

Securities and Exchange Commission

Office of Inspector General

Executive Summary

During this reporting period (October 1, 2000 to March 31, 2001) the Office of Inspector General (Office) issued seven audit reports, one investigative memorandum on management issues, and one audit memorandum. These documents focused on disgorgements; the Commission's Integrity Programs; the Freedom of Information Act (FOIA) process; general computer controls; the distribution of mail; administrative practices in the Central Regional Office; the use of personal resources; and print shop supplies. The Audit Program section below describes this work further.

Twelve investigations were closed during the period. Three subjects were referred to the Commission; one case was referred to the Department of Justice. During the period, two subjects referred during a prior period resigned. Eight subjects, referred to Commission management during this and prior periods, are awaiting disposition. The Investigation Program section below describes the significant cases further.

In this period, we are reporting controls over disgorgement¹ waivers as a significant problem, based on our audit. During the audit, the Division of Enforcement began taking actions to improve the waiver process. It has issued written procedures, hired a firm to provide improved databases, and hired a contractor to evaluate and make recommendations concerning its procedures. We commend the Division on taking prompt action to strengthen the controls.

In a previous period, we also reported the custody of sensitive information as a significant problem. Since then management has established a task force to implement corrective actions, issued an agency-wide policy, and hired a consultant to assist in a comprehensive review of the matter. The Commission recently received the consultant's final report and recommendations. The task force has identified the most significant recommendations, and the Commission has begun implementing them. We recently began a follow-up audit on the controls over sensitive information

¹ Disgorgements represent ill-gotten gains (or losses avoided) resulting from individuals violating the federal securities laws. The Commission seeks disgorgement to ensure that securities law violators do not profit from their illegal activity. When appropriate, the disgorged funds are returned to the injured investors.

We also previously identified information resources management as a significant problem. Although the Commission has taken many positive steps to improve the management of information (e.g., integrating information technology planning, budgeting, and performance measurement process, linking plans and budgets to the Commission's mission and strategic direction) information resources management, as a whole, remains a significant concern.

We believe that the Commission is making progress in the right direction (i.e., full compliance with requirements of the Clinger-Cohen Act). However, many pending management actions need to be completed to implement the operational, procedural, and policy recommendations made in prior audits. We performed a review of general computer controls and a risk assessment of information technology this period. We intend to maintain our oversight of the Commission's management of information resources (including performing a business process review of the IT capital investment decision-making process).

Another previously reported significant problem involves lack of adequate controls over the collection of fees. Since first reported, statutory changes have eliminated many of the fees most at risk. Moreover, Commission management has made significant progress in correcting the most serious weaknesses. However, final corrective actions are awaiting the implementation of a new computerized filing fee collection system.

No management decisions were revised during the period. The Office of Inspector General agrees with all significant management decisions regarding audit recommendations.

Audit Program

The Office issued seven audit reports, one investigative memorandum on management issues, and one audit memorandum during the reporting period. These documents contained a total of 74 recommendations, which are further described below. Management concurred with most of the recommendations.

DISGORGEMENTS (AUDIT 311)

Disgorgements represent ill-gotten gains (or losses avoided) resulting from individuals violating the federal securities laws. The Commission seeks disgorgement to ensure that securities law violators do not profit from their illegal activity. When appropriate, the disgorged funds are returned to the injured investors.

Disgorgements can be ordered in either administrative proceedings or civil actions, and the cases can be settled or litigated. Payment of disgorgements can be either completely or partially waived based on the defendant demonstrating an inability to pay.

In settled administrative proceedings, Enforcement may recommend, if appropriate, that the disgorgement be waived. The Commission makes the final decision. In civil actions, any settlement agreed to by the Commission must be approved by the district court.

Our audit objectives were to determine if the management controls over waivers of disgorgements and identification of investors in disgorgement plans were effective in achieving their objectives and efficient. In addition, we determined compliance with Commission Rule 201.612(c) governing whether disgorgements are paid to the injured investors or the U.S. Treasury.

We found that improvements could be made to the waiver process to achieve greater assurance that waivers were justified. The Division of Enforcement concurred and, during the audit, began taking actions with a view to improving the waiver process. It has issued written procedures relating to the waiver process, hired a firm to provide improved databases, and hired a contractor to help evaluate and make recommendations concerning its procedures.

INTEGRITY PROGRAMS (AUDIT NO. 313)

We evaluated the effectiveness of the Commission's integrity programs (*i.e.*, the ethics program in the Office of General Counsel and Personnel's staff conduct program). The review was a follow-up to two audits performed in 1996-97 (Audit Nos. 250 and 267).

