Executive Summary

Report No. 522
March 31, 2014

Why We Did This Evaluation
The Federal Information Security Management Act (FISMA) provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. FISMA also requires agency Inspectors General to annually assess the effectiveness of agency information security programs and practices and report the results to the Office of Management and Budget (OMB). The overall objective of the fiscal year 2013 FISMA evaluation was to assess the U.S. Securities and Exchange Commission’s (SEC) information systems and information security posture. The Office of Inspector General contracted the services of Networking Institute of Technology, Inc. (referred to as "we" in this executive summary) to conduct the evaluation.

What We Found
To assess the SEC's security controls over its information systems and information security posture, we reviewed the security assessment packages for seven of the SEC's major information systems (five internally hosted systems and two externally hosted systems). The scope of the review consisted of the following 11 areas specified in OMB's fiscal year 2013 FISMA reporting instructions:

1. continuous monitoring management;
2. configuration management;
3. identity and access management;
4. incident response and reporting;
5. risk management;
6. security training;
7. plan of action and milestones;
8. remote access management;
9. contingency planning;
10. contractor systems; and
11. security capital planning.

Overall, we found several areas in which the SEC has implemented improved controls over its information security. For example, the Office of Information Technology (OIT) has made significant progress establishing (1) a risk management program; (2) an incident response and reporting program; and (3) an enterprise-wide business continuity and disaster recovery program, consistent with FISMA requirements and OMB and National Institute of Standards and Technology guidelines. The OIT has also established a plan of action and milestones program and properly tailors its baseline control list in compliance with Federal guidance. Finally, the SEC provided, to its personnel, security awareness and role-based security training and has established an information security capital planning and investment program.

However, we found that the OIT had not taken corrective action on some issues identified during the fiscal year 2011 and 2012 FISMA evaluations. We also found that the agency needs to enhance its efforts regarding contractor systems, multi-factor authentication, user accounts, and configuration management.

What We Recommended
To strengthen the SEC's controls over information security, we reiterated that the OIT should take immediate action to address the outstanding recommendations from the fiscal year 2011 and 2012 FISMA reports. We also made nine new recommendations for corrective action. In response to a draft of this report, SEC management concurred with eight of the nine recommendations and nonconcurred with one recommendation. Management described corrective actions that they plan to take.

Because this report contains sensitive information about the SEC's information security program, we are not releasing it publicly.

For additional information, contact the Office of Inspector General at (202) 551-6061 or visit www.sec.gov/about/offices/inspector_general.shtml.
To Report Fraud, Waste, or Abuse, Please Contact:

Web: www.reportlineweb.com/sec_oig

E-mail: 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 executive summary 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.