



OFFICE OF
INSPECTOR GENERAL

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

MEMORANDUM

March 26, 2010

To: Charles Boucher, Director, Office of Information Technology
From: H. David Kotz, Inspector General, Office of Inspector General (OIG) *HDK*
Subject: *Evaluation of the SEC Privacy Program, Report No. 475*

This memorandum transmits the U.S. Securities and Exchange Commission, OIG's final report detailing the results of our evaluation of the Commission's privacy program.

Based on the written comments that were received and our assessment of the comments, we revised the report accordingly. This report contains one recommendation with which the Office of Information Technology (OIT) concurred. OIT's full comments to this report are included in the appendices.

Within the next 45 days, please provide OIG with a written corrective action plan that is designed to address the recommendation. The corrective action plan should include information such as the responsible official/point of contact, time frames for completing the required actions, milestone dates identifying how you will address the recommendations cited in this report, etc.

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 contractors and auditor.

Attachment

cc: Kayla J. Gillan, Deputy Chief of Staff, Office of the Chairman
Diego Ruiz, Executive Director, Office of the Executive Director
Lewis W. Walker, Deputy Director and Chief Technology Officer, Office of Information Technology
Todd Scharf, Chief Information Security Officer, Office of Information Technology
Barbara Stance, Chief Privacy Officer, Office of Information Technology

Evaluation of the SEC Privacy Program

Executive Summary

The U.S. Securities and Exchange Commission (SEC or Commission), Office of Inspector General (OIG), contracted the services of C5i Federal, Inc. (C5i) to coordinate and complete the OIG's input to the Commission's response to the Office of Management and Budget (OMB) Memorandum M-09-29. OMB Memorandum M-09-29 provides instructions and templates for meeting the fiscal year (FY) 2009 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA), Title III, Pub. L. No. 107-347. C5i's principal tasks included completing OIG's portion of the templates and reporting the results in an executive report. In addition to the standard OIG input, the OIG tasked C5i to examine the Commission's implementation of the privacy processes and technologies.

C5i commenced its work in September 2009, when the final FISMA questionnaires were promulgated by OMB. C5i completed the OIG's portion of the FISMA reporting template (Section C) and developed a report that evaluates the privacy program. C5i reviewed a broad range of issues covering policies, implementation, technologies, the use of encryption and other related aspects of the SEC's privacy program. This report documents the results of C5i's evaluation of the Commission's privacy program.

The privacy office has made significant progress in its development of privacy resources to include outreach to the Commission's headquarter divisions/offices, and regional offices. However, we found the privacy program has not been fully implemented agency-wide and there is needed guidance that must be approved, some of which has been in draft since 2008. Specifically, we found that draft privacy program and privacy incident management policies and procedures need to be finalized, approved, and implemented.

The FISMA, 44 U.S.C. § 3541, *et seq.* is a United States federal law that was enacted in 2002, as Title III of the E-Government Act of 2002. The statute recognizes the importance of information security to the economic and national security interests of the United States and requires federal agencies to develop, document, and implement agency-wide programs that provide information security for its information systems that support the operations and assets of the agency, and those services provided by or managed by other agencies, contractors, or other sources.

FISMA provides the framework for securing the federal government's information technology. FISMA requires that agency program officials, chief information officers, and OIG's conduct annual reviews of the agency's information security and privacy programs, and report the results to OMB. OMB then uses this data to assist in its oversight responsibilities and to prepare its annual government-wide report to Congress regarding FISMA compliance. Federal agencies must implement FISMA requirements and annually report the effectiveness of its privacy program and privacy impact assessment (PIA) process. OMB uses this information to assist in:

- Evaluating agency-specific and government-wide privacy performance;
- Developing the annual security report to Congress;
- Improving and maintaining adequate agency privacy performance; and
- Developing the E-Government Scorecard under the President's Management Agenda.

Objective. The objective of this evaluation was to examine the SEC's implementation of information technology and related processes for the agency's privacy program, to include training, policies and procedures on handling privacy information, roles and responsibilities.

