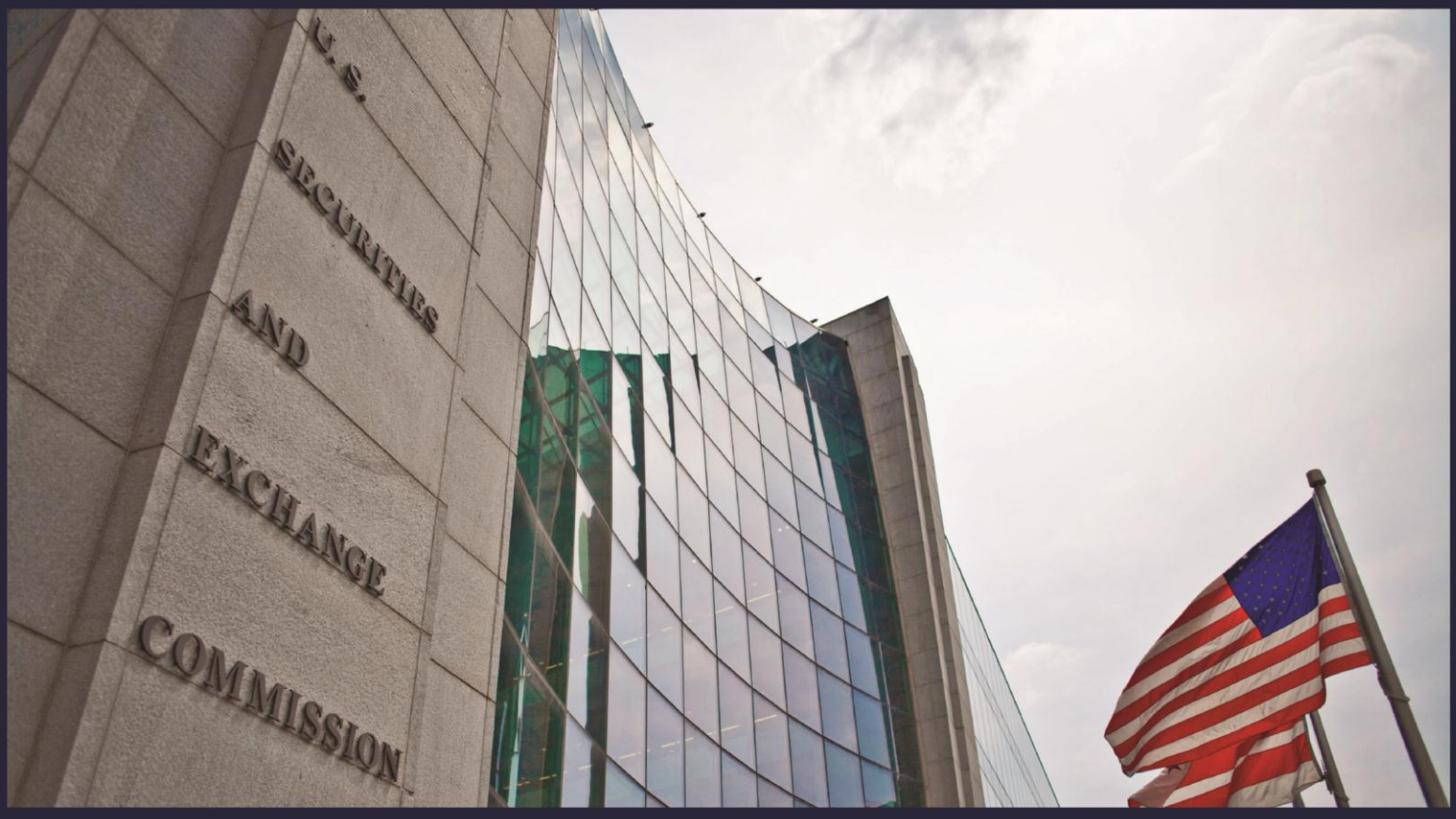
U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Review of the SEC's Practices for Sanitizing Digital Information System Media



May 30, 2014
Report No. 521

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

May 30, 2014

To: Thomas A. Bayer, Chief Information Officer, Office of Information Technology

From: Carl W. Hoecker, Inspector General, Office of Inspector General

Subject: *Review of the SEC's Practices for Sanitizing Digital Information System Media,* Report No. 521

Attached is the Office of Inspector General's (OIG) final report detailing the results of our review of the U.S. Securities and Exchange Commission's (SEC) practices for sanitizing digital information system media (media). The report contains eight recommendations for corrective action that, if fully implemented, should strengthen the SEC's media sanitization controls.

On April 30, 2014, we provided you with a draft of our report for your review and comment. In your May 21, 2014, response, you concurred with all of our recommendations. We have included your response as Appendix IV 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 your office will address the recommendations.

