U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

CTR System Report - 2008 FISMA

ECS
Engineered for Performance

PUBLIC VERSION

February 27, 2009
Report No. 462

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

OFFICE OF
SPECTOR GENERAL

MEMORANDUM

February 27, 2009

To: Charles L. Boucher II, Chief Information Officer, Office of Information Technology
Linda Thomsen, Director, Division of Enforcement

From: H. David Kotz, Inspector General

Subject: *CTR System Report - 2008 FISMA*, Report No. 462

This memorandum transmits the U.S. Securities and Exchange Commission, Office of Inspector General's final report on the 2008 Federal Information Security Management Act (FISMA) System Evaluation of the Complaints/Tips/Referrals System. This report does not contain any recommendations. Thus, the Office of Information Technology and the Division of Enforcement did not provide any written comments to our discussion draft report.

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 contractor and auditor during this evaluation.

Attachment

cc: Diego Ruiz, Executive Director
Ralph Mosios, Acting Chief Security Officer, Office of Information Technology
David Wiederkehr, Director, Office of Technical Services, Enforcement
Darlene L. Pryor, Management Analyst, Office of the Executive Director

TABLE of CONTENTS

PUBLIC VERSION

Background and Objectives

In June 2008, the U.S. Securities and Exchange Commission (SEC or Commission), Office of Inspector General (OIG), contracted the 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 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' principal tasks included completing the OIG portion of the templates and a report. The task order also included completing two system reviews as required by the FY2008 FISMA Reporting Guidelines. This report documents the results of our review of the Complaints/Tips/Referrals (CTR) System.

Background

The CTR system was originally called the Enforcement Contact Tracking System (ECTS), and the name was changed at the request of the Division of Enforcement (Enforcement). The application consists of a [redacted] and a [redacted].

The CTR system is used to track complaints, tips and referrals that are received from the public. This application is a [redacted] until [redacted] are made to the Commission's [redacted] to support this requirement. Previously, Enforcement used a [redacted] that was designed by Enforcement's internal information technology support staff.

Objectives

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

Table 1: NIST 800-53A Controls

IDENTIFIER	CONTROL FAMILY	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 800-53A

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 (i.e. technical, operational, and management) and 17 security control families. Each family contains security controls that are related to the

security functionality of the family. A two-character identifier is assigned to uniquely identify each control family.

Control Classes Defined

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 primarily implemented by people, as opposed to systems.

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

Summary of Control Families

Control families are assigned to their respective classes based on the dominant characteristics of the controls in that family. Many security controls can be logically associated with more than one class. For example, although CP-1, the policy and procedures control from the contingency planning family is identified as an operational control, it also has characteristics that are consistent with security management as well. The NIST 800-53 family of controls used in this evaluation are described in the Results section that follows.

Recommendations

This report does not contain any recommendations.

Results

Our evaluation of CTR revealed no significant security issues or areas of non-compliance. We noted that CTR is a [redacted] that is in [redacted] and has very [redacted]. The system is operated with [redacted] and has [redacted] to common [redacted]. The results of our evaluation were entered into a Microsoft Access database,

which was then used to track and report the results of the assessment. Several controls within Access Control (AC) family were not evaluated because they did not apply to the CTR system. Control families MA and 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

The Access Control (AC) family of controls pertains to mechanisms and procedures that are used to control access to information systems. In our assessment of the AC family of controls, the CTR system passed 15 of 20 controls. Five of the controls ( ) were not evaluated because they did not apply to pre-production systems. ECS evaluated how the Commission implemented the AC controls through observation, performing technical assessments, examining artifacts, and conducting interviews.

ECS determined that the SEC has established an effective access control policy and procedure. For example we found that the Commission develops, disseminates, and periodically reviews/updates its access control policy and procedures. Both the policy and the procedures have all of the required elements (purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance), that are needed to ensure that the Commission has adequate controls.

We further found that CTR does not have:

- .

Because the CTR is a system in there are several controls that were such as; , , and . However, as the CTR system is moved to , the SEC must ensure that additional account management safeguards are implemented.

