May 2008

INFORMATION SECURITY

FDIC Sustains Progress but Needs to Improve Configuration Management of Key Financial Systems

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-564, a report to the Chief Financial Officer and Chief Operating Officer, Federal Deposit Insurance Corporation

Why GAO Did This Study

The Federal Deposit Insurance Corporation (FDIC) has a demanding responsibility enforcing banking laws, regulating financial institutions, and protecting depositors. Effective information security controls are essential to ensure that FDIC systems and information are adequately protected from inadvertent misuse, fraudulent, or improper disclosure.

As part of its audit of FDIC's 2007 financial statements, GAO assessed (1) the progress FDIC has made in mitigating previously reported information security weaknesses and (2) the effectiveness of FDIC's controls in protecting the confidentiality, integrity, and availability of its financial systems and information. To do this, GAO examined security policies, procedures, reports, and other documents; observed controls over key financial applications; and interviewed key FDIC personnel.

What GAO Recommends

GAO recommends that FDIC take actions to improve access and configuration management controls and to perform key information security program activities for two financial systems. FDIC concurred with one and partially concurred with nine of GAO's recommendations and has developed or implemented plans to address these recommendations. In some instances, FDIC chose to pursue alternative corrective actions. If the corporation effectively implements these alternative actions to reduce risk, it will satisfy the intent of our recommendations.

To view the full product, including the scope and methodology, click on GAO-08-564. 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

FDIC has made significant progress in mitigating previously reported information security weaknesses. Specifically, it has corrected or mitigated 16 of the 21 weaknesses that GAO had previously reported as unresolved at the completion of the 2006 audit. For example, FDIC has improved physical security controls over access to its Virginia Square computer processing facility, instructed personnel to use more secure e-mail methods to protect the integrity of certain accounting data transferred over an internal communication network, and updated the security plan and contingency plan of a key financial system. In addition, FDIC stated it has initiated and completed some actions to mitigate the remaining five prior weaknesses. However, we have not verified that these actions have been completed.

Although FDIC has made significant progress improving its information system controls, old and new weaknesses could limit the corporation's ability to effectively protect the confidentiality, integrity, and availability of its financial systems and information. In addition to the five previously reported weaknesses that remain unresolved, newly identified weaknesses in access controls and configuration management controls introduce risk to two key financial systems. For example, FDIC did not always implement adequate access controls. Specifically, multiple FDIC users shared the same login ID and password, had unrestricted access to application source code, and used passwords that were not adequately encrypted. In addition, FDIC did not adequately (1) maintain a full and complete baseline for system requirements; (2) assign unique identifiers to configuration items; (3) authorize, document, and report all configuration changes; and (4) perform configuration audits. Although these weaknesses do not pose significant risk of misstatement of the corporation's financial statements, they do increase preventable risk to the corporation's financial systems and information. A key reason for these weaknesses is that FDIC did not always fully implement key information security program activities. For example, it did not adequately conduct configuration control testing or complete the remedial action plan in a timely manner and did not include necessary and key information. Until FDIC fully performs key information security program activities, its ability to maintain adequate control over its financial systems and information will be limited.