We appreciate the courtesies and cooperation extended to us during the review. 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
Erica Y. Williams, Deputy Chief of Staff, Office of the Chair
Luis A. Aguilar, Commissioner
Paul Gumagay, Counsel, Office of Commissioner Aguilar
Daniel M. Gallagher, Commissioner
Benjamin Brown, Counsel, Office of Commissioner Gallagher
Kara M. Stein, Commissioner
Tyler Gellasch, Counsel, Office of Commissioner Stein
Michael S. Piwowar, Commissioner
Jaime Klima, Counsel, Office of Commissioner Piwowar

Jeffery Heslop, Chief Operating Officer
Anne K. Small, General Counsel
Timothy Henseler, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Public Affairs
Pamela Dyson, Deputy Director, Office of Information Technology
Todd Scharf, Associate Director, Chief Information Security Officer
Barry Walters, Director, Office of Support Operations/Chief FOIA Officer
Olivier Girod, Chief, Office of Building Operations
Vance Cathell, Director, Office of Acquisitions
David Glockner, Regional Director, Chicago Regional Office
Barry Isenman, Assistant Director, Chicago Regional Office
Andrew Calamari, Regional Director, New York Regional Office
Robert Keyes, Associate Regional Director, New York Regional Office
Sharon Binger, Regional Director, Philadelphia Regional Office
Edward Fallacro, Chief of Regional Office Operations, Philadelphia Regional Office
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Executive Summary

Review of the SEC's Practices for Sanitizing Digital Information System Media
Report No. 521
May 30, 2014

Why We Did This Review

The U.S. Securities and Exchange Commission (SEC) generates and collects commercially valuable, market-sensitive, proprietary, and other nonpublic information. To safeguard against unauthorized disclosure of this information, the SEC requires that digital information system media (media), including computer hard drives, compact discs, digital video discs, and data tapes used to process and store information, be sanitized before disposal. Effective sanitization minimizes the risk of unauthorized release of information that is potentially damaging to the agency, its employees and contractors, and those entities that the SEC regulates. To determine whether the SEC effectively sanitizes surplus media before its disposal, the Office of Inspector General contracted the services of Networking Institute of Technology, Inc. (referred to as "we" in this report) to evaluate the agency's media sanitization practices.

What We Recommended

To provide reasonable assurance that the SEC's obsolete and surplus media containing sensitive information are properly safeguarded and sanitized before disposal, we made eight recommendations for corrective action. The recommendations address surplus media storage, laptop encryption, inventorying and tracking of surplus hard drives, sanitization of failed hard disks used in disk arrays, certificates of destruction, media sanitization policies and procedures, and implementation of verification activities. 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 Office of Information Technology (OIT) sanitizes surplus and obsolete media by destroying it, which minimizes the risk of unauthorized disclosure of information. However, we visited the SEC's Washington, D.C., headquarters and three of the agency's regional offices (Philadelphia, New York, and Chicago) and identified needed improvements in the agency's sanitization and disposal practices. Specifically, we found that the SEC did not always

- store media awaiting sanitization, particularly surplus hard drives, in secure containers or cabinets to prevent pilferage;
- encrypt laptop computer hard drives, although encryption is required and unencrypted laptop computer hard drives awaiting sanitization were found to contain large amounts of nonpublic information, including personally identifiable information;
- inventory or track hard drives during the sanitization process; and
- sanitize failed disks that were part of the agency's data center redundant storage arrays before returning such disks to a vendor.

We also determined that SEC employees did not always witness the third-party destruction of media or obtain accurate or complete certificates of destruction.

After issuing to management a discussion draft of our report highlighting these results, we learned that the OIT, on April 7, 2014, rescinded its *Media Destruction Procedure* and revised its *SEC OIT Security Policy Framework* and accompanying handbook. Those documents established many of the media sanitization and disposal requirements that agency personnel were not consistently following.

We communicated to the OIT our concern that those changes eliminated previously established controls over media sanitization and disposal rather than ensure that such controls were working effectively. Subsequently, the OIT agreed to reestablish some requirements to address the weaknesses we observed. Those weaknesses existed because of a lack of clear lines of authority and roles and responsibilities for media sanitization. Also, the OIT did not adequately oversee agencywide sanitization and disposition processes, including those of the regional offices. In addition, responsible personnel did not consistently follow or were unaware of applicable policies and procedures. Finally, there were no enforcement or compliance controls in place to detect and prevent the weaknesses we observed. According to management's response to the draft of our report, the OIT is reviewing its *Media Destruction Procedure* and intends to replace it with multiple procedures addressing media sanitization.

During the course of our review, we also found on the SEC's enterprisewide network drives large amounts of sensitive, nonpublic information that was available to all employees and contractors with access to the network. Upon notification, management restricted access to the drives, pending further review by the OIT.

For additional information, contact the Office of Inspector General at (202) 551-6061 or www.sec.gov/about/offices/inspector_general.shtml.

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

Web: www.reportlineweb.com/sec_oig

Email: oig@sec.gov

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 20549-2736

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 Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects at sharekr@sec.gov or call (202) 551-6083. 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.