March 2005

INFORMATION SECURITY

Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-262, a report to the Chairman, Securities and Exchange Commission

Why GAO Did This Study

The Securities and Exchange Commission (SEC) relies extensively on computerized systems to support its financial and mission-related operations. As part of the audit of SEC's fiscal year 2004 financial statements, GAO assessed the effectiveness of the commission's information system controls in protecting the integrity, confidentiality, and availability of its financial and sensitive information.

What GAO Recommends

GAO recommends that the SEC Chairman direct the Chief Information Officer to take several actions to fully develop and implement an effective agency-wide information security program. In commenting on a draft of this report, SEC agreed with our recommendations. SEC plans to address the identified weaknesses and indicated that significant progress is already being made to address them.

What GAO Found

SEC has not effectively implemented information system controls to protect the integrity, confidentiality, and availability of its financial and sensitive data. Specifically, the commission had not consistently implemented effective electronic access controls, including user accounts and passwords, access rights and permissions, network security, or audit and monitoring of security-relevant events to prevent, limit, and detect access to its critical financial and sensitive systems. In addition, weaknesses in other information system controls, including physical security, segregation of computer functions, application change controls, and service continuity, further increase risk to SEC's information systems. As a result, sensitive data—including payroll and financial transactions, personnel data, regulatory, and other mission critical information—were at increased risk of unauthorized disclosure, modification, or loss, possibly without detection.

A key reason for SEC's information system control weaknesses is that the commission has not fully developed and implemented a comprehensive agency information security program to provide reasonable assurance that effective controls are established and maintained and that information security receives sufficient management attention. Although SEC has taken some actions to improve security management, including establishing a central security management function and appointing a senior information security officer to manage the program, it had not clearly defined roles and responsibilities for security personnel. In addition SEC had not fully (1) assessed its risks, (2) established or implemented security policies, (3) promoted security awareness, and (4) tested and evaluated the effectiveness of its information system controls. As a result, SEC did not have a solid foundation for resolving existing information system control weaknesses and continuously managing information security risks.

www.gao.gov/cgi-bin/getrpt?GAO-05-262.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory Wilshusen at (202) 512-3317 or wilshuseng@gao.gov.