March 2009

INFORMATION SECURITY

Securities and Exchange Commission Needs to Consistently Implement Effective Controls

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-203, a report to the Chairman, Securities and Exchange Commission

Why GAO Did This Study

In carrying out its mission to ensure that securities markets are fair, orderly, and efficiently maintained, the Securities and Exchange Commission (SEC) relies extensively on computerized systems. Effective information security controls are essential to ensure that SEC's financial and sensitive information is protected from inadvertent or deliberate misuse, disclosure, or destruction.

As part of its audit of SEC's financial statements, GAO assessed (1) the status of SEC's actions to correct previously reported information security weaknesses and (2) the effectiveness of SEC's controls for ensuring the confidentiality, integrity, and availability of its information systems and information. To do this, GAO examined security policies and artifacts, interviewed pertinent officials, and conducted tests and observations of controls in operation.

What GAO Recommends

GAO recommends that SEC fully implement its information security program.

In commenting on a draft of this report, SEC agreed with GAO's recommendations and stated that it plans to address the identified weaknesses.

To view the full product, including the scope and methodology, click on GAO-09-203. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

SEC has made important progress toward correcting previously reported information security control weaknesses. Specifically, it has corrected or mitigated 18 of 34 weaknesses previously reported as unresolved at the time of our prior audit. For example, SEC has adequately validated electronic certificates from connections to its network, physically secured the perimeter of its operations center and put in place a process to monitor unusual and suspicious activities, and removed network system accounts and data center access rights from separating employees. In addition, the commission has made progress in improving its information security program. To illustrate, it has developed, documented, and implemented a policy on remedial action plans to ensure that deficiencies are mitigated in an effective and timely manner, and provided individuals with training for incident handling. Nevertheless, SEC has not completed actions to correct 16 previously reported weaknesses. For example, it did not adequately document access privileges granted to users of a key financial application, and did not always implement patches on vulnerable workstations and enterprise database servers.

In addition to the 16 previously reported weakness that remain uncorrected, GAO identified 23 new weaknesses in controls intended to restrict access to data and systems, as well as weaknesses in other information security controls, that continue to jeopardize the confidentiality, integrity, and availability of SEC's financial and sensitive information and information systems. The commission has not fully implemented effective controls to prevent, limit, or detect unauthorized access to computing resources. For example, it did not always (1) consistently enforce strong controls for identifying and authenticating users, (2) sufficiently restrict user access to systems (3) encrypt network services, (4) audit and monitor security-relevant events for its databases, and (5) physically protect its computer resources. SEC also did not consistently ensure appropriate segregation of incompatible duties or adequately manage the configuration of its financial information systems.

A key reason for these weaknesses is that the commission has not yet fully implemented its information security program to ensure that controls are appropriately designed and operating as intended. Specifically, SEC has not effectively or fully implemented key program activities. For example, it has not (1) filled the vacancy for a senior agency information security officer, (2) fully reported or assessed risks, (3) sufficiently tested and evaluated the effectiveness of its information system controls, and (4) certified and accredited a key intermediary subsystem. Although progress has been made, significant and preventable information security control deficiencies create continuing risks of the misuse of federal assets, unauthorized modification or destruction of financial information, inappropriate disclosure of other sensitive information, and disruption of critical operations.