May 2017

INFORMATION SECURITY

FDIC Needs to Improve Controls over Financial Systems and Information

GAO Highlights

Highlights of GAO-17-436, a report to the Chairman, Federal Deposit Insurance Corporation

Why GAO Did This Study

FDIC has a demanding responsibility enforcing banking laws, regulating financial institutions, and protecting depositors. Because of FDIC's reliance on information systems, 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 audit of the 2016 and 2015 financial statements of the Deposit Insurance Fund and the Federal Savings and Loan Insurance Corporation Resolution Fund, which are 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 that FDIC take one action to more fully implement its information security program. In a separate report with limited distribution, GAO made six recommendations to FDIC to address newly identified weaknesses in access and configuration management controls. In commenting on a draft of this report, FDIC agreed with GAO's recommendation and stated that corrective actions to implement the recommendation will be completed by July 2017.

View GAO-17-436. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The Federal Deposit Insurance Corporation (FDIC) implemented numerous information security controls intended to protect its key financial systems. However, further actions are needed to address weaknesses in access controls—including boundary protection, identification and authentication, and authorization controls—and in configuration management controls. For example, the corporation did not sufficiently isolate financial systems from other parts of its network, ensure that users would be held accountable for the use of a key privileged account, or establish a single, accurate listing of all IT assets in its environment.

The corporation established a comprehensive framework for its information security program and implemented many aspects of its program. For example, FDIC (1) defined security categories for the general support systems we reviewed based on risk; (2) assessed the risk from control deficiencies identified during security control tests; and (3) conducted a disaster recovery test of its general support systems and mission-critical applications. In addition, FDIC addressed 15 of the 21 previously reported weaknesses that were unresolved as of December 31, 2015, as indicated in the following table.

Status of GAO Information Security Recommendations to FDIC as of December 2016

Information security control area	Not implemented at the beginning of 2016	Implemented during 2016	Actions still in progress
Access controls	15	13	2
Other controls	4	1	3
Information security program	2	1	1
Total	**21**	**15**	**6**

Source: GAO analysis of FDIC information. | GAO-17-436

However, an underlying reason for many of the information security weaknesses identified during GAO's review was that FDIC did not fully implement other aspects of its program. For example, the corporation did not (1) include necessary information in procedures for granting access to a key financial application and (2) fully address the FDIC Office of the Inspector General's finding that the corporation did not always identify and report major security incidents in a timely manner.

Until FDIC takes the necessary steps to address both new and previously reported control deficiencies, its sensitive financial information and resources will remain at increased risk of inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction. The combination of the continuing and new information security control deficiencies in access and configuration management controls, considered collectively, represent a significant deficiency in FDIC's internal control over financial reporting as of December 31, 2016.