March 2007

INFORMATION SECURITY

Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-256, 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 is protected from inadvertent or deliberate misuse, disclosure, or destruction.

As part of its audit of SEC's financial statements, GAO assessed (1) SEC's actions to correct previously reported information security weaknesses and (2) the effectiveness of controls for ensuring the confidentiality, integrity, and availability of SEC's 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 the SEC Chairman improve the implementation of its policies and procedures, control tests and evaluations, and remedial action plans as part of its agencywide information security program.

In commenting on a draft of this report, SEC stated that it will actively work to implement GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-256.

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

What GAO Found

SEC has made important progress toward correcting previously reported information security control weaknesses. Specifically, it has corrected or mitigated 58 of the 71 weaknesses previously reported as unresolved at the conclusion of GAO's 2005 audit. The commission resolved all of the previously reported weaknesses in security related activities and contingency planning, and made significant progress in resolving access control weaknesses. A key reason for its progress was that SEC's senior management was actively engaged in implementing information security related activities.

Despite this progress, SEC has not consistently implemented certain key controls to effectively safeguard the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to 13 previously identified weaknesses that remain unresolved, 15 new information security weaknesses were identified. By the conclusion of GAO's review, SEC took action to address 11 of the 15 new weaknesses. A primary reason for these control weaknesses is that SEC had not consistently implemented elements of its information security program. This included inconsistent implementation of agency policies and procedures, not sufficiently testing and evaluating the effectiveness of controls for a major system as required by its certification and accreditation process, and not consistently taking effective and timely action to correct deficiencies identified in remedial action plans. Until SEC does, it will have limited assurance that it will be able to manage risks and protect sensitive information on an ongoing basis.