November 2010

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Mitigate Control Weaknesses

GAO Highlights

Accountability • Integrity • Reliability

Highlights of GAO-11-29, a report to the Chairman, 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. Because of the importance of its work, the corporation must employ strong information security controls to ensure that its information systems are adequately protected from inadvertent misuse, fraud, and improper disclosure.

As part of its audit of the 2009 financial statements of the Deposit Insurance Fund and the Federal Savings & Loan Insurance Corporation Resolution Fund administrated by FDIC, GAO assessed (1) the effectiveness of FDIC's controls in protecting the confidentiality, integrity, and availability of its financial systems and information and (2) the progress FDIC has made in mitigating previously reported information security weaknesses. 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 is recommending that FDIC improve key information activities to enhance the corporation's information security program. FDIC generally agreed with GAO's recommendations and stated that it plans to address the identified weaknesses.

View GAO-11-29 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

What GAO Found

FDIC did not sufficiently implement access and other controls intended to protect the confidentiality, integrity, and availability of its financial systems and information. For example, it did not always

- sufficiently restrict user access to systems,
- ensure strong system boundaries,
- consistently enforce strong controls for identifying and authenticating users,
- encrypt sensitive information, or
- audit and monitor security-relevant events.

In addition, FDIC did not have policies, procedures, and controls in place to ensure the appropriate segregation of incompatible duties, adequately manage the configuration of its financial information systems, and update contingency plans. A key reason for these weaknesses is that FDIC did not always fully implement key information security program activities such as effectively developing, documenting, and implementing security policies, and implementing an effective continuous monitoring program. Until these weaknesses and program deficiencies are corrected, the corporation will not have sufficient assurance that its financial information and assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

Despite the newly identified weaknesses, FDIC has mitigated each of the information security weaknesses previously reported by GAO. To its credit, the corporation has made improvements to its configuration management controls and aspects of its security management. For example, it maintained a full and complete requirements baseline for two systems and included key information in a remedial action plan.

Nevertheless, GAO concluded that weaknesses in information security controls constituted a significant deficiency in internal controls over the information systems and data used for financial reporting. Until FDIC corrects the security weaknesses identified during this year's audit, it will face an elevated risk of the misuse of federal assets, unauthorized modification or destruction of financial information, inappropriate disclosure of other sensitive information, and disruption of critical operations.