March 2006

INFORMATION SECURITY

Securities and Exchange Commission Needs to Continue to Improve Its Program

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-408, a report to the Chairman, Securities and Exchange Commission

Why GAO Did This Study

The Securities and Exchange Commission (SEC) has a demanding responsibility enforcing securities laws, regulating the securities markets, and protecting investors. In enforcing these laws, SEC issues rules and regulations to provide protection for investors and to help ensure that the securities markets are fair and honest. It relies extensively on computerized systems to support its financial and mission-related operations. Information security controls affect the integrity, confidentiality, and availability of sensitive information maintained by SEC.

As part of the audit of SEC's fiscal year 2005 financial statements, GAO assessed (1) the status of SEC's actions to correct or mitigate previously reported information security weaknesses and (2) the effectiveness of the commission's information system controls in protecting the confidentiality, integrity, and availability of its financial and sensitive information.

What GAO Recommends

GAO recommends that SEC Chairman direct the Chief Information Officer to fully implement an agencywide information security program. In providing written comments on a draft of this report, SEC said that GAO's recommendations are appropriate and actionable, and that it is focusing on fully implementing the recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-408.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

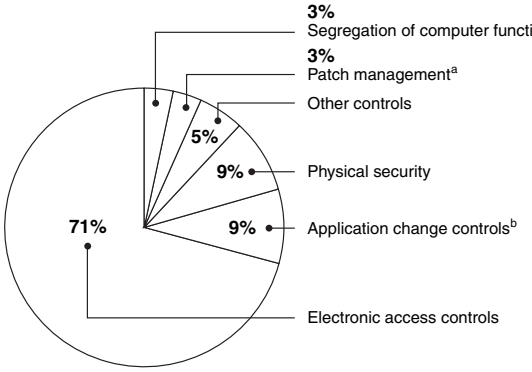
What GAO Found

Although SEC has taken steps to strengthen its information security program, most of the previously reported information security controls and program weaknesses persist. Specifically, the commission has corrected or mitigated 8 of the 51 weaknesses that GAO reported as unresolved in last year's report. Among the corrective actions SEC has taken include replacing a vulnerable, publicly accessible workstation and developing and implementing change control procedures for a major application. However, the commission has not yet effectively controlled remote access to its servers, established controls over passwords, managed access to its systems and data, securely configured network devices and servers, or implemented auditing and monitoring mechanisms to detect and track security incidents.

Overall, SEC has not effectively implemented information security controls to properly protect the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to the 43 previously reported weaknesses that remain uncorrected, GAO identified 15 new information security weaknesses. As illustrated in the figure below, most identified weaknesses pertained to electronic access controls such as user accounts and passwords, access rights and permissions, and network devices and services. These weaknesses increase the risk that financial and sensitive information will be inadequately protected against disclosure, modification, or loss, possibly without detection, and place SEC operations at risk of disruption.

A key reason for SEC's information security controls weaknesses is that the commission has not fully developed, implemented, or documented key elements of an information security program to ensure that effective controls are established and maintained. Until SEC implements such a program, its facilities and computing resources and the information that is processed, stored, and transmitted on its systems will remain vulnerable.

Information Security Weaknesses at SEC



Source: GAO.

[a]Patch management helps mitigate software vulnerabilities

[b]Application change controls help ensure only authorized programs and modifications are implemented.