U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

2008 FISMA Executive Summary Report

PUBLIC REDACTED VERSION

ECS
Engineered for Performance

September 29, 2008
Report No. 451

M E M O R A N D U M

September 29, 2008

To: Lew Walker, Acting Chief Information Officer

From: H. David Kotz, Inspector General

Subject: *2008 FISMA Executive Summary Report*, Report No. 451

This memorandum transmits the Securities and Exchange Commission, Office of Inspector General's (OIG) 2008 Federal Information Security Management Act (FISMA) Executive Summary report. This report details our responses to Section C of the Office of Management and Budget FISMA template. The information in the report is provided as a result of our coordination and input from the Office of Information Technology (OIT) and the Senior Agency Official for Privacy and was used to form a consolidated SEC response.

The final report consists of three recommendations that are addressed to the OIT. OIT concurred with all of the recommendations and indicated that appropriate action will be taken. In addition to responding to the recommendations, OIT provided comments to the draft report.

Should you have any questions regarding this report, please contact Jacqueline Wilson at 202-551-6326.

Attachment

cc: Peter Uhlmann, Chief of Staff
Diego Ruiz, Executive Director, Office of the Executive Director
Ralph Mosios, Acting Chief Security Officer, Office of Information Technology
Barbara Stance, Chief Privacy Office, Office of Information Technology
Darlene Pryor, Management Analyst, Office of the Executive Director

Rick Hillman, Managing Director of Financial Markets and Community Investment, GAO

P U B L I C R E D A C T E D V E R S I O N

EXECUTIVE SUMMARY

In June 2008, the U.S Securities and Exchange Commission (SEC), Office of Inspector General (OIG), contracted with the Electronic Consulting Services, Inc. (ECS) to assist with the completion and coordination of OIG's input to the SEC's response to the Office of Management and Budget (OMB) Memorandum M-08-21. The Memorandum provides instructions and templates for meeting the FY 2008 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) Title III, Pub. L. No. 107-347.

ECS commenced work on the project in early August 2008, when the final FISMA templates were promulgated by the OMB. ECS' principle tasks included the completion of the OIG portion of the templates and the development of an Executive Summary report.

BACKGROUND

FISMA provides the framework for securing the Federal government's information technology. All agencies must implement the requirements of FISMA and annually report to the OMB and Congress the effectiveness of their Privacy and information security program. OMB uses the information to help evaluate agency-specific and government-wide privacy performance, development of its annual security report to Congress, assist in improving and maintaining adequate agency privacy performance, and inform development of the E-Government Scorecard under the President's Management Agenda.

OBJECTIVES

The objectives of this report are to provide background information, clarification, and recommendations regarding the OIG's response and input to Section C of the OMB reporting template. Generally, the reporting categories and questions were generally the same as in 2007; however, there were some updates based on security and privacy policies issued this year. The 2008 reporting topics for the OIG reporting template include:

- FISMA Systems Inventory

- Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing
- Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory
- Evaluation of Agency Plan of Action and Milestone (POA&M) Process
- Inspector General (IG) Assessment of the Certification and Accreditation Process
- IG Assessment of the Agency Privacy Program
- IG Assessment of the Agency Privacy Impact Assessment (PIA) Process
- Configuration Management
- Incident Reporting
- Security Awareness Training
- Collaborative Web Technologies and Peer to Peer File Sharing
- E-Authentication Risk Assessments

There are also some additional questions related to OMB Memorandum M-08-09 of January 18, 2008, New FISMA Privacy Reporting Requirements for FY 2008.

The FISMA IG Reporting template contains responses to a fixed set of options designed into the template. In some cases, the responses are either numeric or binary (yes/no). In other cases, responses are limited to qualitative assessments (excellent, good, poor, etc.), or percentages estimates (96% to 100%, 81% to 95%, etc.). The reporting template also provides several fields for optional text comments.

RESULTS

Key findings and results for the 2008 FISMA evaluation include:

- Our initial OIG evaluation of systems used by the Division of Enforcement for referrals and the Office of Compliance Inspections and Examinations (OCIE) to assist in the monitoring of registered advisers revealed there were no significant issues.

- The SEC operates a total of 49 systems. Forty-four of the systems have been evaluated as having moderate-system impact levels. The remaining systems were evaluated as having a low system impact level.

- SEC almost always performs oversight and evaluations to ensure information systems used or operated by agency contractors, or other organizations on behalf of the agency, to meet applicable requirements.

- The SEC has developed an inventory of major information systems.

- The SEC's POA&M process provides an effective roadmap for continuous security improvement, assists with prioritizing corrective action and resource allocation, and is a valuable management and oversight tool.

- The SEC's overall Certification and Accreditation program is assessed as good.

- The Privacy Office has made significant progress in its development of privacy resources, in outreach within the SEC and Regional Offices, and in benchmarking externally with other agencies.

- The SEC has developed and disseminated a formal, documented, configuration management policy (implementation guidance) that satisfactorily addresses security configuration management requirements.

- SEC systems implement common security configurations; including those available through National Institute of Standards and Technology (NIST) most of the time.

- SEC did not provide evidence that they have implemented the [redacted].

SUMMARY OF RECOMMENDATIONS

1. OIT needs to complete the security controls and contingency plan testing for the remaining systems.
2. OIT needs to address the requirements for [redacted] to include:
   - Adopting and implementing the [redacted].
   - Modifying all contracts related to common security settings to include the New Federal Acquisition Regulation 2007-004 language.
   - Implementing the for [redacted].
3. OIG recommends that this Executive Summary Report, along with the completed OIG Reporting Template (provided separately), be used to develop the SEC's annual consolidated FISMA Report in accordance with OMB Memorandum M-08-21.

AUDIT REQUEST AND IDEAS

The Office of Inspector General welcomes your input. If you would like to request an audit in the future or have an audit idea, please contact us at:

U.S. Securities and Exchange Commission
Office of Inspector General
Attn: Assistant Inspector General, Audits (Audit Request/Idea)
100 F. Street N.E.
Washington D.C. 20549-2736
202-551-6037
202-772-9265
Email: oig@sec.gov

Hotline

To report fraud, waste, abuse, and mismanagement at SEC, contact the Office of Inspector General at:

Phone: 877.442.0854

Web-Based Hotline Complaint Form:
www.reportlineweb.com/sec_oig