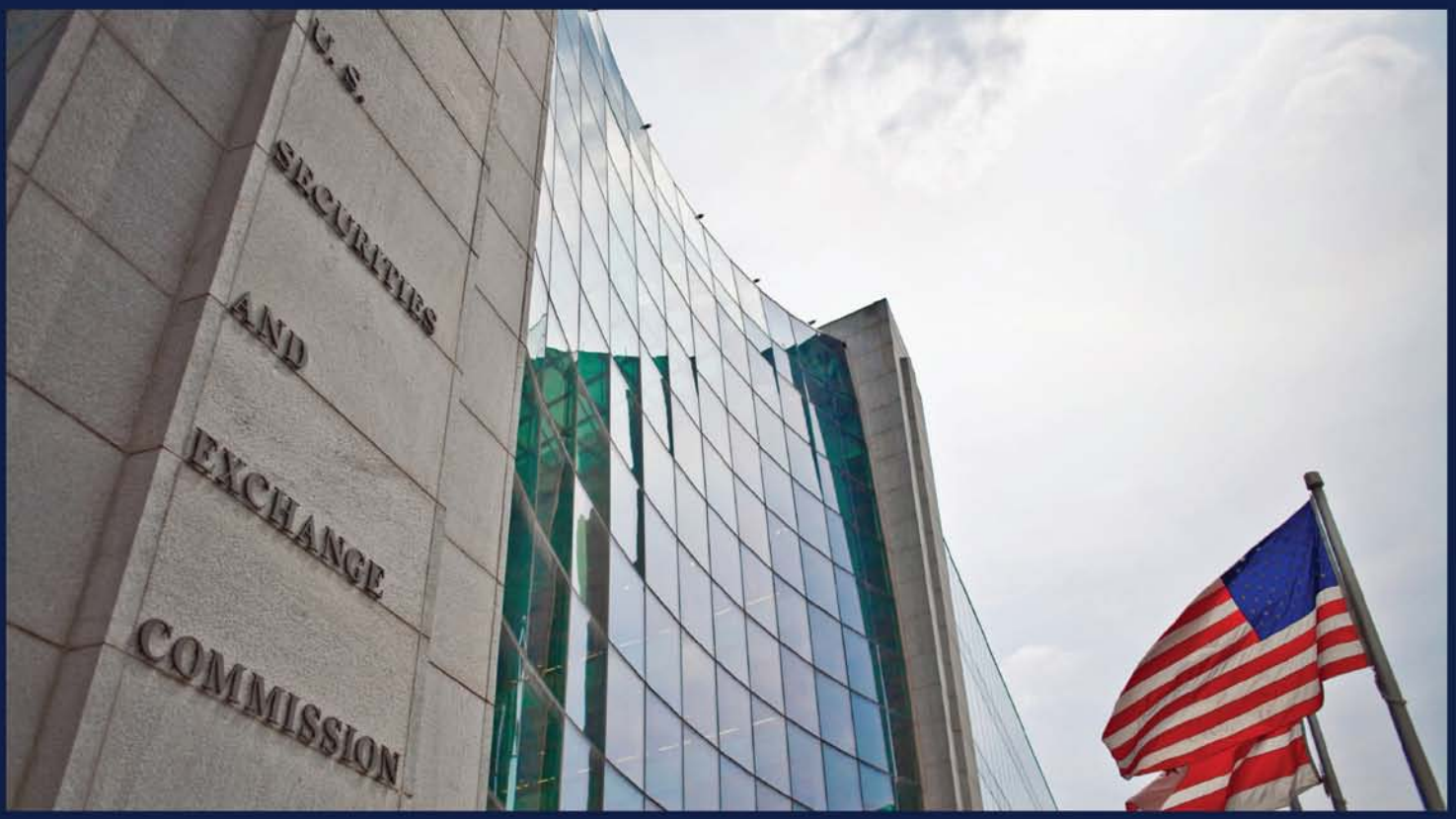
U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Review of SEC Contracts for Inclusion of Language Addressing Privacy Act Requirements



July 18, 2011
Report No. 496

Review Conducted by C5i Federal, Inc.

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

July 18, 2011

To: Jayne L. Seidman, Acting Associate Chief Operating Officer, Office of Administrative Services (OAS)

Thomas Bayer, Chief Information Officer, Office of Information Technology (OIT)

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

Subject: *Review of SEC Contracts for Inclusion of Language Addressing Privacy Act Requirements*, Report No. 496

This memorandum transmits the U.S. Securities and Exchange Commission's Office of Inspector General's (OIG's) final report on the OIG's review of SEC contracts for inclusion of language that addresses privacy act requirements. The report contains two recommendations which if implemented should strengthen OAS's contract oversight. We are pleased your offices concurred with both recommendations. Your written response to the draft report is included in Appendix IV.

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

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

Attachment

cc: James R. Burns, Deputy Chief of Staff, Office of the Chairman
Luis A. Aguilar, Commissioner
Troy A. Paredes, Commissioner
Elisse B. Walter, Commissioner
Kathleen L. Casey, Commissioner
Jeff Heslop, Chief Operating Officer, Executive Director, Office of Chief of Operations
Todd Scharf, Chief Information Security Officer, Office of Information Technology

Review of SEC Contracts for Inclusion of Language Addressing Privacy Act Requirements

Background

In August 2010, the U.S. Securities and Exchange Commission (SEC or Commission), Office of Inspector General (OIG), contracted with C5i Federal, Inc. (C5i), for assistance in completing and coordinating the OIG's input to the Commission's response to Office of Management and Budget (OMB) Memorandum M-10-15, fiscal year (FY) 2010 Reporting Instructions for the Federal Information Security Management Act (FISMA) and agency privacy management,[1] and to perform two additional FISMA-related reviews. One of these additional reviews addresses the SEC's Continuous Monitoring Program.[2] This report presents the results of the other review, which addresses whether SEC contracts contain appropriate language addressing Privacy Act requirements, including provisions for protecting SEC personally identifiable information (PII).[3]

Subsection (m)(1) of the Privacy Act of 1974 provides that when an agency contracts for the operation of a system of records to accomplish an agency function, the agency must include in the terms of the contract provisions making the contractor responsible for complying with the Privacy Act. It also makes these contractors liable under the criminal provisions of the Act.[4] SEC Administrative Regulation 24-08 (SECR 24-08) establishes policy for the Commission's privacy program, including the protection of PII that is collected by the SEC. SECR 24-08 applies not only to SEC employees, but also to contractors and others working on behalf of the SEC who handle, control, or have access to information, documents, or systems that contain PII.[5]

In conducting this assessment, C5i reviewed a judgment sample consisting of 11 SEC contracts that included language requiring the contractors to handle SEC PII. C5i also reviewed the results of the SEC's FY 2010 Section (m) Contracts Compliance Review memorandum, which contains the results of the SEC Privacy

[1] OIG, *2010 Annual FISMA Executive Summary Report,* Report No. 489 (Mar. 3, 2011).
[2] OIG, *Assessment of the SEC's Continuous Monitoring Program*, Report No. 497 to be issued in late July 2011.
[3] In August 2010, the SEC's Ethics and Compliance Employee Hotline received a call expressing concern over the handling of PII by third-party vendors during the disgorgement process. This assessment does not specifically describe the assessment of the handling of PII by third-party vendors engaged to administer disgorgements because: (1) the complaint was not found to be substantiated and (2) most disgorgements are administered by court-appointed third-party vendors who are not under contract with the SEC.
[4] 5 U.S.C. § 552a(m)(1).
[5] SECR 24-08, Management and Protection of Privacy Act Records and Other Personally Identifiable Information (Apr. 14, 2010), p. 1.

Office's review of eight randomly selected SEC contracts for compliance with Privacy Act requirements.

Objective

The objective of this review was to determine whether the Securities and Exchange Commission's contracts contain appropriate language addressing Privacy Act requirements.

Finding 1: OAS's Contracts Contain Appropriate Language Addressing Privacy Act Requirements

C5i reviewed a judgment sample consisting of 11 SEC contracts that included language requiring vendors to handle SEC PII. The sample contained employee recruitment, financial systems management, and information technology contracts. C5i found that each of the contracts in the sample contained the appropriate sections addressing such requirements as nondisclosure agreements, system security, and PII protection.

C5i also reviewed the results of the SEC's FY 2010 Section (m) Contracts Compliance Review memorandum, dated November 3, 2010, which details the results of the SEC Privacy Office's review of eight randomly selected SEC contracts for compliance with Privacy Act requirements. The review concluded that all sampled contracts included language binding vendors to the requirements of the Privacy Act. C5i examined 6 additional contracts to verify that they contained the appropriate provisions required by the Privacy Act for nondisclosure agreements, background investigations of personnel, PII handling, and security of systems. C5i found that the contracts did include such provisions and therefore concurs with the conclusions of the FY 2010 Section (m) Contracts Compliance Review Memorandum.

Although C5i's assessment found that the SEC's contracts contain language requiring that vendors and their employees comply with the Privacy Act, strengthening the language in SEC contracts that pertains to privacy and information might help to ensure vendors' compliance with those provisions. For example, new contracts could include provisions requiring vendors to provide copies of their privacy policies, privacy impact assessments, and evidence that their systems have been certified and accredited consistent with industry best practices. New contracts and interconnectivity agreements could also include provisions requiring that security requirements defined by the Office of Information Technology (OIT) are achieved for PII data transmitted over public networks or stored on portable medial. Including such provisions could further reduce the risk that PII will be mishandled.

Recommendation 1:

The Office of Administrative Services should add language provided by the Office of Information Technology to new service contracts that require the handling of PII data stating that the U.S. Securities and Exchange Commission requires the contractor to provide copies of the contractor's privacy policies and privacy impact assessments.

Management Comments. OAS and OIT concurred with this recommendation. See Appendix IV for management's full comments.

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

Recommendation 2:

The Office of Administrative Services should add Office of Information Technology-defined security requirements to applicable contracts stating that contractors handling electronic personally identifiable information (PII) data may be required to meet defined security requirements when transmitting PII data across public networks (i.e., Internet) or stored on portable media. The Office of Information Technology should also add language to applicable interconnectivity agreements stating that partners transmitting electronic PII data across public networks (i.e., Internet) are required to meet the Office of Information Technology-defined security requirements.

Management Comments. OAS and OIT concurred with this recommendation. See Appendix IV for management's full comments.

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

Abbreviations/Acronyms

FY	fiscal year
OIG	Office of Inspector General
OMB	Office of Management and Budget
OIT	Office of Information Technology
PII	personally identifiable information
SEC or Commission	U.S. Securities and Exchange Commission

Scope and Methodology

Scope. Initially the scope of this review was to review the handling of PII by third-party vendors during the disgorgement process. This review was initiated because of concerns raised in an anonymous call to the Ethics and Compliance Employee Hotline about mishandling of PII by third-party vendors during the disgorgement process. Following a review of the disgorgement process and interviews with SEC Enforcement Division staff, C5i learned that the SEC is not a party to contracts with third-party vendors appointed by courts to process disgorgements and therefore has no liability related to PII in such cases. Therefore, the scope of work was modified and limited to a review of the disgorgement process and a sample of SEC contracts to determine whether they included language that bound vendors to comply with the Privacy Act.

Methodology. C5i reviewed a judgmental sample of 11 contracts to determine whether they included appropriate language related to the Privacy Act; the results of a Privacy Office review of contracts to determine whether they included provisions required by the Privacy Act, including provision for the protection of PII; and documentation provided by the Enforcement Division detailing disgorgement processes and procedures. We relied on information requested from and supplied by the Enforcement Division and on interviews with Enforcement Division staff to understand the division's policies, methods of operation, and procedures with respect to disgorgements. C5i also interviewed staff in the Office of Administrative Services and the Privacy Office concerning contracting procedures and which Privacy Act provisions were required to be included in contracts.

Use of Computer-Processed Data. C5i used data provided in an Excel spreadsheet by the Enforcement Division that showed disgorgements processed in FYs 2009 and 2010.

Recent OIG Reports Addressing Privacy-Related Issues. The following OIG reports also address privacy-related issues:

- OIG Report No. 489, *2010 Annual FISMA Executive Summary Report*, issued on March 3, 2011, which contained eight recommendation to strengthen the Commission's security posture.

- OIG Report No. 485, *Assessment of the SEC's Privacy Program*, issued on September 29, 2010, which contained 20 recommendations to strengthen and improve the Commission's security posture for protecting PII.

- OIG Report No. 476, *Evaluation of the SEC Encryption Program*, issued on March 26, 2010, which contained three recommendations to strengthen information technology management controls for safeguarding the Commission's information.

- OIG Report No. 475, *Evaluation of the SEC Privacy Program*, issued on March 26, 2010, which contained one recommendation to manage and operate the privacy program with appropriate internal controls, privacy controls, and oversight.

