July 2014

INFORMATION SECURITY

FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain

GAO Highlights

Highlights of GAO-14-674, 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 FDIC's work, effective information security controls are essential to ensure that the corporation's systems and information are adequately protected from inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction.

As part of its audits of the 2013 financial statements of the Deposit Insurance Fund and the Federal Savings and Loan Insurance Corporation Resolution Fund administered 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 do so, GAO examined security policies, procedures, reports, and other documents; tested controls over key financial applications; and interviewed FDIC personnel.

What GAO Recommends

GAO is recommending four actions for FDIC to enhance its information security management program. FDIC concurred with GAO's recommendations. In a separate report with limited distribution, GAO is recommending that FDIC take 21 specific actions to address weaknesses in security controls.

View GAO-14-674. 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

The Federal Deposit Insurance Corporation (FDIC) has implemented numerous information security controls intended to protect its key financial systems; nevertheless, weaknesses place the confidentiality, integrity, and availability of financial systems and information at unnecessary risk. During 2013, the corporation implemented 28 of the 39 open GAO recommendations pertaining to previously-reported security weaknesses that were unaddressed as of December 31, 2012. The table below details the status of previously-reported recommendations by year.

Status of Previously-Reported Information Security Recommendations

Year Reported	Not implemented at the beginning of 2013	Implemented during 2013	Not Implemented
2011	8[a]	7	1
2012	1[b]	0	1
2013	30	21	9
Total	**39**	**28**	**11**

Source: GAO analysis of FDIC data. | GAO-14-674

[a]FDIC had previously implemented 31 of the 38 recommendations GAO originally reported in 2011.

[b]FDIC had previously implemented 41 of the 42 recommendations GAO originally reported in 2012.

However, FDIC had not fully implemented controls for (1) identifying and authenticating the identity of users, (2) restricting access to sensitive systems and data, (3) encrypting sensitive data, (4) completing background reinvestigations for employees and (4) auditing and monitoring system access.

An underlying reason for many of these weaknesses is that FDIC did not fully or consistently implement aspects of its information security program. Specifically, FDIC did not:

- fully document and implement information security controls;
- ensure that employees and contractors received security awareness training;
- conduct ongoing assessments of security controls for all systems; and
- remediate agency identified weaknesses in a timely manner.

These weaknesses individually or collectively do not constitute either a material weakness or a significant deficiency for financial reporting purposes. Nevertheless, unless FDIC takes further steps to mitigate these weaknesses, the corporation's sensitive financial information and resources will remain exposed to unnecessary risk of inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction.