2005 FISMA Executive Summary Report

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

Submitted to
Mr. Nelson Egbert
Deputy Inspector General

September 23, 2005

From

ECS

2750 Prosperity Avenue, Suite 510
Fairfax, Virginia 22031

Contact Person
Bob Richardson
Project Manager
Phone (703) 270-1540   Fax (703) 270-1541

1 Introduction

The U.S Securities and Exchange Commission (SEC), Office of Inspector General (OIG), contracted with Electronic Consulting Services, Inc. (ECS) to perform an independent evaluation of its information technology (IT) systems in order to meet its responsibilities under the Federal Information Security Management Act (FISMA). This report discusses the results of ECS's evaluation and the effectiveness of the SEC's security controls in protecting its IT systems and data.

1.1 Overview

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

This report summarizes the answers to the 2005 FISMA questionnaire published by OMB. ECS's responses are based on the results of the annual system and program reviews, the agency's work in correcting weaknesses identified in their Plan of Action and Milestones (POA&Ms), as well as ECS's evaluation of two of the SEC's major applications (ACTS Plus and EFOIA). Quantitative responses are provided in the FISMA questionnaire, and narrative comments are included where necessary to provide meaningful insight into the status of the agency's security program.

1.2 Objectives and Scope

The objectives of this evaluation were threefold: 1) Perform the necessary evaluation procedures to answer those questions published by OMB in its reporting guidance; 2) Compile an Executive Summary for the SEC's OIG; and 3) Perform an assessment of two of the SEC's major systems (ACTS Plus and EFOIA) that have been certified and accredited (GAO assessed six other major systems).

The 2005 OMB guidance is similar to prior year guidance in requiring the OIG to independently evaluate and report on how the Chairman, CIO, and program officials implemented mandated information security requirements related to information systems program reviews; life cycle security; security incident and response; corrective action reporting; and measuring information security performance.

This year, OMB allowed agencies the choice of conducting FISMA evaluations according to NIST Special Publication 800-26, *Security Self- Assessment Guide for Information Technology Systems* (November 2001) or NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (February, 2005). With the concurrence of the OIG, ECS conducted this FISMA evaluation against the controls found in NIST SP 800-53 due to the fact that 800-53 is the standard used for certification and accreditation (C&A) of Federal IT systems, and the fact that 800-53 will soon become the standard used for future FISMA evaluations.

1.3 Background

ECS evaluated the two major applications (ACTS Plus and EFOIA) in accordance with NIST SP 800-53 and answered the questions published by OMB in its FISMA questionnaire. The results of ECS's evaluations of the two major applications are presented in the following reports:

- 2005 FISMA Assessment Findings and Recommendations reports for ACTS Plus, September 2005 (Audit No. 409)
- 2005 FISMA Assessment Findings and Recommendations reports for EFOIA, September 2005 (Audit No. 410)

In response to OMB's questions and the OIG's request, ECS also performed an especially thorough assessment of the C&A process that the SEC followed for the certification and accreditation of the major applications. The results of ECS's evaluation of the SEC's C&A process are presented in the report *Evaluation of the SEC's C&A Process,* September 2005 (Audit No.411).

ECS performed the assessment as required by the Computer Security Act of 1987 to determine if the applications meet the necessary security requirements prescribed in the Federal Information Systems Control Audit Manual (FISCAM) and National Institute of Standards and Technology (NIST) Special Publications 800-53. Components of the SEC's Security Program that were evaluated included:

- SEC's security management structure
- Risk management process
- System security plans
- Certification and accreditation process
- Computer incident response capability
- Contingency planning process and procedures
- Security awareness environment
- Life-cycle management of security, management of personnel security

- Privacy

To determine whether the IT security objectives have been met, ECS reviewed pertinent documentation, including regulations and standards, security documentation, and system documentation. ECS also interviewed and corresponded with staff and performed visual inspections and examinations.

The evaluations were performed in accordance with Government Auditing Standards 2003 (the Yellow Book), and all analyses were performed in accordance with guidance from the following:

- OMB Memorandum M-04-25, Reporting Instructions for the Federal Information Security Management Act (8/23/04)
- OMB Memorandum M-03-22, Guidance for Implementing Privacy Provisions of the E-Government Act of 2002
- OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies
- OMB Guidance M-04-15, Guidance Development of Homeland Security Directive (HSPD) – 7 Critical Infrastructure Protection Plans to Protect Federal Infrastructure and Key Resources
- Federal Information Processing Standards Publication (FIPS PUB) 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-18, Guide for Developing Security Plans for IT Systems
- NIST SP 800-30, Risk Management Guide for IT Systems
- NIST SP 800-34, Contingency Planning Guide for IT Systems
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal IT Systems
- NIST SP 800-47, Security Guide for Interconnecting IT Systems
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- NIST SP 800-61, Computer Security Incident Handling Guide

Fieldwork was conducted between July 1 and September 3, 2005.