Recommendation. The Office of Information Technology should finalize its outstanding draft privacy related policies and procedures and implement them throughout the agency by the end of the fiscal year.

TABLE OF CONTENTS

Executive Summary	ii
Table of Contents	iv
Results and Recommendations	1
Background	1
Results	4
Recommendation 1	7
Appendices	
Appendix I: Acronyms.	8
Appendix II: Scope and Methodology	9
Appendix III Criteria.....	10
Appendix IV: List of Recommendations	11
Appendix V: Management Comments.....	12
Appendix VI: OIG Response to Management’s Comments	13

Results and Recommendations

Background

In recent years the U.S. Securities and Exchange Commission (SEC or Commission), Office of Information Technology's (OIT), privacy office has made progress in acquiring resources, performing outreach within headquarters and the regional offices, and benchmarking best practices with external agencies. The SEC's privacy office has devoted a significant amount of time to drafting an agency privacy policy and implementing guidance. However, the policy and guidance has not been formally approved. Therefore, C5i Federal, Inc. (C5i) cannot state with assurance that the SEC is currently managing and operating the privacy program with the appropriate internal controls and privacy controls.

The privacy office issued draft guidance covering the privacy program and privacy incident management as follows:

- Draft SECR 24-08 (01.0), *Management and Protection of Privacy Act Records and Other Personally Identifiable Information*; and
- Draft OD 24-08.07 (01.0), *Privacy Incident Management*.

The draft guidance thoroughly documents the roles and responsibilities of the Chief Privacy Officer (CPO) and the Senior Agency Official for Privacy (SAOP), identify procedures and provide direction based on governing guidance.¹

The Commission continues to make progress in its outreach to Headquarters and Regional Offices to increase compliance with privacy documentation such as, Privacy Analysis Worksheets (PAW), Privacy Impact Assessments (PIA), and Privacy Act System of Records Notices (SORN) for programs and systems involving Personally Identifiable Information (PII). Compliance efforts have included updating and disseminating the *Privacy Impact Assessment Guide* (January 2007) and conducting training and seminars to apprise employees and contractors regarding needed requirements. The privacy office developed privacy policies regarding the management and protection of privacy act records and breach notification, (i.e., incident management), which are pending approval.

¹ See *The Privacy Act of 1974*, Title 5 U.S. C. §552a; *Federal Information Security Management Act (FISMA) of 2002*, *E-Government Act of 2002* Public Law 107-347, Title III; the Office of Management and Budget (OMB) Memorandum 05-08 (M-05-08), *Designation of Senior Agency Officials for Privacy*; OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*; *Regulations Pertaining to the Privacy of Individuals and Systems of Records Maintained by the Commission*, Title 17 C.F.R § 200.301 – 200.313, and OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

Additionally, the privacy office conducted a review of its existing inventory of SORNs for the purpose of reducing the use of social security numbers (SSN) within the Commission.

We found the SEC Privacy Program and PIA process will be fully implemented with finalizing and approving draft SEC Regulation (SECR) 24-08, *Management and Protection of Privacy Act Records and other PII*. The Commission has identified appropriate responsible personnel including a Senior Agency Official for Privacy/Chief Information Officer and the Chief Privacy Officer (CPO).

Per the current draft policy that is out for review the roles and responsibilities for the SAOP and CPO are as shown below.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

We found that the SEC is currently developing a privacy program that will include the appropriate controls and guidance mandated in the National Institute of Standards and Technology and OMB documents and is developing draft policy documents that have not yet been implemented.

OIT developed and issued the Privacy Impact Assessment Guide (January 2007). The guide includes instructions and templates for conducting preliminary assessments using the PAW and there is a full assessment using the PIA, of privacy implications in the development of IT systems and projects.

OIT also developed draft breach notification policy, OD 24-08.07 (01.0) Privacy Incident Management. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

We found that the SEC is developing policies that are consistent with guidance that has been provided by *The Privacy Act of 1974*, Title 5 U.S. C. §552a; *Federal Information Security Management Act (FISMA) of 2002*, *E-Government Act of 2002* Public Law 107-347, Title III; OMB Memorandum 05-08 (M-05-08), *Designation of Senior Agency Officials for Privacy*; OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*; *Regulations Pertaining to the Privacy of Individuals and Systems of Records Maintained by the Commission*, Title 17 C.F.R § 200.301 – 200.313. However, these policies (SECR 24-08 (01.0) *SEC Regulation: Management and*

Protection of Privacy Act Records and other PII) which are still in draft and have not been approved and implemented throughout the Commission.

