EXECUTIVE SUMMARY

The Securities and Exchange Commission (SEC), Office of Inspector General (OIG) sought to determine whether the SEC's current data back-up procedures were reasonably effective in insuring that back-up data was available and complete in the event a contingency occurred requiring the restoration of back-up data. The OIG tasked Tichenor & Associates to evaluate the effectiveness of back-up procedures to minimize loss for data residing on Securities and Exchange Commission mainframe and network computer systems.

We found that back-up activities were reasonably effective to minimize data loss but that improvements were needed in the areas of:

- Written policies and procedures for back-up activities,
- Training of back-up operators and their alternates,
- Disaster recovery and contingency planning, and
- Security awareness training.

SEC, and its office responsible for data back-up procedures, the Office of Information and Technology (OIT), were aware of the need for improvements. In fact, some of these areas were highlighted in the 1996 through 1998 reports issued by SEC under the Federal Managers' Financial Integrity Act (FMFIA) and OIT had taken some actions, especially in the area of security. However, these actions were limited, and had not yet been implemented by the personnel responsible for back-up procedures at the SEC regional and district offices.

Our findings and recommendations are included in the Findings section of this report.

BACKGROUND

The United States Securities and Exchange Commission (SEC), created under the Securities and Exchange Act of 1934, is an independent, nonpartisan, quasi-judicial, regulatory agency. Its mandate is to administer and enforce the federal securities laws in order to protect investors, maintain fair, honest, efficient markets, and facilitate capital formation. The SEC is composed of five members appointed by the President, with the advice and consent of the United States Senate, for five-year terms.

The Office of Information Technology (OIT), headed by the Chief Information Officer, oversees all data management systems for the SEC, participates in the investment review process for information systems, and monitors and evaluates the performance of those information systems. As part of its handling of data management systems, OIT is responsible for the integrity of the SEC data back-up systems.

The data managed by OIT for the SEC is maintained using two database management systems products. One product, ADABAS, is used to support SEC applications operating on an IBM mainframe. The other product, Sybase, is used to support applications developed and maintained by OIT in a client-server environment. Sybase is also the database management system supporting the Electronic Data Gathering, Analysis, and Retrieval (EDGAR). This system is used by SEC to collect and maintain information from corporate filings to the SEC and is currently administered by a contractor on-site at the SEC Operations Center in Alexandria, Virginia. The mainframe operating IBM's OS-/390, while the network uses operating systems such as: Novell and, Windows NT.

OIT is responsible for data back-up of the mainframe and other SEC headquarters systems. The SEC field offices are responsible for the back up of their own network data. OIT uses tape silos for backing up mainframe data (from an IBM 2003-126 at the Operations Center and an IBM 2003-215 at Headquarters) and individual tape drives network data. For the Internet web site and its Sybase data management system (DBMS), the SEC uses Sun Microsystems tape back-up systems. The EDGAR contractor is responsible for tape back-up of the EDGAR Stratus computers.

To provide back-up capability, OIT relies on several software products such as FDR/Upstream, and ArcServ. FDR/Upstream is used for both mainframe back-ups; ArcServ is used for the network. The tape back-ups for the mainframe and main servers housed in OIT and Headquarters are transported and stored off-site by an OIT contractor.

The Computer Security Act of 1987 emphasizes that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and creates a means for establishing minimum acceptable security practices for such systems. OMB Circular A-130, dated February 8, 1996, calls for increased protection for Federal computers by all Executive departments and agencies. Specifically, it requires each department and agency to:

- Establish a management process to assure that appropriate safeguards are built into all new computer applications;
- Assign responsibility for security of each new installation to a management official;
- Establish personnel security policies for both Federal and contractor personnel;
- Conduct periodic audits of all sensitive computer applications;
- Include security requirements in specifications for the acquisition or operation of computer facilities or related services;
- Conduct periodic risk analysis of each computer installation; and,
- Assure that appropriate contingency plans are developed to reduce the effect of computer breakdowns, fires, or natural disasters.

Presidential Executive Order 130.11 of July 17, 1996, assigns the responsibility for these functions to the Agency's Chief Information Officer (CIO). The CIO is to have the visibility and management responsibilities necessary to advise the agency head on the design, development and implementation of those information systems.