Successes, obstacles, recommendations, and effectiveness ratings related to the Commission's integrity objectives were obtained through twenty-two workshops involving approximately eight per cent of Commission employees. Composite ratings were consistent with the previous audit results. Indications are that all supporting objectives are generally being implemented. We believe that, taken as a whole, the Commission is achieving its primary objective to promote high individual and agency integrity.

With almost no exceptions, the workshop participants indicated that they felt a personal sense of responsibility for maintaining the integrity of the Commission. There were no material control weaknesses identified during the workshops. It is evident from all available evidence that Commission employees place a high premium on ethical integrity.

The participants in the workshops made a number of comments and suggestions for improvement. We shared many of them with management. We made two audit recommendations to improve staff access to integrity guidance and to notify staff seeking ethics counseling of confidentiality limitations.

FOIA PROCESS (AUDIT 318)

The Freedom of Information and Privacy Act Branch, in the Office of Filings and Information Services (Branch), processes Freedom of Information Act (FOIA) requests for agency records. The Branch includes approximately eighteen staff. It received 2,985 requests in FY 1999.

The audit objective was to evaluate the Commission's compliance with the Freedom of Information Act in processing requests and determine whether processing improvements were needed. We did not address the Privacy Act during this audit.

The Freedom of Information Act requests that we reviewed appeared to be processed generally in compliance with the FOIA.

In FY 2000, the Branch continued its efforts to acquire a new tracking system for FOIA requests, completed a new training manual for its staff, updated the Commission's FOIA regulations, and conducted a conference for Headquarters and field office FOIA liaisons.

Also, the Branch addressed several matters that we noted during the audit. We found that staff passwords for the FOIA tracking system were provided in the users' guide, a risk to the security of the tracking system. The FOIA/PA Officer promptly had the passwords changed. Also, the Officer coordinated with the Commission's Webmaster to add a link on the Commission's home web page to its FOIA web page. In addition, the Officer requested the capability to run ad hoc reports from the current FOIA tracking system. These actions demonstrate the Branch's commitment to enhancing its operations.

To further enhance FOIA request processing, we recommended that the Branch: notify requesters of their appeal rights in responses indicating that no records were found; always notify requesters when their requests will take longer than 20 business days to process; clarify language in response letters; require fee agreement in initial FOIA requests; improve documentation of searches and fees assessed; link information to the FOIA web page; and improve maintenance of the FOIA request files.

GENERAL COMPUTER CONTROLS (AUDIT 320)

The Office of Inspector General sought to determine whether the general controls over the information systems of the Commission's Office of Information Technology (OIT) were effective. The OIG contracted with Tichenor & Associates, an independent CPA firm, to perform a review of the general controls over information technology (IT) planning and organization, data processing operations, physical and logical access to IT assets, program change controls, and other data processing related activities.

The review disclosed that the general controls over information systems were generally effective due to the Year 2000 (Y2K) moratorium on changes to the production environment and the comprehensive review and clean up of information systems and technology associated with Y2K compliance and certification efforts. However, while OIT has devoted much effort to improving and aligning agency and information technology plans, re-structuring the OIT, improving staff core competencies, and developing a comprehensive configuration management infrastructure, significant improvements must be made for SEC to continue to rely on the general controls over information systems. Specifically, improvements are needed in the areas of:

- Policies and procedures related to approval and implementation of configuration change control;
- Policies and procedures related to OIT oversight of project deliverables;
- Segregation of duties between the systems software, configuration management, user access administration, and production control functions;
- Security planning for controlling and administering user access to applications; and
- Performance, problem and compliance reporting.

The report made recommendations to improve these areas. It found that OIT management was aware of many of these conditions and had already implemented improvements in some areas. However, OIT management acknowledged that they are still working on the evolving configuration control structure and the required supporting policies, procedures and automated tools.

DISTRIBUTION OF MAIL (AUDIT 324)

The General Services Administration (GSA) issued guidance to agencies on Federal Mail Management (41 Code of Federal Regulations, 101-9). The guidance requires the agency head to designate a mail manager.

Commission mail policies and procedures are described in the Mail Management regulation (SECR 22-1). The Branch Chief of Publishing in the Office of Administrative and Personnel Management is the Commission's mail manager. Approximately 15 staff and a supervisor handle day-to-day distribution of mail in headquarters.

Our review of the distribution of mail found that it generally complied with applicable guidance and was cost effective. We made several recommendations to enhance mail management, including: considering additional automation; promoting efficient use of express mail methods; issuing updated mail guidance; establishing a mail site on the Intranet; and providing additional information to mail room staff.

GENERAL COMPUTER CONTROLS - REGIONS (AUDIT 327)

The OIG contracted with Tichenor & Associates, an independent CPA firm, to perform a review of the general controls over data processing in the regions. The objective of the review was to determine whether the controls are in place and effective, and can be relied upon by the OIG in assessing the validity and reliability of data from SEC computer-based systems. The scope of the review included both mainframe and server general controls.

