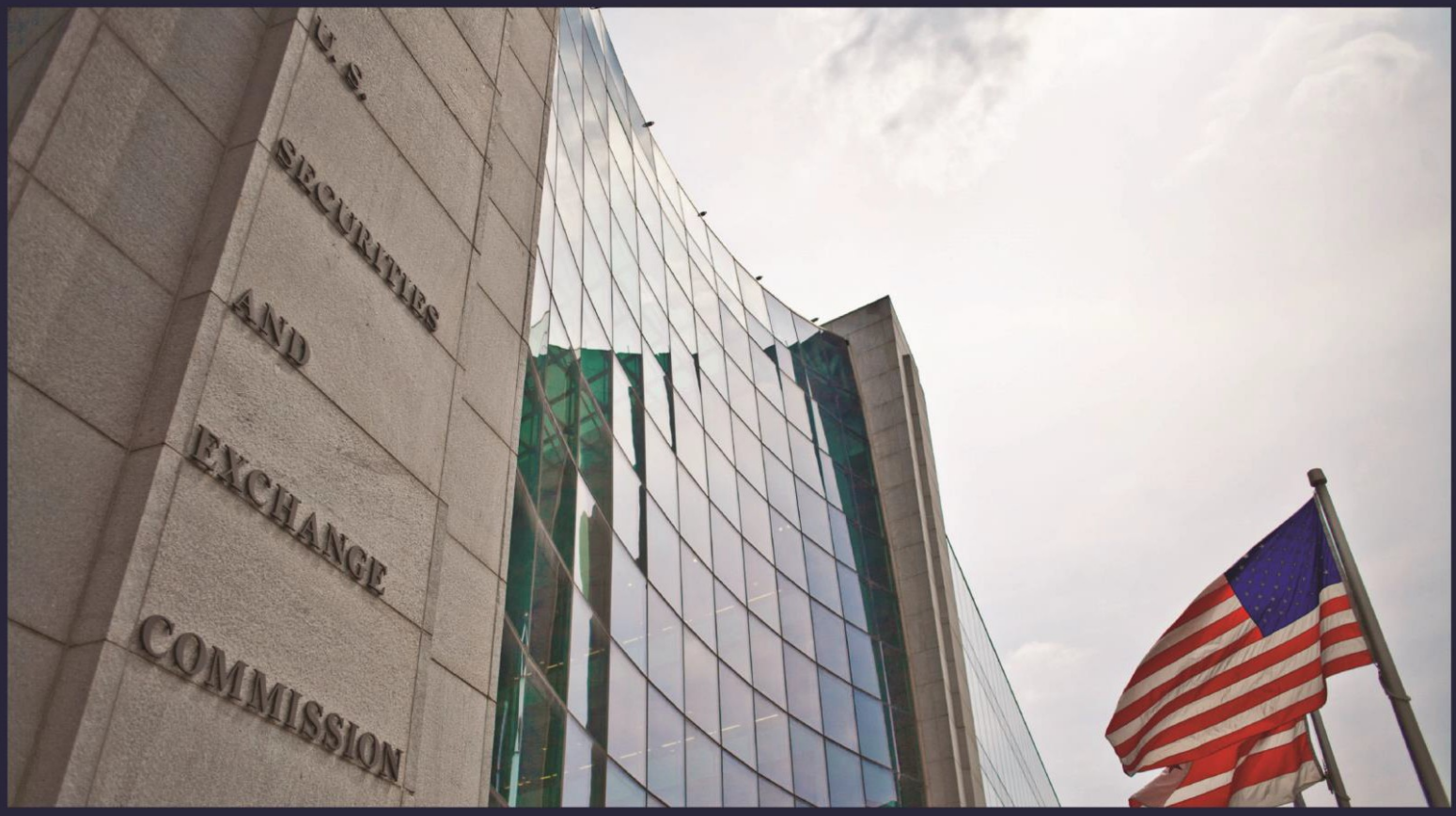
U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015



June 2, 2016
Report No. 535

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

June 2, 2016

TO: Jeffrey Heslop, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015,* Report No. 535

Attached is the Office of Inspector General's (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC) compliance with the Federal Information Security Modernization Act for Fiscal Year 2015. To improve the SEC's information security program, we urge management to take action on all outstanding recommendations from prior year evaluations and areas of potential risk identified in this report. In addition, the report contains four new recommendations for corrective action that, if fully implemented, should strengthen the SEC's information security posture.