SCOPE AND METHODOLOGY

The SEC Office of Inspector General tasked Tichenor & Associates to evaluate the effectiveness of back-up procedures to minimize loss for data residing on SEC mainframe and network systems in the event of a contingency. We reviewed pertinent files and policy documents, observed relevant processes, tested back-up file restoration, and interviewed key OIT personnel. We also review pertinent laws, regulations, and Office of Management and Budget Circulars. With regard to the EDGAR system (operated by a contractor), we limited our work to assessing the adequacy of SEC back-up policies and procedures, the adequacy of contractor back-up policies and procedures, and evaluating the results of contractor back-up testing results. The audit was performed at the SEC Headquarters Office in Washington D.C., the SEC Operations Center in Alexandria, Virginia, and the SEC Regional and District Offices in Atlanta, Boston, Chicago, Denver, Fort Worth, Los Angeles, Miami, New York, Philadelphia, Salt Lake City, and San Francisco.

Specifically, our audit objectives were to evaluate the adequacy of SEC controls over:

- Back-up and storage of programs and data files,
- Training of back-up operators,
- Disaster recovery and contingency planning, and
- Security awareness training.

Our audit was conducted in accordance with Government Auditing Standards. We also used the COBIT (Control Objectives for Information and Related Technology) Audit Guidelines and the Computerized Information Audit Manual established by the Information Systems Audit and Control Foundation. As necessary, we also used applicable industry standards defining best practices for data and record management, server administration, and electronic data processing operations.

Our audit fieldwork was conducted between January and September 1999.

We found that back-up activities were reasonably effective to minimize data loss. Overall personnel responsible for back-up activities were aware of their roles and responsibilities, physical security was good, and our testing of back-up files showed no instances when files could not be recovered. However, we found that improvements were needed because the back-up activities existed with little or no guidance from OIT, or if guidance was available, personnel were not aware of it. Instead, back-up personnel relied on their experience and knowledge of industry practices. While reliance on knowledge and experience are critical, they are no substitute for agency-wide written policies and procedures, training, contingency planning, and security awareness. Specifically, OIT needs to:

- Provide written policies and procedures for back-up activities,
- Train back-up operators and their alternates,
- Implement disaster recovery and contingency plans, and,
- Implement security awareness training.

Our visits to OIT and the SEC Regional and District Offices showed that lack of guidance caused procedures to vary from office to office as shown in the following matrix:

OIT and Regional and District Offices	NY	Bos	Phil	Mia	Atl	Chi	Den	FW	SL	LA	SF	OIT
No SEC approved written policies and procedures were available on site	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Servers were not secured or door to computer room were left unlocked			**X**				**X**					
Computer room had no temperature regulating devices or fire suppression equipment	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	
Back-up personnel did not fully understand back-up and storage software and hardware	**X**						**X**		**X**	**X**	**X**	
Back-up and storage personnel primary job function was not Information Technology							**X**		**X**		**X**	
Personnel did not have adequate training on back-up and storage software/hardware	**X**	**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**	**X**	
Alternate operators did not have adequate skills/knowledge to handle back-up and storage		**X**	**X**	**X**	**X**		**X**	**X**	**X**			
No SEC approved disaster and contingency plans were available on site	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
No security awareness training was made available to personnel on site	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Personnel took data tapes home over the weekend as "safety measure"		**X**	**X**	**X**	**X**							

SEC was aware of some of these problems and had reported on them in its FMFIA reports in 1996 through 1998. For example, SEC reported in 1996, that it lacked a long-term disaster recovery plan to maintain the continuity of the EDGAR systems, and showed that corrective action was being taken. In 1996 through 1998, SEC reported that ADP security controls should

be enhanced, strengthened, and communicated to all staff and indicated corrective action was being taken. However, we found no evidence that these corrective actions had been implemented by the SEC Regional and District Offices.

Finding 1: Provide Policies and Procedures for Back-Up Activities

OMB Circular A-130 requires Federal agencies to document all policies and procedures relating to the functions of computerized activities. This circular requires that such policies and procedures be applied agency-wide, on a consistent basis. SEC did not have current written policies and procedures in place to govern and monitor such critical areas as (1) data back-up procedures, (2) storage of data, and (3) security. As a result, personnel responsible for these areas at the Regional and District SEC offices had to rely on their own judgement and experience to ensure adequate back-up. We recognize that reliance on judgement and experience are an integral part of a system of management. However, written agency-wide policies and procedures are needed to ensure consistent and complete application.

SEC has been aware of these problems for several years and had taken limited steps to correct them. In December 1998, OIT had initiated a document that provided general policy guidance and program requirements for Information Technology (IT) security. This document was the first step of a program designed to establish uniform policies to carry out the SEC's Information Technology Security Program. The program was to document and implement security standards, educate users, technical staff, and system owners, and conduct system certification and accreditation activities. In September 1999, OIT also drafted procedures for performing weekly tape back-ups.

Presidential Executive Order 130.11 of July 17, 1996, assigns the responsibility of all IT functions to the Agency's Chief Information Officer (CIO). The order provides the CIO with the authority and management responsibilities necessary to advise the agency head on the design, development and implementation of those information systems. At SEC, the Associate Executive Director of Information Technology has been designated the Commission's CIO. The CIO is responsible to the Executive Director, Chairman and the Commission for the internal technological management functions of the Commission.

To ascertain that data was backed up and could be retrieved, we tested back-up and storage data, at each of the SEC Regional and District Offices. We selected a back-up tape picked at random from storage. We observed the progress of the restoration of this tape from the ArcServ job manager screen and when completed, launched the file to verify its readability. At all of the offices, the reliability and accuracy of the tape identification, the data stored on the tape, and the prescribed procedures appeared adequate as a result of this test.

While this type of test offers some assurance that data can be restored, it does not provide assurance that such restoration would occur in a contingency situation. To obtain such assurance, a test of the system under a contingency would have to be conducted. SEC had not issued guidance to the regional and district offices on what type of test should be conducted and how frequently.

With regard to physical security, at the Regional and District Offices, there were no temperature regulating devices, or fire suppression equipment to protect the "computer room". Also, 2 of 11 offices did not have servers secured or did not always keep the doors to the server rooms locked.

RECOMMENDATIONS

We recommend that SEC:

A. Design and implement policies and procedures that provide back-up operators and their alternates with operating guidance.
B. Design and implement policies and procedures to control physical security.

MANAGEMENT'S COMMENT

Management believes appropriate polices and procedures exist to provide operating guidance to personnel responsible for data back up activities. More precisely, three contractors are responsible for conducting the majority of the agency's data back-up and that each of these contractors have extensive and well documented standard operating procedures and conduct regularly scheduled data back-up and recover activities. The effectiveness of these programs is evidenced by the audit results showing no instances when files could not be recovered.

In September 1998, the SEC issued an Information Technology Security Policy covering responsibilities for protecting agency systems and data. Concurrently, OIT issued a series of technical bulletins identifying specific guidance on standards and implementation practices in support of the policy. This information was published on the SEC's intranet, made available to contractors and COTRs, and incorporated in a variety of training programs.

During 1999, system administration practices were covered with the ADP liaisons as part of the agency's NT operating system upgrade. In September 1999, a full day of training was provided to ADP liaisons on troubleshooting and system administration practices as part of the annual ADP liaison conference. During the last half of calendar 1999 ADP liaisons and contractor staff were all involved in contingency planning and disaster recovery activities as part of the SEC's Year 2000 program.

Physical security for controlling access and protecting equipment is addressed in the agency's security policy and related technical bulletins. However, modifications to buildings were SEC equipment is located must be requested through the agency's Office of Personnel and Administrative Management.

AUDITOR'S RESPONSE

We do not agree with management's response related to Finding 1 and do not think that appropriate policies and procedures existed or were adequately disseminated to provide operating guidance to personnel responsible for data back-up activities at the close of fieldwork.

We met with all three contractors and confirmed that all three had consistent practices in place and that the contractors were conducting regularly scheduled data back-up and recovery activities. However, except for the EDGAR contractors, approved procedures did not exist. More precisely, the contractors for the mainframe provided us with a User Guide that showed how to program the backup, but stated that they did not have actual approved policies and we were directed to an outdated policy on the intranet. Additionally, the contractor for the LAN/WAN servers had ad-hoc procedures written up by the contractor for their personal files, but no authorized written policy existed. Again we were directed to outdated policies on the Intranet. Only the EDGAR contractors had extensive documentation showing policy and procedures as well as evidence of each backup and supervisory review, and the EDGAR contract had a specific contract requirement that they develop and maintain adequate policies and procedures. The other contractors answer directly to the OIT Operations staff on a daily basis and are bound by the OIT policies and procedures.

We agree that in September 1998, the SEC issued an Information Technology Security Policy covering responsibilities for protecting agency systems and data. However, the "Security Policy" initially only established the office of Security Officer. During our audit the Security Officer published a security policy outline on the intranet. Portions of the outline were completed during our audit. However none of the completed topics covered data back-up and recovery procedures. Furthermore, during our site visits field personnel didn't have (or know where to find) guidance related to policies on data backup procedures. In addition, the portion of the policy related to physical security for controlling access and protecting equipment at the district and regional offices had not been updated at the close of fieldwork. In addition, regional and district office personnel had not received and did not know of any security awareness training that was available to them

The annual conference held in September 1999 with ADP liaison, subsequent to fieldwork, covered the administration practices related the agency's migration to the NT operating system. However, we did not find evidence supporting that the ADP liaisons received any other guidance during the year covering data back-up policies and procedures. Additionally, during the last half of calendar 1999, the staff involvement with contingency planning and disaster recovery activity was limited to headquarters and did not include the regional contingency and disaster recovery plans.