Based on the review, Tichenor determined that the Office of Information Technology (OIT) has devoted much effort to improving and aligning SEC information technology plans. However, it

identified further improvements, which must be made for the Commission to continue to rely on the general controls. Specifically, improvements are needed in the areas of:

- Implementing technology with proper testing and approval;
- Communication between the OIT Technical Liaison and regional management on information technology plans and issues;
- Development of regional IT-related procedures and automated processes;
- Increased reliance on the Help Desk for problem resolution by the regions; and
- Storage and retrieval of data stored on workstations.

OIT management was aware of many of these conditions and has already implemented improvements in some areas.

CENTRAL REGIONAL OFFICE (AUDIT NO. 328)

The Central Regional Office exercises a broad range of financial and administrative functions, including maintaining time and attendance records; procuring supplies and services; arranging for staff travel; maintaining an inventory of property; and recording budgeted and actual expenditures of the office.

The Office of Inspector General conducted a limited audit of the financial and administrative internal controls of the office. The purpose of the audit was to provide the Commission with negative assurance that the internal controls were adequate, being implemented economically and efficiently, and in compliance with Commission policies and procedures. The audit procedures were limited to analyzing representations made by staff, reviewing supporting documentation, and conducting some tests of transactions.

During the limited audit described above, no material weaknesses in the internal control structure involving financial and administrative functions came to our attention. Some minor problems were verbally discussed with management. The office concurred with these findings and is implementing our suggestions.

USE OF PERSONAL RESOURCES (INVESTIGATIVE MEMORANDUM ON MANAGEMENT ISSUES G317)

A recent investigation in a district office disclosed that a manager in the office used personal resources for Commission business, including office furniture and equipment; computer consulting services performed in the office; and training for office staff.

The manager also connected his personally owned computer to the Commission's network, and used an office analog line to access his personal Internet account. When we informed the Associate Executive Director of the Office of Information Technology (OIT), he ordered that the

manager's computer be disconnected from the network because it represented a potential security threat.

We recommended that the Office of General Counsel (OGC) consult with other relevant offices to determine whether the manager's actions constituted an improper augmentation of appropriated funds, and to decide on the appropriate disposition of the personal property in the district office.

Based on OGC's consultations and its own analysis, OGC determined that no improper augmentation of appropriated funds occurred. However, it indicated (1) that the manager should acknowledge in writing that the loaned furniture, equipment, and other services procured with his own funds were rendered gratuitously with no expectation of reimbursement, and (2) the personal property at issue should be removed prior to, or at the time of, the departure of the manager from the Commission.

We also recommended that OIT, in consultation with the Office of Administrative and Personnel Management, issue additional guidance to Commission employees on the use of personal resources (including computers and Internet Service Provider accounts) in combination with Commission computer and telecommunication resources. The guidance should cover security considerations, describe if and when such combinations are allowed, and set forth approval procedures.

PRINT SHOP SUPPLIES (AUDIT MEMORANDUM M21)

The print shop orders supplies quarterly after receiving a budget allocation. Supplies are kept in the print shop and in a caged storage area of the parking garage (OAPM plans to install a security camera for this caged area).

This memorandum made recommendations to improve controls over print shop supplies, based on a recent incident there. A print shop manager noticed that over half of the toner for the color copier was missing from the print shop supply room. He estimated its value between \$7,000 and \$10,000 on the incident report. In addition, several other items were missing.

We recommended that the Office of Administrative and Personnel Management periodically change the combination lock on the supply room door, and provide the combination only to selected employees. We also recommended that OAPM maintain perpetual inventory records of toner for the color copier, and periodically compare these records to toner on hand to identify and resolve discrepancies.

Investigative Program

Twelve investigations were closed during the period. Three subjects were referred to the Commission; one case was referred to the Department of Justice. During the period, two

subjects referred during a prior period resigned. Eight subjects, referred to Commission management during this and prior periods, are awaiting disposition. The most significant cases closed during the period are described below.

UNAUTHORIZED DISCLOSURE OF NONPUBLIC INFORMATION

The Office investigated an allegation that a Commission employee may have leaked nonpublic information concerning an ongoing investigation to a member of the press. The evidence obtained during our investigation failed to substantiate the allegation. We interviewed numerous staff members who had access to the nonpublic information. All denied making any unauthorized disclosures of that information. We also learned that the reporter in question had stated that the source of the information was not a Commission employee.

POST-EMPLOYMENT VIOLATION

The Office developed evidence that a former Commission staff member may have violated a federal conflict of interest statute by working for a special master in a matter the employee had worked on while employed by the Commission. We also obtained evidence that the staff member had continued to work on the matter while still employed by the Commission after accepting an offer of employment with the special master. The Department of Justice declined prosecution.

