February 2008

INFORMATION SECURITY

Securities and Exchange Commission Needs to Continue to Improve Its Program

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-280, 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. Integrating effective information security controls into a layered control strategy is essential to ensure that SEC's financial and sensitive information are protected from inadvertent or deliberate misuse, disclosure, or destruction.

As part of its audit of SEC's fiscal year 2007 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 plans, policies, and practices; interviewed pertinent officials; and conducted tests and observations of controls in operation.

What GAO Recommends

GAO recommends that the SEC Chairman take several actions to fully implement an agencywide information security program.

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

To view the full product, including the scope and methodology, click on GAO-08-280. For more information, contact Greg Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or 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 8 of 20 weaknesses previously reported as unresolved at the time of our prior audit. For example, SEC has documented authorizations for software modifications, developed a comprehensive program for monitoring access activities to its computer network environment, and tested and evaluated the effectiveness of controls for the general ledger system. In addition, the commission has made progress in improving its information security program. To illustrate, it has developed remedial action plans to mitigate identified weaknesses in its systems and developed a mechanism to track the progress of actions to correct deficiencies. A key reason for its progress is that SEC senior management has been actively engaged in implementing information security activities. Nevertheless, SEC has not completed actions to correct 12 previously reported weaknesses. For example, SEC workstations are susceptible to malicious code attacks and perimeter security is not properly implemented at its Operations Center.

Significant control weaknesses intended to restrict access to data and systems, as well as other information security controls, continue to threaten the confidentiality, integrity, and availability of SEC's financial and sensitive information and information systems. SEC has not consistently 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) limit user access to only those individuals who need such access to perform their job functions, (3) encrypt sensitive data, (4) log and monitor security related events, (5) physically protect its computer resources, and (6) fully implement certain configuration management controls. A key reason for these weaknesses is that SEC has not yet fully implemented its information security program to ensure that controls are appropriately designed and operating effectively. Specifically, SEC has not effectively or fully implemented key program activities. For example, security plans for certain enterprise database applications were incomplete, information security training for certain key personnel was not sufficiently documented and monitored, security tests and evaluations of enterprise database applications were not comprehensive, and continuity of operations plans were not always complete. As a result, SEC is at increased risk of unauthorized access to and disclosure, modification, or destruction of its financial information, as well as inadvertent or deliberate disruption of its financial systems, operations, and services.