Results

Privacy Policies Not Approved or Implemented. When the privacy office transitioned to OIT, a contractor was brought in to review the existing draft SECR 31-1 and to draft other SEC privacy policies for review. The SEC's OIT Policy Development/Approval process is as follows.

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The following documents are posted on OIT's website to assist in the preparation of policy documents IT Policy Development Process, Writing Tips and Tools and II 24-06.05.01, Preparing and Approving Information Technology-Related Policy.

OIT hired a contractor to perform a privacy policy review. The contractor was to update the existing privacy policies and develop any additional policies needed to meet the necessary requirements. Specifically, the contractor was to address the following:

C.3.4.8.1 Current Policies. The contractor shall review current privacy policies, procedures, standards, and guidelines for conformance with current federal requirements and industry standards. The contractor shall address the content and effectiveness of SEC documents for adequacy and consistency with legislation, regulations, and guidelines considering the SEC mission.

C.3.4.8.2 New Requirements Review. The contractor shall review and comment on new and proposed policies, legislation, standards, and guidance from federal policy authorities such as circulars and memoranda from OMB. The contractor shall keep the privacy office informed of all new privacy issues, topics, policy, and guidance in a timely manner. The contractor shall develop and deliver to the TM for review and approval any required guidance and memoranda on new privacy requirements, topics, and issues.

C.3.4.8.3 Policy Changes. The contractor shall work with SEC personnel to develop or update internal and web-based privacy policies, procedures, standards, and guidelines based on new federal legislation, regulations,

policies, standards, and guidelines to serve as the foundation of SEC privacy practices. The contractor shall update the documents as required by new guidelines. The contractor shall deliver these documents to the TM for review and approval.

The draft SECR 31-1 policy was initially submitted to the IRM branch in March 2007, per OIT policy review process, and changed hands in IRM in September 2007 due to at that time, the OIT Policy Manager leaving the SEC. This resulted in several internal iterations of the draft SECR 31-1. Subsequently and pursuant to OMB Memo 07-16, additional draft policies were submitted to IRM for review. These included policies for breach notification (Privacy Incident Management); Reduction of SSNs; and Rules of Conduct for Safeguarding PII.

On the dates listed below, OIT issued the following policy documents for external reviews.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The OED provided comments to the SECR 24.08 Privacy Program on December 8, 2008, which resulted in the restructuring of the privacy tiered framework and essentially redrafting the SECR. As a result of the redrafted SECR, policy provisions for Use and Reduction of SSNs and Rules of Conduct were

incorporated into the draft SECR. The privacy office met with the OED and discussed their comments and plans to revise policy at the agency. Based on that meeting and written comments, another draft SECR with attachments was

provided to OED on March 31, 2009. The OED requested clarification, and in some instances, additional information such as sources of definitions. The OED then restructured the outline of the document and edited/added content, and provide to OIT a rewrite of the SECR on November 17, 2009, including renaming the SECR to Management and Protection of Privacy Act Records and other PII. The draft OD, Privacy Incident Management is still under OED review.²

There have been incidents of lost PII consisting of both [REDACTED] that were stored on [REDACTED]

[REDACTED] Without having formal, approved privacy program policies and procedures implemented throughout the Commission, the loss of PII is very significant and a real problem.

Recommendation 1:

The Office of Information Technology should finalize its outstanding draft privacy related policies and procedures and implement them throughout the agency by the end of the fiscal year.

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that OIT has concurred with this recommendation.

² Since the submission of the responses to the FISMA questionnaires, a draft policy was submitted on December 17, 2009 for external and internal OIT management review with a January 18, 2010 comment due date.