Significant Problems

DISGORGEMENTS

In this reporting period, we completed an audit of disgorgements (Audit No. 311, described above). We found that improvements could be made to the waiver process to achieve greater assurance that waivers were justified.

The Division of Enforcement concurred and, during the audit, began taking actions to improve the waiver process. It has issued written procedures relating to the waiver process, hired a firm to provide improved databases, and hired a contractor to help evaluate and make recommendations concerning its procedures. We commend the Division on taking prompt action to strengthen the controls.

We intend to monitor the Division's actions to improve the waiver process.

Significant Problems Identified Previously

SENSITIVE INFORMATION

In a previous period, we reported the custody of sensitive information as a significant problem. Since then, management established a task force to implement corrective actions, issued agency-wide policy, and hired a security consultant to assist in a more comprehensive review of overall security.

The Commission has received the consultant's final report and recommendations. The task force has identified the most significant recommendations, and the Commission has begun implementing them. We recently began a follow-up audit on certain controls over sensitive information.

INFORMATION RESOURCES MANAGEMENT

We previously identified information resources management as a significant problem based on prior audits, investigative work, and management studies that identified significant weaknesses in many aspects of the Commission's management of information resources. Since then, the Commission has taken many positive steps to improve the management of information resources throughout the Commission.

Although the Commission has made significant progress in complying with requirements of the Clinger-Cohen Act, many pending audit recommendations need to be implemented. During this period, we completed reviews of the Commission's general computer controls (see above), and conducted a risk assessment of information resources management. We also initiated a business process review of the IT capital investment decision-making process.

In future periods, we intend to maintain our oversight of the Commission's management of information resources.

COLLECTION OF FILING FEES

Starting in 1996, we have identified the Commission's collection of filing fees as a significant problem. Since then statutory changes have eliminated many of the fees most at risk. Moreover, Commission management has made significant progress in correcting the most serious weaknesses. However, final corrective actions are awaiting the implementation of a new computerized filing fee collection system.

The strengthening of automated controls, related to filing fee collection, has been awaiting modernization of the EDGAR system (which receives and disseminates filings from public

companies). EDGAR Release 7.5, scheduled for May 2001, and EDGAR Release 8.0, scheduled by the end of the fiscal year, are planned to implement a new filing fee collection system. The new system is designed to contain adequate financial controls. Until then, the overall control structure continues to fail to provide adequate accountability over filing fees.

Access to Information

The Office of Inspector General has received access to all information required to carry out its activities. No reports to the Chairman, concerning refusal of such information, were made during the period.

Other Matters

EXECUTIVE COUNCIL ON INTEGRITY AND EFFICIENCY

The Office actively participates in the activities of the Executive Council on Integrity and Efficiency (ECIE). The Inspector General attends ECIE meetings, is an active member of its Financial Institutions Regulatory Committee, and serves as the ECIE member of the Integrity Committee established by Executive Order No. 12993.

The Counsel to the Inspector General is an active member of the PCIE Council of Counsels. The Council considers legal issues relevant to the Inspector General community.

Questioned Costs

		DOLLAR VALUE (IN THOUSANDS)		
	NUMBER	UNSUPPORTED COSTS	QUESTIONED COSTS	
A	For which no management decision has been made by the commencement of the reporting period	0	0	0
B	<i>Which were issued during the reporting period</i>	<u>0</u>	<u>0</u>	<u>0</u>
	Subtotals (A+B)	0	0	0
C	For which a management decision was made during the reporting period	0	0	0
(i)	Dollar value of disallowed costs	0	0	0
(ii)	Dollar value of costs not disallowed	0	0	0
D	For which no management decision has been made by the end of the period	0	0	0
	Reports for which no management decision was made within six months of issuance	0	0	0

Recommendations That Funds Be Put To Better Use

		<u>NUMBER</u>	<u>DOLLAR VALUE (IN THOUSANDS)</u>
A	For which no management decision has been made by the commencement of the reporting period	0	0
B	Which were issued during the reporting period	<u>0</u>	<u>0</u>
	Subtotals (A+B)	0	0
C	For which a management decision was made during the period	0	0
(i)	Dollar value of recommendations that were agreed to by management	0	0
-	Based on proposed management action	0	0
-	Based on proposed legislative action	0	0
(ii)	Dollar value of recommendations that were not agreed to by management	0	0
D	For which no management decision has been made by the end of the reporting period	0	0
	Reports for which no management decision was made within six months of issuance	0	0

Reports with No Management Decisions

Management decisions have been made on all audit reports issued before the beginning of this reporting period (October 1, 2000).

Revised Management Decisions

No management decisions were revised during the period.

Agreement with Significant Management Decisions

The Office of Inspector General agrees with all significant management decisions regarding audit recommendations.