COTTON & COMPANY LLP
auditors • advisors

333 North Fairfax Street • Suite 401 • Alexandria, Virginia 22314 • 703/836/6701 • fax 703/836/0941 • www.cottoncpa.com

September 10, 2004

Mr. Walter Stachnik
United States Securities and Exchange Commission
Office of the Inspector General
450 Fifth Street, NW
Washington, DC 20549

Mr. Stachnik:

I am pleased to submit the attached Fiscal Year 2004 Federal Information Security Management Act (FISMA) executive summary report. This report provides the United States Securities and Exchange Commission (SEC), Office of Inspector General (OIG), with responses to Office of Management and Budget (OMB) Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act.

FISMA requires OIGs to complete an annual review of agency security program and practices and to report the results of its evaluation. To assist agencies in fulfilling their FISMA evaluation and reporting responsibilities, OMB issued the above-mentioned memorandum that provides a consistent form and format for agencies to report back to OMB. We completed our responses primarily based on our subsequent review of documentation supporting the entity-wide security program and review of agency Plans of Action and Milestones. Also, we coordinated with SEC management in preparing the responses and appreciate their cooperation in this effort.

We value your feedback and would appreciate your comments on the enclosed work and the services provided. Should you have any questions or concerns, please do not hesitate to contact me at 703.836.6701.

Very truly yours,

COTTON & COMPANY LLP

Loren F. Schwartz, CPA, CISA
Partner

Enclosures

Federal Information Security Management Act

FY 2004 Executive Summary Report

U.S. Securities and Exchange Commission
Office of Inspector General

September 10, 2004

Prepared by Cotton & Company LLP
333 North Fairfax Street
Alexandria, Virginia 22314

Contract No. SECHQ1-03-D-0175
Task Order No. 0002

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

FY 2004 EXECUTIVE SUMMARY REPORT

The Office of Inspector General (OIG) of the Securities and Exchange Commission (SEC) engaged Cotton & Company LLP to conduct an independent evaluation of its information systems and security program and controls for compliance with the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002. This report discusses the effectiveness of information system controls to protect and secure SEC's information technology infrastructure and assets.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

Every agency shares the responsibility to secure the federal government's information and information systems. Administration policy requires federal agencies to take a risk-based cost-effective approach to secure all information and systems, identify and resolve current IT security weaknesses and risks, as well as protect against future vulnerabilities and threats.

On December 17, 2002, the President signed into law the E-Government Act (Public Law 107-347), which includes Title III, Information Security. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA continues annual review and reporting requirements introduced in GISRA. In addition, FISMA includes new provisions aimed at further strengthening the security of the federal government's information and information systems, such as development of minimum standards for agency systems. In general, FISMA:

- Lays out a framework for annual information technology security reviews, reporting, and remediation planning/
- Codifies existing OMB security policies, including those specified in Circular A-130, *Management of Federal Information Resources*, and Appendix III.
- Reiterates security responsibilities outlined in the Computer Security Act of 1987, Paperwork Reduction Act of 1995, and Clinger-Cohen Act of 1996.

Under this framework, the federal government is able to objectively measure IT security progress and remaining problems. This information is essential to ensuring that priorities are placed on remediation efforts and IT resources, resulting in the timely resolution of IT security weaknesses.

OMB issued Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, on August 23, 2004. This guidance provides clarification to agencies for implementing, meeting, and reporting FISMA requirements to OMB and Congress. POA&M reports to OMB—provided quarterly beginning January 31, 2002—are intended to assist the agency in identifying, assessing, prioritizing, and monitoring its progress in correcting security weaknesses in programs and systems.

SECURITIES AND EXCHANGE COMMISSION

Congress established SEC in 1934 to enforce the Securities Act of 1933 and the Securities Exchange Act of 1934 and to promote stability in the markets and to protect investors. The primary mission of SEC today is still to protect investors and maintain the integrity of the securities markets.

SEC is comprised of five Presidentially-appointed Commissioners, four divisions, and 18 offices and approximately 3,100 staff. SEC's four divisions are consistent with its organizational structure:

Division of Corporate Finance: Oversees corporate disclosures of important information to the investing public.

Division of Market Regulation: Establishes and maintains standards for fair, orderly, and efficient markets.

Division of Investment Management: Oversees and regulates the investment management industry and administers securities laws affecting investment companies and investment advisers.

Division of Enforcement: Investigates possible violations of securities laws and recommends Commission action when appropriate.

SCOPE AND METHODOLOGY

As discussed in OMB Memorandum M-04-25, within the context of FISMA, an evaluation is contemplated rather than an audit. Our review was not intended to result in the issuance of an opinion and we therefore do not issue an opinion as defined by the American Institute of Certified Public Accountants. Our review objective was to assist the OIG in performing an independent evaluation of SEC's information security policies and procedures for compliance with FISMA and federal regulations and standards and to evaluate SEC's efforts to:

- Meet its responsibilities under FISMA.
- Implement plans of actions and milestones.
- Provide sufficient supporting evidence of SEC's security program to enable OIG to complete its reporting requirements to OMB.

To develop a response for each OMB question, we met with SEC officials and reviewed applicable documentation to develop an understanding of the SEC's entity-wide security program. Additionally, we reviewed the internal controls work and results of the most recent financial statement audit. These results, although still in draft, have been validated by SEC management. In doing our work, we reviewed a number of security components, including:

1. Security management structure.
2. Risk management.
3. System security planning.
4. Certification and accreditation.
5. Computer incident response capability.
6. Contingency planning.
7. Security awareness.
8. Life cycle security.
9. Personnel security.

We have provided quantitative and, where indicated, narrative responses to OMB questions. Responses to these questions are based on a limited review of documentation provided by the client and interviews with key management and personnel. We performed this work from July 13 through September 10, 2004.

RESULTS

In the prior year, one material weakness and three significant deficiencies were identified. One significant deficiency related to the lack of a Chief Information Officer. We would like to commend management for resolving this deficiency by appointing a new Chief Information Officer in January 2004. Additionally, a Chief Security Officer was appointed in August 2004. During the year SEC's Certification and Accreditation process was initiated for 8 systems.

The material weakness and the two remaining significant deficiencies identified in the prior year, remain unresolved. The material weakness was reported in FY 2002 and related to weak security controls within the financial management systems. The two significant deficiencies related to failure to maintain a Plan of Actions and Milestones (POA&M) process, and IT security costs not being properly identified by project, tracked, and reported in SEC's Exhibits 53 and 300.

In addition to the material weakness and two remaining significant deficiencies reported last year, we are reporting four new significant deficiencies:

1. SEC is not substantially in compliance with OMB Circular A-130, Appendix III, *Management of Federal Information Resources*. During the financial statement audit numerous findings were issued. Such findings include not certifying and accrediting major systems and not creating contingency plans for all major applications.

2. SEC is not substantially in compliance with FISMA requirements. Specifically we noted that quarterly POA&M reports were not submitted to OMB.

3. SEC is not substantially in compliance with National Institute of Standards and Technology (NIST) guidance. During the review, we noted that several findings were issued in draft as part of the financial statement audit for non-compliance with standards.

4. SEC has not adequately addressed information security issues from prior years. Several weaknesses at SEC identified in previous audits have not been resolved. Such weaknesses include the ADP weakness that was first identified in 1989.

FISMA defines a significant deficiency as:

> *…a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of an agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.*

The significant deficiencies enumerated above, may have existed in previous years and are being reported now due to the detailed nature of the financial statement audit that was performed this year. This is the first time that a financial statement audit will be performed at SEC in-line with the Accountability of Tax Dollars Act of 2002.

For each of these significant deficiencies, numerous system-specific weaknesses require management's attention. Before management can address these weaknesses, however, certain structures need to be in place. These structures include:

1. A process for tracking and resolving identified weaknesses.

2. A process for performing annual systems reviews and completing certification and accreditations for all systems.

3. A process for ensuring compliance with applicable information technology laws and regulations.

4. Security baseline configurations for systems.

5. A budgetary process that considers information technology security needs and incorporates the POA&M process.

The reported material weakness and significant deficiencies listed above require senior management's immediate attention to ensure that proper corrective action is taken to mitigate the potential for further deficiencies; ensure compliance with OMB's FISMA reporting requirements, OMB Circular A-130, and NIST standards; and strengthen SEC's management of its information infrastructure.