Finding 2: Train Back-Up Operators and their Alternates

OMB Circular A-130 requires regular training to maintain adequate personnel competence and skill level in the management of information. We found that SEC had not provided training specifically related to carrying out data back-up and related storage activities to operators primarily responsible for these activities or to alternate operators (personnel designated to carry out back-up and storage activities in case primary operators are not available). As a result, primary operators had varying degrees of knowledge about back-up procedures, and alternates operators often had only rudimentary skills.

Our discussions disclosed that whereas some primary operators appeared well capable of handling back-up and storage activities, most alternate operators could only carry out only minimal tasks. Therefore, alternate operators were not trained to respond to emergencies.

In the absence of regular training, we did find that some operators had ordered manuals from manufacturers and exchanged information with other operators within the SEC in order to maintain competence and skills. We also noted that, September 21, 1999, OIT was holding a training session on Troubleshooting Windows NT (an upgrade of a current system) for ADP Liaison personnel (primary operators and alternate back-up and storage personnel), and was making training information available on a Web site. These steps, if incorporated as part of a required formal training program directed at primary operators and alternates, would greatly contribute toward better training.

RECOMMENDATION

We recommend that SEC:

A. Establish a formal training program for primary operators and alternates responsible for data back-up and storage activities.

MANAGEMENT'S COMMENT

Management believes that the contractors' personnel are adequately trained to conduct data back-up and recovery responsibilities to meet their contractual obligations, but agree that more vigorous training could be provided to ADP liaisons and their alternates to enhance their understanding of data back-up and recovery practices. OIT is working with the Office of the Executive Director on approaches to providing more formal and regularly scheduled training.

AUDITOR'S RESPONSE

Although Management's response does not specifically address Finding 2 recommendation A, management does agree that more vigorous training could be provided to ADP liaisons and their alternates to enhance their understanding of data back-up and recovery practices. We agree with management's response that working with the Office of the Executive Director on approaches to providing more formal and regularly scheduled training for these personnel is the first step in establishing a formal training program for primary operators and alternates responsible for data back-up and storage activities.

Finding 3: Implement Disaster and Contingency Plans

OMB Circular A-130 requires that Executive departments and agencies assure that appropriate disaster recovery and contingency plans are developed to reduce the effect of computer breakdowns, fires, or natural disasters. We found that SEC had not developed or implemented disaster recovery and contingency plans to handle back-up activities in the event of loss or interruption of the computer systems. As a result, SEC personnel had no written guidance as to what action it would have to take in such key areas as (1) off-site processing during power failures or other crisis, (2) notification of personnel in case of emergency, and (3) priorities as to what critical data should be recovered. The lack of a disaster recovery and contingency plans had been reported by the SEC since 1996 in its annual FMFIA reports and SEC had recognized that the lack of such plans had the potential to impair the mission of the agency.

SEC field personnel expressed concern over the lack of guidance in case of emergency. For example, most ADP Liaisons indicated that they had some sense of what was the most critical data to be recovered, and they recognized the value of a formal plan to prioritize data in the event recovery was necessary, based on criticality to the organization.

RECOMMENDATION

We recommend SEC:

A. Develop and implement a disaster and contingency plan.

MANAGEMENT'S COMMENT

Management agrees with the finding and recommendation.

Finding 4: Implement Security Awareness Training

The Computer Security Act of 1987 and OMB Circular A-130 emphasize the criticality of security for Federal computer systems. Since 1996, SEC had been reporting under FMFIA about the need for the agency to enhance, strengthen, and communicate ADP security controls to all staff. One of the keystones to security is a strong program of security awareness. Staff involved with back-up of SEC data indicated that they had not received security awareness training, and they were not aware if SEC had such a program. As a result, the staff did not know what actions the agency expected of them in this critical area.

While personnel did not know what the agency expected of them, there was evidence that they were concerned about security. Some field personnel went to the extraordinary safety measure of keeping the last data tape for each week of operation stored at home over the weekend.

RECOMMENDATION

We recommend SEC:

A. Develop and implement a security awareness program.

MANAGEMENT'S COMMENT

Management refers to their response to Finding 1, regarding that an extensive security program is in place at the SEC, and that extensive training has been provided to ADP liaisons and technical personnel. Management agrees that additional training is beneficial and stated that recently the security-training program has been extended to include non-technical personnel in the agency.