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 within AT-1 through AT-5, and found from our assessment that the Commission has complied with all the controls. The AT family of controls consists of the following:

- 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 reviewed the SEC's implementation of the AU family of controls and determined that the Commission fully complies with the controls. The controls consist of the following:

- 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) families of controls refers to compliance with C&A and security policies and

requirements. ECS found that the Commission fully complied with the CA family of controls for CA-1 through CA-7. For example, based on our examination of artifacts and interviews we conducted regarding the CA-5, Plan of Action and Milestones control, ECS determined that the SEC periodically develops and updates a plan of action and milestones for the CTR system that documents the Commission's [redacted], [redacted], and [redacted] to [redacted] noted during the assessment of the security controls, and to [redacted] or [redacted] known [redacted] in the system. With regard to the, [redacted] control, based on examination of the artifacts and interviews that were conducted, ECS determined that the SEC monitors the security controls in the information system on an [redacted] basis. Within the CA family the following controls are:

- 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 of controls is used to control the hardware and software configuration of an information system. ECS determined that the SEC fully complied with all the controls in CM-1 to CM-8. We determined that the SEC develops, disseminates, and periodically reviews/updates its configuration management policy and the associated configuration management controls. The CM family of controls consists 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 that are undertaken to prepare for man-made and/or natural disaster which may affect the Commission's information systems. ECS determined that the SEC complies with all controls in the CP family (CP-1 through CP-10). For example, for Alternate Processing Site (CP-7) requires an organization to identify an alternate processing site and initiate necessary agreements needed to permit the resumption of information system operations for critical mission/business functions when the primary processing capabilities are unavailable. The SEC fully complies with this requirement. The CP family of controls consists of:

- 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 consists of controls used to identify and authenticate users. ECS' assessment of how the SEC implemented controls within the IA family found that the SEC is in full compliance. 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 has determined that the SEC has met this requirement. The IA family consists of the following controls:

- 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 that are implemented in response to an incident. We looked at how the SEC implemented the controls within the IR family and determined that the SEC fully complies with all the controls. For instance, Incident Training (IR-2) control requires organizations to provide its personnel training to incident response on an annual basis. The IR family of controls consists of:

- 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 area [redacted] because these controls have a [redacted] on the [redacted].

Media Protection

The Media Protection (MP) family of controls that includes those related to protecting the system media. ECS assessed how the Commission had implemented controls within the MP family and determined that the SEC fully complied. For example, the MP-2, Media Access control provides that the organization restrict access to information system media to only authorized

individuals. We found that the SEC fully complies with this requirement. The MP family of controls consists of the following:

- 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 are controls related to the physical and environmental protection of the information system. Due to [redacted], we [redacted] the physical and environmental security controls as part of our system evaluation. The PE family of controls consists of:

- 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) control requires organizations to develop and implement a security plan for the information system. The plan must provide an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan. Based on interviews and an examination of appropriate artifacts, ECS found that the SEC fully complies with this requirement. The PL family of controls consists of the following:

- PL-1 Security Planning Policy and 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) consists of controls that pertain to the 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 an employee's employment, to terminate information system access, conduct exit interviews, retrieve all organizational information system-related property, and provide appropriate personnel with access to official records that were created by the terminated employee and are stored on the organization's information system. We found that the SEC complies with this requirement. The PS family of controls consists of the following:

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

- 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 concluded that the SEC complied with the SA controls. Information System Documentation (SA–5) control is designed for an organization to obtain, protect, and make available to authorized personnel, adequate documentation for the information system. The SEC complied with this requirement. The SA family of controls consists of the following:

- 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 applies to the protection of information transmitted within and outside the information system. ECS evaluated the SEC's implementation of the SC controls and determined that the Commission fully complies with all the controls. Regarding Denial of Service Protection (SC-5) control, the information system must protect against or limit the effects of the certain types of denial of service attacks. We found that the SEC fully complies with this requirement. The SC control family is made up of:

- 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 SI controls and determined that the SEC fully complied with all the controls. The Spam Protection (SI-8) cannot occur when the information system implements protection against unsolicited/junk bulk e-mail. We found that the SEC complies with this requirement. The SI family of controls consists of:

- 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

The CTR system is a [redacted] and will soon be [redacted] when [redacted] are made to the Commission's "[redacted] that will support this requirement. Therefore, no recommendations were made for this system. The CTR system is [redacted] with [redacted] and has [redacted] to common [redacted].

PUBLIC VERSION

Acronyms and Abbreviations

ACTS	Agency Correspondence Tracking System
OMB	Office of Management and Budget
FISMA	Federal Information Systems Management Act
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
SEC or Commission	U.S. Securities and Exchange Commission

PUBLIC VERSION

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