U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

OASIS System Report - 2008 FISMA

PUBLIC REDACTED VERSION

ECS
Engineered for Performance

March 24, 2009
Report No. 463

This report was redacted at management's request because of concern over the release of information regarding the SEC's computer system's to the general public.

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

March 24, 2009

To: Charles L. Boucher II, Chief Information Officer, Office of Information Technology
Lori Richards, Director, Office of Compliance Inspections and Examinations

From: H. David Kotz, Inspector General, Office of Inspector General

Subject: *OASIS System Report - 2008 FISMA*, Report No. 463

This memorandum transmits the U.S. Securities and Exchange Commission, Office of Inspector General's (OIG) final report detailing the results of our assessment of the OCIE Advisor Intelligence System (OASIS). The evaluation was conducted as part of our 2008 Federal Information Security Management Act (FISMA) response to the Office and Management and Budget.

This report contains three recommendations to the Office of Information Technology (OIT) and the Office of Compliance Inspections and Examinations (OCIE). The recommendations when implemented will help to improve OASIS' security posture once it is fully deployed throughout the Commission. The OIT concurred with all the report's recommendations with clarification. The OCIE also concurred with all the report's recommendations.

Should you have any questions regarding this report, please do not hesitate to contact me. We appreciate the courtesy and cooperation that you and your staff extended to our auditor during this evaluation.

Attachment

cc: Kayla J. Gillan, Deputy Chief of Staff, Office of the Chairman
Diego Ruiz, Executive Director, Office of the Executive Director

Ralph Mosios, Acting Chief Information Security Officer, Office of Information Technology
Darlene Pryor, Management Analyst, Office of the Executive Director

TABLE OF CONTENTS

BACKGROUND AND OBJECTIVES

In June 2008, the U.S. Securities and Exchange Commission (SEC or Commission), Office of Inspector General (OIG), contracted the services of Electronic Consulting Services, Inc. (ECS) to complete and coordinate OIG's input to the Commission's response to the Office of Management and Budget (OMB) Memorandum M-08-21. The Memorandum consists of instructions and templates that federal agencies must use to complete select information system assessments, in compliance with the fiscal year (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 evaluation in August 2008, when OMB promulgated the final FISMA templates. ECS' principal tasks included the completion of the OIG portion of the templates and the development of a report. The task order also included the completing two system reviews as required by the FY 2008 FISMA Reporting Guidelines. The reports discuss the results of our review of OCIE Advisor Intelligence System (OASIS).

Background

The OASIS application provides extensive integrated search capabilities into various [redacted] and [redacted] data sources to perform "'fact finding" of certain entities and it can generate reports and alerts. The search begins with [redacted] data currently available to the Office of Compliance Inspections and Examinations (OCIE).

The application searches [redacted] such as [redacted], [redacted], [redacted], [redacted], [redacted], [redacted] and [redacted] to collect specific information regarding an [redacted] from the [redacted] data. The application then does an [redacted] search. The application will attempt to synthesize information found in internal and external data sources about an entity, and/or its employees and then

generates dashboard reports specifically related to investment advisers, investment companies, hedge funds, transfer agents, and administrators. In addition, OASIS will also be able to generate alerts and send emails to specific OCIE users and staff in its regional offices.

This report supports OIG's response to Section C of the Office of Management and Budget FISMA template.

Objectives

The objective of this evaluation was to assess the OASIS system. We also evaluated the SEC's compliance with the security controls that are prescribed by the National Institute of Standards and Technology (NIST) Special Publication 800-53A (NIST 800-53A). NIST 800-53A was developed to promulgate standards, guidelines, and other publications to assist federal agencies in implementing the FISMA and to manage cost-effective programs that protect information and information systems. NIST 800-53A prescribes the following controls as shown in Table 1:

Table 1: NIST 800-53A Controls

IDENTIFIER	FAMILY OF CONTROLS	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	C&A and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational

RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

Source: NIST

Classes and Families of Security Controls

Security controls are organized into classes and families for ease of use in the control selection and specification process. There are three general classes of security controls (management, operational, and technical), and 17 security control families. Each family contains security controls that are related to the security's functionality of the family. A two-character identifier is assigned to uniquely identify each control family.

