August 2006

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Improve Its Program

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-620, a report to the Board of Directors, 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. The corporation relies extensively on computerized systems to support and carry out its financial and mission-related operations.

As part of the audit of the calendar year 2005 financial statements, GAO assessed (1) the progress FDIC has made in correcting or mitigating information security weaknesses previously reported and (2) the effectiveness of the corporation's information system controls to protect the confidentiality, integrity, and availability of its key financial information and information systems.

What GAO Recommends

GAO recommends that the FDIC Chairman fully implement key elements of its agencywide information security program. In providing written comments on a draft of this report, FDIC's Deputy to the Chairman and Chief Financial Officer stated that FDIC concurred with one of GAO's recommendations, partially concurred with three, and did not concur with one. FDIC also disagreed with GAO's assessment that its information system control weaknesses were sufficient to constitute a reportable condition.

www.gao.gov/cgi-bin/getrpt?GAO-06-620.

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

What GAO Found

FDIC has made progress in correcting previously reported weaknesses. Specifically, the corporation has corrected or mitigated 18 of the 24 weaknesses that GAO previously reported as unresolved at the time of the last review. Among actions FDIC has taken are developing and implementing procedures to comply with its computer file naming convention standards and developing and implementing automated procedures for limiting access to sensitive information.

Nevertheless, FDIC has not consistently 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 remaining six previously reported weaknesses for which FDIC has not completed corrective actions, GAO identified 20 new information security weaknesses. Most identified weaknesses pertain to access controls over (1) user accounts and passwords; (2) access rights and permissions; (3) network services; (4) configuration assurance; (5) audit and monitoring of security-related events; and (6) physical security that are to prevent, limit, or detect access to its critical financial and sensitive systems and information. In addition, weaknesses exist in other information security controls relating to segregation of duties and application change controls.

A key reason for these weaknesses is that FDIC has not fully implemented elements of its information security program. For example, it has not consistently implemented its security-related policies, addressed security plans for certain applications, provided specialized training to individuals with significant security responsibilities, implemented remedial action plans for resolving known weaknesses, and updated or tested continuity plans in light of its implementation of the new financial environment. As a result, financial and sensitive information are at increased risk of unauthorized access, modification, and/or disclosure, possibly without detection. Because of this, GAO reported information system control weaknesses to be a reportable condition in 2005.