Criteria

Privacy Act of 1974, subsection (m)(1). Statutory provision requiring that when an agency contracts for the operation of a system of records to accomplish an agency function, the agency must include in the terms of the contract provisions making the contractor responsible for complying with the Privacy Act.

SEC Administrative Regulation 24-08, April 14, 2010. Internal policy document that establishes agencywide policy for the Commission's privacy program, including protection of PII collected by the SEC. It applies to all SEC employees, contractors, interns, and other working on behalf of the SEC who handle, control, or access information or systems that contain PII or records subject to the Privacy Act.

Management's Comments

MEMORANDUM

July 15, 2010

To: H. David Kotz
Inspector General
Office of Inspector General

From: Jayne L. Seidman
Acting Associate Chief Operating Officer
Office of Administrative Services

Subject: OAS Response to OIG Draft Audit *Review of SEC Contracts for Inclusion of Language Addressing Privacy Act Requirements*, Report No. 496

Thank you for the opportunity to review and comment.

Recommendation 1:

The Office of Administrative Services (OAS) should add language provided by the Office of Information Technology to new service contracts that require the handling of PII data stating that the U.S. Securities and Exchange Commission requires the contractor to provide copies of the contractor's privacy policies and privacy impact assessments.

OAS concurs. OA will include in new service contracts the language provided by the Office of Information Technology.

Recommendation 2:

The Office of Administrative Services should add Office of Information Technology-defined security requirements to applicable contacts stating that contractors handling electronic personally identifiable information (PII) data may be required to meet defined security requirements when transmitting PII data across public networks (i.e. Internet) or stored on portable media. The Office of Information Technology should add language to applicable interconnectivity agreements (IAA) stating that partners transmitting electronic PII data across public networks (i.e. Internet) are required to meet the Office of Information Technology-defined security requirements.

OAS concurs. OA will include the security requirements defined by the Office of Information Technology in applicable contracts.

MEMORANDUM

July 14, 2011

TO: H. David Kotz, Inspector General
Office of Inspector General (OIG)

Jacqueline Wilson, Assistant Inspector General for Audits
Office of Inspector General

FROM: Thomas A. Bayer, Chief Information Officer
Office of Information Technology (OIT)

SUBJECT: OIT's Response to the OIG Draft Report No. 496, *Review of SEC Contracts for Inclusion of Language Addressing Privacy Act Requirements*

This memorandum is in response to the Office of Inspector General Draft Report No. 496, *Review of SEC Contracts for Inclusion of Language Addressing Privacy Act Requirements.* Thank you for the opportunity to review and respond to this report.

Recommendation 1

The Office of Administrative Services (OAS) should add language provided by the Office of Information Technology to new service contracts that require the handling of PII data stating that the U.S. Securities and Exchange Commission requires the contractor to provide copies of the contractor's privacy policies and privacy impact assessments.

OIT concurs with this recommendation and will provide to OAS language regarding privacy policies and privacy impact assessments for inclusion in new service contracts that require the handling of PII data.

Recommendation 2

The Office of Administrative Services should add Office of Information Technology-defined security requirements to applicable contacts stating that contractors handling electronic personally identifiable information (PII) data may be required to meet defined security requirements when transmitting PII data across public networks (i.e. Internet) or stored on portable media. The Office of Information Technology should add language to applicable interconnectivity agreements (IAA) stating that partners transmitting electronic PII data across public networks (i.e. Internet) are required to meet the Office of Information Technology-defined security requirements.

OIT concurs with this recommendation and will provide to OAS language regarding specific security requirements for inclusion in applicable contracts. In addition, OIT will add language regarding specific security requirements to its IAA related to transmitting electronic PII.

OIG Response to Management's Comments

We are pleased that OAS and OIT have concurred with the report's two recommendations. We are also encouraged that OAS and OIT have indicated that they will work together to implement the recommendations and that they have already taken steps to implement the recommendations. We believe that OAS and OIT's proposed actions are responsive to the report's findings and recommendations.

Once both recommendations are fully implemented, we believe the SEC's security posture will be strengthened, and contractors wanting to conduct business with the agency will be fully aware of the SEC's expectations for adequately protecting Commission data.

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

Telephone: 202-551-6061
Fax: 202-772-9265
E-mail: oig@sec.gov

Hotline

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

Telephone: 877.442.0854

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