GAO Highlights

Highlights of GAO-15-426, a report to the Chairman, Federal Deposit Insurance Corporation

April 2015

INFORMATION SECURITY

FDIC Implemented Many Controls over Financial Systems, but Opportunities for Improvement Remain

Why GAO Did This Study

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 2014 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 making two recommendations to FDIC to improve its implementation of its information security program. FDIC concurred with GAO's recommendations. In a separate report with limited distribution, GAO is recommending that FDIC take five specific actions to address weaknesses in security controls.

View GAO-15-426. 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 remain that place the confidentiality, integrity, and availability of financial systems and information at risk. During 2014, the corporation implemented 27 of the 36 GAO recommendations pertaining to previously reported security weaknesses that were unaddressed as of December 31, 2013; actions to implement the remaining 9 recommendations were in progress. The table below details the status of these recommendations.

Status of Previously Reported Information Security Recommendations

Year reported	Not implemented at the beginning of 2014	Implemented during 2014	Actions in progress
2010	1[a]	1	0
2012	1[b]	1	0
2013	9[c]	6	3
2014	25	19	6
Total	**36**	**27**	**9**

Source: GAO analysis of FDIC data. | GAO-15-426

[a]FDIC had previously implemented 32 of the 33 recommendations GAO originally reported in 2010.

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

[c]FDIC had previously implemented 21 of the 30 recommendations GAO originally reported in 2013.

Although FDIC developed and implemented elements of its information security program, shortcomings remain in key program activities. For example:

- FDIC had taken steps to improve its security policies and procedures, but important activities were not always required by its policies. For example, although FDIC had a policy on controlling physical access to its primary data center, the policy did not apply to all FDIC data centers.
- FDIC did not consistently remediate agency-identified weaknesses in a timely manner. However, to its credit, the corporation created a strategy outlining planned actions to address weaknesses in its remedial action processes.

Additionally, FDIC has designed and documented numerous information security controls intended to protect its key financial systems; nevertheless, controls were not always consistently implemented. For example, the corporation had not always (1) ensured that passwords for a financial application complied with FDIC policy for password length or (2) centrally collected audit logs on certain servers.

These weaknesses individually or collectively do not constitute either a material weakness or a significant deficiency for financial reporting purposes. Nonetheless, by mitigating known information security weaknesses and consistently applying information security controls, FDIC could continue to reduce risks and better protect its sensitive financial information and resources from inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction.