



Highlights of [GAO-07-351](#), 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. As part of its audit of the calendar year 2006 financial statements, GAO assessed (1) the progress FDIC has made in correcting or mitigating information security weaknesses previously reported and (2) the effectiveness of FDIC's system integrity controls to protect the confidentiality and availability of its financial information and information systems.

To do this, GAO examined pertinent security policies, procedures, and relevant reports. In addition, GAO conducted tests and observations of controls in operation.

What GAO Recommends

GAO recommends that FDIC take actions to address control weaknesses and fully integrate the NFE into the corporation's information security program. In written comments on a draft of this report, FDIC's Deputy to the Chairman and Chief Financial Officer stated that FDIC concurred with seven of GAO's recommendations and partially concurred with five and has implemented or will implement corrective actions. If the corporation adequately implements these actions, it will have satisfied the intent of GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-351.

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

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program

What GAO Found

FDIC has made substantial progress in correcting previously reported weaknesses in its information security controls. Specifically, it has corrected or mitigated 21 of the 26 weaknesses that GAO had reported as unresolved at the completion of the calendar year 2005 audit. Actions FDIC has taken include developing and implementing procedures to prohibit the transmission of mainframe user and administrator passwords in readable text across the network, implementing procedures to change vendor-supplied account/passwords, and improving mainframe security monitoring controls.

Although FDIC has made important progress improving its information system controls, old and new weaknesses could limit the corporation's ability to effectively protect the integrity, confidentiality, and availability of its financial and sensitive information and systems. In addition to the five previously reported weaknesses that are in the process of being mitigated, GAO identified new weaknesses in controls related to (1) e-mail security, (2) physical security, and (3) configuration management. 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 and sensitive systems and information.

In addition, FDIC has not fully integrated its new financial system—the New Financial Environment (NFE)—into its information security program. For example, it did not fully implement key control activities for the NFE. Until FDIC fully integrates the NFE with the information security program, its ability to maintain adequate system controls over its financial and sensitive information will be limited.