2 Results

ECS found that the SEC has made significant progress in developing a mature information security program, and has addressed many security vulnerabilities discussed in the FY 2004 FISMA report and elsewhere. For example, the SEC:

- Certified and accredited over half of its systems (12 out of 20 systems), including its contractor-operated systems
- Made improvements in its POA&M tracking and reporting process, including instituting the use a software tool called CommandCenter
- Submitted quarterly POA&M reports to OMB for the first time
- Developed an inventory of SEC systems, including contractor-operated systems
- Completed and tested contingency plans for several major applications
- Developed new policies and procedures and updated existing policies and procedures to address various security issues, especially IT Planning and Investment processes
- Provided security awareness training to the majority of its employees and contractors using a new training portal called E-Training; tracked training attendance; and sent out reminder emails regularly to those who have not yet completed the required modules
- Provided information on peer-to-peer (P2P) file sharing in its monthly security awareness newsletter and added it to its training program
- Moved the alternate site for its data center from its headquarters in Washington, DC, to a more secure location
- Developed a draft of the CSIRT Handbook to provide procedures to all SEC employees and contractors on handling and reporting computer security incidents
- Initiated a Privacy Impact Assessment (PIA) program, which will be implemented in FY06

As a result of these actions, ECS believes that the SEC continues to make steady progress in the development of a mature security program in accordance with FISMA requirements.

Notwithstanding progress made by the SEC in the areas identified above, ECS found other areas where improvements are still needed. ECS identified the following significant deficiencies:[1]

1. Not all of the SEC's systems have been certified and accredited. Currently, only 12 out of 20 systems have been accredited.
2. The SEC's C&A process, used to accredit the 12 systems cited above, is problematic. The General Support System, used as a critical security component for all 20 major systems, has not been accredited. This omission casts significant doubt on the security of all systems that depend on it.

   We also have concerns about the approach that was used by the Commission to certify and accredit the 12 systems. Most importantly, the contractor hired to accredit the 12 systems is the same contractor that developed the draft system documentation and was hired by OIT as the certification agent for the same 12 systems. The applicable NIST standards state that the certification agent "be independent of those individuals responsible for correcting security deficiencies identified during the security certification." In our opinion, the certification agent was not independent.
3. Not all of the SEC's systems have had POA&Ms created. Only systems that have been certified and accredited have had POA&Ms created; therefore, only 12 out of 20 systems have POA&Ms.
4. Not all employees and contractors have received security awareness training. Approximately 15% have not taken the online courses as of the date of this review.
5. Even though OIT uses industry best practices and tries to ensure that a standardized foundation is deployed on all SEC computer systems, there is no agency-wide security configuration policy. In addition, there are no security configuration guides for the various operating systems that the SEC utilizes.
6. The SEC has not yet completed e-authentication risk assessments for its systems. The OMB memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, established the requirement for agencies to conduct an e-authentication risk assessment on systems remotely authenticating users over a network for the purposes of e-government and commerce. E-authentication risk assessments should be conducted in parallel with the overall system risk assessment, addressed in system security plans, and certified before authorization to process.

[1] A *significant finding* or deficiency is defined 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 the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. Significant deficiencies are usually high- or medium-risk vulnerabilities.
A *reportable condition* is a low-risk vulnerability that does not have to be fixed immediately, but be addressed at some time in the future. Agencies are no longer required to report the number of significant deficiencies during the annual FISMA report to OMB; however, all security weaknesses must be included in and tracked on the system's POA&Ms.

7. Although a Privacy Impact Assessment (PIA) program has been established, PIAs have not been performed for any system. The SEC has several systems that fall under the Privacy Act and therefore require PIAs.

   Additional findings respective to the two applications assessed as part of this effort can be examined in the 2005 FISMA Assessment Findings and Recommendations reports for ACTS Plus and EFOIA.

In order to mitigate these weaknesses, we recommend that the SEC consider implementing the following:

A. Certify and accredit the remaining eight systems, especially the general infrastructure support system (GSS) upon which all the other systems depend.

B. Ensure that all certifications follow NIST and OMB standards to guarantee accurate, unbiased results (refer to the ECS report *Evaluation of the SEC's C&A Process*, September 2005, for more details).

C. Create POA&MS for the remaining eight systems once they are certified and accredited.

D. Ensure that 100 percent of the SEC employees and contractors take the online security awareness training course.

E. Develop an agency-wide security configuration policy as well as security configuration guides for the various operating systems that the SEC utilizes.

F. Ensure that e-authentication risk assessments are completed for all systems remotely authenticating users over a network for the purposes of e-government and commerce.

G. Conduct PIAs for all systems that fall under the Privacy Act.