April 2014

INFORMATION SECURITY

SEC Needs to Improve Controls over Financial Systems and Data

GAO Highlights

Highlights of GAO-14-419, a report to the Chair, U.S Securities and Exchange Commission

Why GAO Did This Study

SEC is responsible for enforcing securities laws, issuing rules and regulations that protect investors, and helping to ensure that securities markets are fair and honest. In carrying out its mission, the commission relies extensively on computerized systems that collect and process financial and sensitive information. Accordingly, it is essential that SEC have effective information security controls in place to protect this information from misuse, fraudulent use, improper disclosure, manipulation, or destruction.

As part of its audit of SEC's fiscal years 2013 and 2012 financial statements, GAO assessed the commission's information security controls. The objective was to determine the effectiveness of information security controls for protecting the confidentiality, integrity, and availability of SEC's key financial systems and information. To do this, GAO assessed security controls in key areas by reviewing SEC documents, testing selected systems, and interviewing relevant officials.

What GAO Recommends

GAO is recommending that SEC take two actions to (1) more effectively oversee contractors performing security-related tasks and (2) improve risk management. In a separate report for limited distribution, GAO is recommending that SEC take 49 specific actions to address weaknesses in security controls. In commenting on a draft of this report, SEC generally agreed with GAO's recommendations and described steps it is taking to address them.

View GAO-14-419.For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

Although the Securities and Exchange Commission (SEC) had implemented and made progress in strengthening information security controls, weaknesses limited their effectiveness in protecting the confidentiality, integrity, and availability of a key financial system. For this system's network, servers, applications, and databases, weaknesses in several controls were found, as the following examples illustrate:

- **Access controls:** SEC did not consistently protect its system boundary from possible intrusions; identify and authenticate users; authorize access to resources; encrypt sensitive data; audit and monitor actions taken on the commission's networks, systems, and databases; and restrict physical access to sensitive assets.
- **Configuration and patch management:** SEC did not securely configure the system at its new data center according to its configuration baseline requirements. In addition, it did not consistently apply software patches intended to fix vulnerabilities to servers and databases in a timely manner.
- **Segregation of duties:** SEC did not adequately segregate its development and production computing environments. For example, development user accounts were active on the system's production servers.
- **Contingency and disaster recovery planning:** Although SEC had developed contingency and disaster recovery plans, it did not ensure redundancy of a critical server.

The information security weaknesses existed, in part, because SEC did not effectively oversee and manage the implementation of information security controls during the migration of this key financial system to a new location. Specifically, during the migration, SEC did not (1) consistently oversee the information security-related work performed by the contractor and (2) effectively manage risk.

Until SEC mitigates control deficiencies and strengthens the implementation of its security program, its financial information and systems may be exposed to unauthorized disclosure, modification, use, and disruption. These weaknesses, considered collectively, contributed to GAO's determination that SEC had a significant deficiency in internal control over financial reporting for fiscal year 2013.