Control Classes

Technical Controls (i.e., safeguards or countermeasures) - Controls which are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Operational Controls - Controls which are primarily implemented by people as opposed to systems.

Management Controls - Controls that focus on the management of risk and the management of information systems security.

Control Families

Families are assigned to a respective class based on the dominant characteristics of the controls in that family. Many security controls, however, can be logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning family is listed as an operational control; however, it also has characteristics that are consistent with security management. The NIST 800-53 family of controls are described in the "Results" section of this report.

Results

Our evaluation of OASIS revealed there were no significant security issues or areas of non-compliance. We noted that OASIS is in the [redacted] of its system lifecycle. There [redacted], and the system is not [redacted] to other Commission, or [redacted] or [redacted]. For this reason, it has little [redacted] to common [redacted]. The results of our assessment were entered into a Microsoft Access database, which was used to track and report the results of the assessment. Some controls within a family were not evaluated because they did not apply to this type of system. Control families Maintenance (MA) and Physical and Environmental Protection (PE) were not examined due to access constraints, although, in a few cases, we were able to evaluate one or more of these controls.

Access Control

Access Control (AC) pertains to the mechanisms and procedures that are used to control access to the information system. In the AC family of controls, AC-1 – AC-20, the OASIS passed 13 of 20 controls. Seven of the AC controls ([redacted]) were not evaluated because they did not apply to this type of system.

ECS evaluated how the SEC implemented controls within the AC family through observation, performing technical assessments, examining artifacts, and conducting interviews. We determined that the SEC has established an effective access control policy and procedures. The Commission develops, disseminates, and periodically reviews/updates its access control policy and procedures. Both the policy and the procedures have all of the necessary elements (purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance) needed to ensure adequate controls within the SEC.

- Access Management - ECS determined that OASIS [redacted] since it currently has [redacted]. However, once the system is moved towards [redacted], additional [redacted] should be implemented.

- [redacted] - ECS determined that it [redacted] be truly [redacted] while the system is in the [redacted]. This safeguard occurs when the [redacted] for [redacted] the [redacted] of [redacted] within the [redacted] and [redacted].
- [redacted], [redacted], [redacted] and [redacted] - ECS determined that these controls [redacted], and therefore, they [redacted]

Awareness and Training

The Awareness and Training (AT) family of controls refers to security training and awareness activities. ECS assessed how the SEC implemented controls in AT-1 to AT-5, and determined that the Commission complied or passed all the controls within this family. The AT family of controls consists of:

- AT-1 Security Awareness and Training Policy And Procedures
- AT-2 Security Awareness
- AT-3 Security Training
- AT-4 Security Training Records
- AT-5 Contacts With Security Groups and Associations

Audit and Accountability

The Audit and Accountability (AU) family of controls contains safeguards used to record user interactions with the system in order to ensure accountability. ECS determined that the SEC fully complies with all the controls in the AU family of controls. The AU family of controls consists of:

- AU-1 Audit and Accountability Policy and Procedures
- AU-2 Auditable Events
- AU-3 Content of Audit Records
- AU-4 Audit Storage Capacity
- AU-5 Response To Audit Processing Failure
- AU-6 Audit Monitoring, Analysis, and Reporting

- AU-7 Audit Reduction and Report
- AU-8 Time Stamps
- AU-9 Protection of Audit Information
- AU-10 Non-Repudiation
- AU-11 Audit Record Retention

Certification, Accreditation, and Security Assessments

The Certification and Accreditation (C&A) and Security Assessments (CA) family of controls refers to compliance with C&A and security policies and requirements. ECS concluded that the SEC fully complies with all the controls in the CA family of controls. For example, with respect to CA-5, Plan of Action and Milestones (POA&M) the SEC develops and updates a plan of action and milestones for OASIS that documents the Commission's [redacted], [redacted], and [redacted] [redacted] noted during the assessment of the security controls, and to [redacted] or [redacted] known [redacted] in the system. With regard to [redacted], ECS determined that the SEC monitors security controls on an [redacted] basis. The CA family of controls consists of the following:

- CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures
- CA-2 Security Assessments
- CA-3 Information System Connections
- CA-4 Security Certification
- CA-5 Plan of Action and Milestones (POA&M)
- CA-6 Security Accreditation
- CA-7 Continuous Monitoring