On May 19, 2016, we provided management with a draft of our report for review and comment. In its May 24, 2016, response, management concurred with our recommendations. We have included management's response as Appendix III in the final report.

Within the next 45 days, please provide the OIG with a written corrective action plan that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing required actions, and milestones identifying how the Office of Information Technology will address the recommendations.

We appreciate the courtesies and cooperation extended to us during the audit. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Mary Jo White, Chair
Andrew Donohue, Chief of Staff, Office of the Chair
Michael Liftik, Deputy Chief of Staff, Office of the Chair
Nathaniel Stankard, Deputy Chief of Staff, Office of the Chair
Michael S. Piwowar, Commissioner
Jaime Klima, Counsel, Office of Commissioner Piwowar

Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Anne K. Small, General Counsel
Keith Cassidy, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Pamela C. Dyson, Director/Chief Information Officer, Office of Information Technology
Andrew Krug, Associate Director/Chief Information Security Officer, Office of Information Technology
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Executive Summary

Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015
Report No. 535
June 2, 2016

Why We Did This Audit

The U.S. Securities and Exchange Commission's (SEC or agency) information systems process and store significant amounts of sensitive, nonpublic information including information that is personally identifiable, commercially valuable, and market-sensitive. The SEC's information security program protects the agency from the risk of unauthorized disclosure, modification, use, and disruption of this sensitive, nonpublic information. Without these controls, the agency's ability to accomplish its mission could be inhibited, and privacy laws and regulations that protect such information could be violated. To comply with the Federal Information Security Modernization Act of 2014 (FISMA), the SEC Office of Inspector General, with assistance from a contracting firm, Wingate, Carpenter, and Associates, P.C., assessed the SEC's implementation of FISMA information security requirements.

What We Recommended

To improve the SEC's information security program, we urge management to take action on all outstanding recommendations from prior year evaluations and areas of potential risk identified in this report. We also made four new recommendations that address (a) support for risk-based decisions, (b) OIT Risk Committee functionality, and (c) configuration management requirements. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. Because this report contains sensitive information about the SEC's information security program, we are not releasing it publicly.

What We Found

The SEC's Office of Information Technology (OIT) has overall management responsibility for the SEC's information technology program, including information security. Since last year, OIT improved in key information security program areas, including implementing personal identity verification to the maximum extent practicable, establishing multi-factor authentication for external systems, and improving identity and access management. However, we found that:

- OIT's risk management program did not effectively monitor risks associated with system authorizations; and
- OIT's configuration management program did not ensure that system owners adhered to baseline configuration requirements.

These weaknesses existed, in part, because OIT management did not (1) effectively implement the OIT Risk Committee tasked with managing risk from individual information systems, and (2) establish adequate controls to ensure effective and consistent implementation of OIT's risk and configuration management programs.

In addition, OIT had not fully addressed some areas of potential risk identified in prior Federal Information Security Management Act evaluations. Specifically, SEC systems continued to operate without current authorizations; user accounts were not always deactivated in accordance with policy; continuous monitoring review procedures were developed, but not consistently implemented; and some policies and procedures remained outdated or inconsistent. As a result, these areas continued to pose potential risk to the agency.

Finally, we identified three other matters of interest related to the agency's information technology environment. Specifically, we determined that the SEC did not always (1) update Business Impact Analyses to reflect major system changes, (2) update contingency planning documents to reflect changes in alternate site locations, or (3) track security awareness training. We encourage OIT management to consider these matters and ensure that sufficient controls exist.

For additional information, contact the Office of Inspector General at (202) 551-6061 or http://www.sec.gov/oig.

To Report Fraud, Waste, or Abuse, Please Contact:

Web: www.reportlineweb.com/sec_oig

Telephone: (877) 442-0854

Fax: (202) 772-9265

Address: U.S. Securities and Exchange Commission
Office of Inspector General
100 F Street, N.E.
Washington, DC 20549

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, please contact Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects at sharekr@sec.gov or call (202) 551-6061. Comments, suggestions, and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed above.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu