August 2011

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-708, a report to the Acting Chairman, Federal Deposit Insurance Corporation

INFORMATION SECURITY

Federal Deposit Insurance Corporation Has Made Progress, but Further Actions Are Needed to Protect Financial Data

Why GAO Did This Study

The Federal Deposit Insurance Corporation (FDIC) has a demanding responsibility enforcing banking laws, regulating financial institutions, and protecting depositors. Because of the importance of FDIC's work, effective information security controls are essential to ensure that the corporation's systems and information are adequately protected from inadvertent misuse, fraudulent use, or improper disclosure.

As part of its audits of the 2010 financial statements of the Deposit Insurance Fund and the Federal Savings & Loan Insurance Corporation Resolution Fund administrated by FDIC, GAO assessed the effectiveness of the corporation's controls in protecting the confidentiality, integrity, and availability of its financial systems and information. To perform the audit, GAO examined security policies, procedures, reports, and other documents; tested controls over key financial applications; and interviewed key FDIC personnel.

What GAO Recommends

GAO recommends that FDIC take two actions to enhance its comprehensive information security program. In commenting on a draft of this report, FDIC discussed actions that it has taken or plans to take to address these recommendations.

What GAO Found

Although FDIC had implemented numerous controls in its systems, it had not always implemented access and other controls to protect the confidentiality, integrity, and availability of its financial systems and information. FDIC has implemented controls to detect and change default user accounts and passwords in vendor-supplied software, restricted access to network management servers, developed and tested contingency plans for major systems, and improved mainframe logging controls. However, the corporation had not always (1) required strong passwords on financial systems and databases; (2) reviewed user access to financial information in its document sharing system in accordance with policy; (3) encrypted financial information transmitted over and stored on its network; and (4) protected powerful database accounts and privileges from unauthorized use. In addition, other weaknesses existed in FDIC's controls that were intended to appropriately segregate incompatible duties, manage system configurations, and implement patches.

An underlying reason for the information security weaknesses is that FDIC had not always implemented key information security program activities. To its credit, FDIC had developed and documented a security program and had completed actions to correct or mitigate 26 of the 33 information security weaknesses that were previously identified by GAO. However, the corporation had not assessed risks, documented security controls, or performed periodic testing on the programs and data used to support the estimates of losses and costs associated with the servicing and disposal of the assets of failed institutions. Additionally, FDIC had not always implemented its policies for restricting user access or for monitoring the progress of security patch installation.

Because FDIC had made progress in correcting or mitigating previously reported weaknesses and had implemented compensating management and reconciliation controls during 2010, GAO concluded that FDIC had resolved the significant deficiency in internal control over financial reporting related to information security reported in GAO's 2009 audit, and that the remaining unresolved issues and the new issues identified did not individually or collectively constitute a material weakness or significant deficiency in 2010. However, if left unaddressed, these issues will continue to increase FDIC's risk that its sensitive and financial information will be subject to unauthorized disclosure, modification, or destruction.

View GAO-11-708 or key components. 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.