Configuration Management

The Configuration Management (CM) family uses control hardware and software configuration for the information system. ECS reviewed how the SEC implemented controls within the CM family (CM-1 through CM-8) and determined that the Commission fully complied with all the controls. In addition, we determined that the SEC developed, disseminated, and periodically

reviews/updates its configuration management policy and associated configuration management controls. Controls in the CM family consist of:

- CM-1 Configuration Management Policy and Procedures
- CM-2 Baseline Configuration
- CM-3 Configuration Change Control
- CM-4 Monitoring Configuration Changes
- CM-5 Access Restrictions for Change
- CM-6 Configuration Settings
- CM-7 Least Functionality
- CM-8 Information System Component Inventory

Contingency Planning

The Contingency Planning (CP) family of controls is comprised of efforts taken to prepare for a man-made or natural disaster which may affect the information system. ECS found that the SEC complies with all the CP controls. For example, the Alternate Processing Site control (CP-7) requires an organization to identify an alternate processing site and initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions when the primary processing capabilities are unavailable. The SEC fully complied with this requirement. The CP family of controls consists of the following:

- CP-1 Contingency Planning Policy and Procedures
- CP-2 Contingency Plan
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- CP-5 Contingency Plan Update
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-8 Telecommunication Services
- CP-9 Information System Backup
- CP-10 Information System Recovery and Reconstitution

Identification and Authentication

The Identification and Authentication (IA) family of controls consists of controls used to identify and authenticate users. ECS assessed the SEC's implementation of these controls and determined that the SEC fully complied with its requirements. For example, the Cryptographic Module Authentication (IA-7) control provides that an organization employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a defined cryptographic module. ECS determined that the SEC met this requirement. Within the IA family the seven controls are:

- IA-1 Identification and Authentication Policy and Procedures
- IA-2 User Identification and Authentication
- IA-3 Device Identification and Authentication
- IA-4 Identifier Management
- IA-5 Authenticator Management
- IA-6 Authenticator Feedback
- IA-7 Cryptographic Module Authentication

Incident Response

The Incident Response (IR) family of controls refers to processes and procedures implemented to respond to an incident. We looked at how the SEC implemented the IR controls and determined that the Commission fully complies with this requirement. For example, the Incident Response Training (IR-2) requires organizations to provide personnel training to an incident's response on an annual basis. The IR families of controls consist of:

- IR-1 Incident Response Policy and Procedures
- IR-2 Incident Response Training
- IR-3 Incident Response Testing and Exercises
- IR-4 Incident Handling
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- IR-7 Incident Response Assistance

Maintenance

The Maintenance (MA) family of controls pertains to system maintenance. This family of controls [redacted], because these controls have [redacted] on [redacted].

Media Protection

The Media Protection (MP) family of controls includes controls related to the protection of system media. ECS assessed how the SEC implemented controls within the MP family of controls and determined that the SEC fully complies with all the controls. For example, the Media Access (MP-2) control provides that the organization restricts access to information system media to authorized individuals. Based on interviews and an examination of appropriate artifacts, ECS determined that the SEC fully complied with this requirement. The MP family of controls are as follows:

- MP-1 Media Protection Policy and Procedures
- MP-2 Media Access
- MP-3 Media Labeling
- MP-4 Media Storage
- MP-5 Media Transport
- MP-6 Media Sanitization and Disposal

Physical and Environmental Protection

The Physical and Environmental Protection (PE) family of controls are related to the physical and environmental protection of the information system. Due to [redacted], we [redacted] the physical or environmental security controls as part of the system evaluation. The PE family of controls consists of the following:

- PE-1 Physical And Environmental Protection Policy And Procedures
- PE-2 Physical Access Authorizations
- PE-3 Physical Access Control
- PE-4 Access Control for Transmission Medium

- PE-5 Access Control for Display Medium
- PE-6 Monitoring Physical Access
- PE-7 Visitor Control
- PE-8 Access Record
- PE-9 Power Equipment And Power Cabling
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature And Humidity Controls
- PE-15 Water Damage Protection
- PE-16 Delivery and Removal
- PE-17 Alternate Work Site
- PE-18 Location of Information System Components
- PE-19 Information Leakage