Acronyms

CIO	Chief Information Officer
CPO	Chief Privacy Officer
FISMA	Federal Information Systems Management Act
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PAW	Privacy Analysis Worksheet
PIA	Privacy Impact Assessment
PII	Personally Identifying Information
PIRT	Privacy Incident Response Team
SAOP	Senior Agency Official for Privacy
SEC or Commission	Securities and Exchange Commission
SORN	System of Records Notice
SSN	Social Security Number

Scope and Methodology

This evaluation was not conducted in accordance with government auditing standards.

Scope. The scope of this effort was an evaluation of the SEC Privacy Program.

Methodology. The objective to examine the SEC's implementation of information technology and related processes for the agency's privacy program, training, policies and procedures on handling privacy information, etc., was accomplished by conducting interviews with key personnel, making independent observations, and evaluating and examining support documentation that was provided.

Interviews with key personnel included systems owners, business line managers, OIT representatives, and OIG personnel. Personnel were interviewed regarding the issues germane to completing an evaluation of the SEC Privacy Program. Interview areas discussed included:

- Privacy program and privacy impact assessments;
- Privacy policies and procedures; and
- PII incidents and incident response.

C5i also reviewed an extensive collection of system artifacts, policies, and other documentation relating to the systems and issues that were identified.

Internal Controls. We reviewed the existing controls that were considered significant for FISMA and within the context of the Privacy program and the assessment objectives.

Prior Audit Coverage. We conducted an assessment of the Commission's FISMA program in 2008. The review looked at the FISMA major security areas as well as performed an assessment of two of the Agencies information systems; the Complaints/Tips/Referrals, and the Office of Compliance Inspections and Examinations, Adviser Surveillance Intelligence System applications. The report contained three recommendations and revealed that there were no significant issues with the systems however we found some problems with the overall security program as it related to the Commission completing security control and contingency testing for some systems. We also identified a problem with the Commission's implementation of the requirements for Federal Core Desktop Configuration.

Criteria

OMB Memorandum M-09-29, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. This memorandum provides instructions for meeting agency FY 2009 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347). It also includes reporting instructions for agency privacy management programs.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)*. This memorandum requires agencies to develop and implement a breach notification policy. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974.

OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006)*. This memorandum provides updated guidance on the reporting of security incidents involving personally identifiable information and to remind you of existing requirements, and explain new requirements your agency will need to provide addressing security and privacy in your fiscal year 2009 budget submissions for information technology).

OMB Memorandum M-06-16, *Protection of Sensitive Agency Information (June 23, 2006)*. This memorandum recommends a number of actions necessary to protect sensitive information.

OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information (May 22, 2006)*. This memorandum reemphasizes agency responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and to train employees on their responsibilities.

OMB Memorandum M-03-22, *Guidance for Implementing Privacy Provisions of the E-Government Act of 2002 (September 30, 2003)*. This memorandum provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

List of Recommendations

Recommendation 1:

The Office of Information Technology should finalize its outstanding draft privacy related policies and procedures and implement them throughout the agency by the end of the fiscal year.

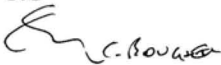
Management Comments



Memorandum

Date: March 9, 2010

To: David Kotz, Inspector General, OIG
Jacqueline Wilson, Assistant Inspector General, OIG

From : Charles Boucher, Chief Information Officer, OIT 

Subject: Management Response to OIG Report 475, *Evaluation of the SEC Privacy Program*

The Office of Information Technology appreciates the opportunity to comment on the subject report. We are pleased that the OIG "found that the SEC is currently developing a privacy program that will include the appropriate controls and guidance mandated in the National Institute of Standards and Technology and OMB documents" and that "the SEC Privacy Program and PIA [Privacy Impact Assessment] process will be fully implemented with finalizing and approving draft SEC Regulation (SECR) 24-08". We concur with the one recommendation in the report, which is to finalize that regulation.

OIG Response to Management's Comments

We are pleased that OIT concurred with the report's recommendation and intends to finalize and issue policies and procedures that will allow them to manage and operate the privacy program with appropriately needed internal controls, privacy controls and oversight.

Audit Requests 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