Targeted Correction Date in Last Year's Report: 2000

Current Target Date: 2001

Reason for Change of Date(s): Not applicable. Corrective actions were completed in 2001.

Description of Agency Impact: The management controls for safeguarding sensitive, non-public information need to be strengthened to significantly enhance their effectiveness.

Source of Discovery of Material Weakness: The weakness was identified during an audit conducted by the Office of Inspector General.

Critical Milestones in Corrective Action:

| <u>Critical Milestone</u> | <u>Original Plan</u> | <u>Current Plan</u> | <u>Actual</u> |
|--|----------------------|---------------------|---------------|
| Establish Senior Level Task Force | 1999 | 1999 | 1999 |
| Implement New Building Access Procedures | 1999 | 1999 | 1999 |
| Hire Consultant to Review Information Security | 1999 | 1999 | 1999 |
| Issue Comprehensive Policy and Procedures to All Employees | 2000 | 2000 | 2000 |
| Implement Security Consultant Recommendations | 2000 | 2001 | 2001 |

A. Completed actions/events: To address this weakness, the Commission established a task force of senior staff to enhance the effectiveness of the agency's controls over sensitive information, enhanced building access procedures, issued a new policy that addresses employees' responsibilities to safeguard non-public information and hired a security consultant to review sensitive information security. The Commission implemented the consultant's most significant recommendations in fiscal 2001.

Enclosure C

Page 4

B. Planned actions/events (short-term, *i.e.*, next 12 months): The Commission will continue to monitor and improve information security.

C. Planned actions/events (long-term): Same as item B.

Enclosure D

SECURITIES AND EXCHANGE COMMISSION
MATERIAL NON-CONFORMANCE/CORRECTIVE ACTION

1. Entity, Filing and Fee System (EFFF)

Bureau/Appropriation/Account Number: Office of Filings and Information Services

Administrative Activity/Program Activity: Track the receipt and allocation of filing fee and account data.

Pace of Corrective Action:

Year Identified: 1993

Original Targeted Corrective Action Date: 1994

Targeted Corrective Date in Last Year's Report: 2000

Current Target Correction Date: 2001

Reason for Change in Date(s): Not Applicable. Corrective actions were completed in 2001.

Description and Agency Impact: The SEC needs to track the receipt and allocation of filing fee and related account data and provide a consolidated source for on-line inquiry, on a real-time basis, of specific filing fee information. A new agency on-line system was implemented in late fiscal 1992. However, since implementation several problems have been identified that inhibit the agency from maintaining real-time, accurate data. The current system does not fully meet the requirements of the agency or the requirements outlined in OMB Circular A-127 (including the internal control standards as defined in OMB Circular A-123) for financial management systems.

The following are specific identified deficiencies:

Internal Controls. Internal control deficiencies include (1) an unreliable electronic link with Mellon Bank which is used to transmit data on fees deposited for SEC at Mellon; (2) interface problems with the agency's EDGAR system; (3) difficulty in linking fees and filings; (4) limited data validation; (5) inadequate separation of duties; (6) insufficient audit trails; and (7) a lack of access level security.

Documentation. The EFFF system does not have sufficient current documentation describing functional requirements, system specifications, data and transaction requirements, and user and training materials.

Enclosure D

Page 2

Maintenance. The current EDFS system is difficult to maintain due primarily to its structure and reliance on a few key individuals.

Source of Discovery of Non-conformance: The non-conformance was identified in early fiscal 1993 by the system manager and the Comptroller of the agency. Subsequently, two SEC task forces and an audit conducted by the Office of the Inspector General from January 1995 through October 1995 identified additional deficiencies.

Critical Milestones in Corrective Action:

| <u>Critical Milestone</u> | <u>Original Plan</u> | <u>Current Plan</u> | <u>Actual</u> |
|--|----------------------|---------------------|-------------------|
| Establish Task Force to Identify and Resolve System Problems | 12/92 | N/A | 12/92 |
| Identify and Resolve Critical Problems | 9/93 | N/A | 9/94 |
| Implement Programming Changes | 9/93 | N/A | 8/95 |
| Establish Second Task Force | 11/94 | N/A | 11/94 |
| Implement New Processing Procedures and Access Codes | | | 2/96 |
| Correct Audit Trail Weaknesses | | | 2/96 ¹ |
| Prepare Formal, Written Procedures | | | 2/96 |
| Requirements for Redesign | 2/95 | N/A | 4/96 |
| Completion of Redesign and Implementation of New System | 12/97 | 2001 | 9/01 |

A. Completed actions/events: A task force was established by the Executive Director of the agency to identify and resolve system problems that inhibit agency needs and compromise compliance with OMB Circular A-127 requirements. Several critical problems were identified and resolved and some system changes were implemented. Due to the unusual complexity of the

¹Audit trail weaknesses were corrected in February 1996, with the exception of system changes to accommodate a "reason" code.

Enclosure D

Page 3

problems identified by this task force, a second task force was assembled. This task force was able to improve significantly several features of the system and the reliability of EFFF financial data. These improvements enabled the agency to send account statements to over 17,500 filers and registrants. However, the task force and an audit conducted by the Office of the Inspector General identified insufficient internal controls (*i.e.*, separation of duties, access levels, and audit trails), lack of documentation, and difficulties in maintaining the system such that a determination was made to redesign the system and to delay full implementation of some corrective actions until EFFF is redesigned. The EFFF re-write requirements were included in the modernization initiative for the Commission's EDGAR system. A three-year contract for the modernization of EDGAR was awarded in July 1998. The EFFF replacement was implemented in September 2001. The design of the new system contains adequate financial controls.

B. Planned actions/events (short-term, *i.e.*, next 12 months): The SEC will be generating Account Activity Statements from the new system by the end of February 2002. This will allow each filer to verify the accuracy of their account information at the SEC.

C. Planned actions/events (long-term, *i.e.*, long-term): We will monitor the new system to ensure that it tracks the receipt and allocation of filing fee and related account data accurately and provides a consolidated source for on-line information.