Planning

The Planning (PL) family of controls is related to information systems security planning for the system. ECS determined that the SEC has implemented the PL controls. For example, the System Security Plan (PL-2) requires organizations to develop and implement a security plan for information systems. This provides an overview of the security requirements for the system and provides a description of the security controls in place or are planned for meeting those requirements. Designated officials within the organization review and approve the plan. Based on interviews and an examination of the appropriate artifacts, ECS has determined that the SEC fully complied with this requirement. The PL family of controls is made up of:

- PL-1 Security Planning Policy an
- d Procedures
- PL-2 System Security Plan
- PL-3 System Security Plan Update
- PL-4 Rules of Behavior
- PL-5 Privacy Impact Assessment
- PL-6 Security-Related Activity Planning

Personnel Security

The Personnel Security (PS) family of controls pertains to the controls and security of systems personnel. We determined that the SEC complies with the PS controls. For example, the Personnel Termination, PS-4 requires an organization, upon termination of individual employment, to terminate information system access, conduct an exit interviews, retrieve all organizational information system-related property, and provide appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems. ECS found that the SEC fully complies with the PS requirements. The PS family is comprised of eight controls:

- PS-1 Personnel Security Policy And Procedures
- PS-2 Position Categorization
- PS-3 Personnel Screening
- PS-4 Personnel Termination
- PS-5 Personnel Transfer
- PS-6 Access Agreements
- PS-7 Third-Party Personnel Security
- PS-8 Personnel Sanctions

Risk Assessment

The Risk Assessment (RA) family of controls encompasses those controls that are used to estimate the threats and risks to an information system. ECS looked at how the Commission implemented the RA controls and determined that the SEC complied with all of the controls. For example, the Risk Assessment (RA-4) provides that an organization conduct risk assessments to the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or the and information systems that support the operations and assets of the agency. This further includes information and information systems that are managed/operated by external parties. The SEC fully complied with this requirement. Within the RA family the following controls include:

- RA-1 Risk Assessment Policy and Procedures

- RA-2 Security Categorization
- RA-3 Risk Assessment
- RA-4 Risk Assessment Update
- RA-5 Vulnerability Scanning

Systems and Services Acquisition

The Systems and Services Acquisition (SA) family of controls consist of procedures used to purchase and operate the information system. ECS found that the SEC fully complies with all the SA controls. For example, the Information System Documentation (SA-5) control provides that the organization obtain, protect, and make available to authorized personnel, adequate system documentation. We determined that the SEC fully complies with this requirement. The SA family consists of the following 11 controls:

- SA-1 System and Services Acquisition Policy and Procedures
- SA-2 Allocation of Resources
- SA-3 Life Cycle Support
- SA-4 Acquisitions
- SA-5 Information System Documentation
- SA-6 Software Usage Restrictions
- SA-7 User Installed Software
- SA-8 Security Engineering Principles
- SA-9 External Information System Services
- SA-10 Developer Configuration Management
- SA-11 Developer Security Testing

System and Communications Protection

The System and Communications Protection (SC) family of controls apply to the protection of information that is transmitted within and outside the information system. ECS evaluated how the SEC implemented the SC controls and determined that the SEC complied with all the SC controls. For example, the Denial of Service Protection (SC-5) control states that the information system protects against or limits the effects on certain types of denial of service attacks. We determined that the SEC met this requirement. The SC controls consists of the following:

- SC-1 System And Communications Protection Policy And Procedures
- SC-2 Application Partitioning
- SC-3 Security Function Isolation
- SC-4 Information Remnance
- SC-5 Denial of Service Protection
- SC-6 Resource Priority
- SC-7 Boundary Protection
- SC-8 Transmission Integrity
- SC-9 Transmission Confidentiality
- SC-10 Network Disconnect
- SC-11 Trusted Path
- SC-12 Cryptographic Key Establishment and Management
- SC-13 Use of Cryptography
- SC-14 Public Access Protections
- SC-15 Collaborative Computing
- SC-16 Transmission Of Security Parameters
- SC-17 Public Key Infrastructure Certificates
- SC-18 Mobile Code
- SC-19 Voice Over Internet Protocol
- SC-20 Secure Name / Address Resolution Service (Authoritative Source)
- SC-21 Secure Name / Address Resolution Service (Recursive Or Caching Resolver)
- SC-22 Architecture And Provisioning For Name / Address Resolution Service
- SC-23 Session Authenticity

System and Information Integrity

The System and Information Integrity (SI) family of controls are implemented to ensure the stability and integrity of the information system.

ECS assessed the SEC's implementation of the SC family of controls and determined that the SEC complied with all the controls. For example, the Spam Protection (SI-8) control provides that the information system implements spam protection. We determined that the SEC fully complies with this requirement. The SI controls include:

- SI-1 System and System and Information Integrity Policy and Procedures
- SI-2 Flaw Remediation
- SI-3 Malicious Code
- SI-4 Information System Monitoring Tools and Techniques
- SI-5 Security Alerts and Advisories
- SI-6 Security Functionality Verification
- SI-7 Software and Information Integrity
- SI-8 Spam Protection
- SI-9 Information Input Restrictions
- SI-10 Information Accuracy, Completeness, Validity, and Authenticity
- SI-11 Error Handling
- SI-12 Information Output Handling and Retention

RECOMMENDATIONS

OASIS System

The OCIE Advisor Intelligence System (OASIS) must be evaluated to ensure that the additional security risks that are introduced as the system's exposures increases are properly mitigated.

Recommendation 1:

Prior to deployment, the Office of Compliance Inspections and Examinations in conjunction with the Office of Information Technology should thoroughly evaluate the OCIE Advisor Intelligence System within its [redacted].

Access Control Family and Access Management Assessment

Based on our assessment of the Access Control family and Access Management, we determined that the OCIE Advisor Intelligence System [redacted] have a [redacted]. We determined that this occurred because the system currently only has [redacted] a[redacted]. However, once the system is [redacted] to [redacted], additional account management safeguards must be implemented.

Recommendation 2:

The Office of Compliance Inspections and Examinations in conjunction with the Office of Information Technology should evaluate [redacted] to ensure that the OCIE Advisor Intelligence System has an adequate [redacted].

Information Flow Enforcement Control

Our assessment found that the Information Flow Enforcement control [redacted] because the system was in [redacted]. This safeguard occurs when the system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems. Once the OASIS is moved towards production [redacted] and [redacted] must be [redacted] to [redacted] the [redacted] of [redacted] between the designated sources and destinations (e.g., individuals, devices).

The OASIS should ensure that any operation that causes information to flow to or from a user is covered by an information flow control policy. Controls are needed to implement strong protection against disclosure and modification by untrusted software. Examples of security attributes include sensitivity labels, clearance labels, and identifiers.

Recommendation 3:

The Office of Compliance Inspections and Examinations in conjunction with the Office of Information Technology should implement an adequate Information Flow Enforcement control for the OCIE Advisor Intelligence System.

Acronyms and Abbreviations

ACTS	Agency Correspondence Tracking System
APTS	Administrative Proceedings Tracking System
CATS	Case Activity Tracking System
EDGAR	Electronic Data Gathering and Retrieval System
FISMA	Federal Information Systems Management Act
IARD	Investment Advisory Registration Depository
NIST	National Institute of Standards and Technology
OASIS	OCIE Advisor Intelligence System
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SEC or Commission	U.S. Securities and Exchange Commission
STARS	Super Tracking and Reporting System

Management's Response

The Office of Information Technology March 11, 2009

The Office of Information Technology (OIT) provided written comments to the report, but indicated that their response could not be released to the public. The OIT agreed with the report's three recommendations and provided clarification for each recommendation.

Office of Compliance Inspections and Examinations March 13, 2009

OCIE stated that it concurred with all three recommendations made in the report and will work with OIT to implement those recommendations.

OIG's Response to Management's Comments

The Office of Inspector General is pleased that the Office of Information Technology (OIT) and the Office of Compliance, Inspections and Examinations (OCIE) concurred with all three of the report's recommendations and with OCIE's assertion to work with OIT to implement the recommendations. We believe that the OCIE Advisor Intelligence System security posture will greatly improve once the system is fully deployed throughout the Commission and our recommendations are fully implemented.

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

Tel. #: 202-551-6061
Fax #: 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