AUDITOR'S RESPONSE

We agree that in September 1998, the SEC issued an Information Technology Security Policy covering responsibilities for protecting agency systems and data. During our audit the Security Officer published a security policy outline on the Intranet. Portions of the outline were completed during our audit. However none of the completed topics covered data back-up and recovery procedures.

Additionally, during fieldwork the Security Officer was developing curriculum to address agency wide security awareness. Regional and district office personnel had not received and did not know of any security awareness training that was available to them.

Memorandum

March 9, 2000

TO: Walter Stachnik
Inspector General

FROM: Michael Bartell, Chief Information Officer
Office of Information Technology

SUBJECT: Audit Report No. __ on Data Back-Up Procedures

Thank you for the opportunity to comment on your office's audit on the SEC's data back-up procedures. I am pleased that the audit found that the agency's procedures, and OIT's actions in particular, are effective in minimizing the risk of data loss. OIT agrees in general with the audit recommendations that improvements could be made to enhance the overall effectiveness of the data back-up and recovery program. In particular, we agree training of non-OIT personnel could be enhanced and have taken actions to expand the security and system administration programs to address these concerns.

However, we believe a number of the audit findings presented inaccurate, or incomplete information. Specifically, a number of OIT personnel responsible for either conducting data back-up activities or managing contractors responsible for this activity were not interviewed as part of the audit resulting in an over emphasis on the field office findings as representative of the entire program. Further, in regard to field office findings, the audit incorrectly states that the ADP liaisons in the regions and districts are not the primary and secondary personnel responsible for back-up activities. Our understanding is that ADP liaisons in the region and districts are the primary personnel responsible for backing up systems and data located on servers in their office and we identified this inconsistency to the audit team.

Finding 1: Provide Policies and Procedures for Back-Up Activities (Recommendation A and B)

OIT Response: We believe appropriate policies and procedures exist to provide operating guidance to personnel responsible for data back up activities.

Three contractors are responsible for conducting a majority of the agency's data back-up for the agency's systems and data. The three operational areas covered by contractors include helpdesk (conducting regular server back-ups), mainframe systems, and the EDGAR system. Each of these contractors have extensive and well documented standard operating procedures and conduct regularly scheduled data back-up and recovery activities. The effectiveness of these programs is evidenced by the audit test results of back-up files showing no instances when files could not be recovered.

In September 1998, the SEC issued an Information Technology Security Policy covering responsibilities for protecting agency systems and data. Concurrently, OIT issued a series of technical bulletins identifying specific guidance on standards and implementation practices in support of the policy. This information was published on the SEC's intranet, made available to contractors and COTRs, and incorporated in a variety of training programs.

During 1999, system administration practices were covered with the ADP liaisons as part of the agency's NT operating system upgrade. In September 1999, a full day of training was provided to ADP liaisons on troubleshooting and system administration practices as part of the annual ADP liaison conference. During the last half of calendar 1999 ADP liaisons and contractor staff were all involved in contingency planning and disaster recovery activities as part of the SEC's Year 2000 program.

Physical security for controlling access and protecting equipment is addressed in the agency's security policy and related technical bulletins. However, modifications to buildings were SEC equipment is located must be requested through the agency's Office of Personnel and Administrative Management.

Finding 2: Train Back-Up Operators and their Alternates (Recommendations A)

OIT Response: We believe our contractor staff are adequately trained to conduct data back up and recovery responsibilities to meet their contractual obligations. We agree that more vigorous training could be provided to ADP liaisons and their alternates to enhance their understanding of data back-up and recovery practices. OIT is working with the Office of the Executive Director on approaches to providing more formal and regularly scheduled training for these personnel.

Finding 3: Implement Disaster and Contingency Plans (Recommendation A)

OIT Response: As part of the SEC's Year 2000 effort, offices were required to identify the mission critical activities the agency must conduct during an emergency and their contingency plans for operating during an emergency. This information was shared with contingency planning personnel throughout the agency. Also as part of this program, offices identified critical personnel that were required to respond during any emergencies experienced as a result of the century rollover. OIT worked extensively with those individuals to ensure they understood their roles and responsibilities and that they implemented the agency's plan depending upon the which scenario played out during the rollover period covered by the plan.

These activities occurred after the audit fieldwork was completed. However, we believe they provided the agency with a significant foundation on which to build future disaster recovery and contingency planning activities.

Finding 4: Implement Security Awareness Training (Recommendation A)

OIT Response: As indicated in OIT's response to Finding 1, an extensive security program is in place at the SEC. Extensive training has been provided to ADP liaisons and technical personnel. We agree that additional training is beneficial and recently expanded the security training program to include non-technical personnel in the agency.

cc: Darlene Pryor