April 2016

INFORMATION SECURITY

Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data

GAO Highlights

Highlights of GAO-16-493, a report to the Chair, U.S. Securities and Exchange Commission

Why GAO Did This Study

The SEC is responsible for enforcing securities laws, issuing rules and regulations that provide protection for investors, and helping to ensure that the securities markets are fair and honest. In carrying out its mission, the SEC relies on computerized information systems to collect, process, and store sensitive information, including financial data. Having effective information security controls in place is essential to protecting these systems and the information they contain.

This report details weaknesses GAO identified in the information security program at SEC during its audit of the commission's fiscal years 2015 and 2014 financial statements. GAO's 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 examined information security policies, plans, and procedures; tested controls over key financial applications; interviewed agency officials; and assessed corrective actions taken to address previously reported weaknesses.

What GAO Recommends

In addition to the 15 prior recommendations that have not been fully implemented, GAO is recommending that SEC take 6 additional actions to more fully implement its information security program. In a separate report with limited distribution, GAO recommended SEC take 30 actions to address newly identified control weaknesses. SEC concurred with GAO's recommendations.

View GAO-16-493. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wishuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The Securities and Exchange Commission (SEC) improved its information security by addressing weaknesses previously identified by GAO, including separating the user production network from the internal management network. However, weaknesses continue to limit the effectiveness of other security controls. In particular:

- While SEC had issued policies and implemented controls based on those policies, it did not consistently protect access to its systems. Organizations should design and implement controls to prevent, limit, and detect unauthorized access to computer resources. The commission did not consistently protect its network from possible intrusions, identify and authenticate users, authorize access to resources, audit and monitor actions taken on its systems and network, and restrict physical access to sensitive assets.
- The commission did not consistently manage the configuration of its systems. Configuration management includes ensuring that hardware and software are configured with appropriate security features and that changes are systematically controlled. However, SEC did not maintain and monitor official configuration baselines for its financial systems and general support system.
- The commission did not always appropriately separate incompatible duties. Separation of duties involves dividing responsibilities so that a single individual does not control all critical stages of a process. However, SEC did not adequately separate duties among its three computing environments.
- While SEC had developed contingency and disaster recovery plans for its information systems, those plans were not fully reviewed, completed, or up-to-date. Contingency and disaster recovery planning are essential to resuming operations in the event of a disruption or disaster.

These weaknesses existed in part because SEC had not fully implemented an organization-wide information security program, as called for by federal law and guidance. In particular, the commission had not (1) consistently reviewed and updated its information security policies in a timely manner, (2) completely documented plans of action to address weaknesses, (3) documented a physical inventory of its systems and applications, and (4) fully implemented a program to continuously monitor the security of its systems and networks.

Finally, of 20 weaknesses previously identified by GAO that remained unresolved as of September 30, 2014, SEC had resolved 5 and made progress in addressing the other 15 as of September 30, 2015. Two resolved weaknesses were important to improving SEC security.

Collectively, these weaknesses increase the risk that SEC's systems could be compromised, jeopardizing the confidentiality, integrity, and availability of sensitive financial information. While not constituting material weaknesses or significant deficiencies, they warrant SEC management's attention.