

Independent Evaluation of the FDIC's Information Security Program—2003

(Audit Report No. 03-040, September 17, 2003)

Summary

As required by the Federal Information Security Management Act of 2002 (FISMA), we completed an independent evaluation of the Federal Deposit Insurance Corporation's (FDIC) information security program and practices. The FISMA directs federal agencies to report annually to the Office of Management and Budget (OMB), the Comptroller General, and the Congress on the adequacy and effectiveness of their information security policies, procedures, and practices, including compliance with the FISMA. The FISMA also requires agencies to have an annual independent evaluation performed of their information security program and practices and for agencies to report the results of the evaluation to the OMB. The independent evaluation must be performed by the agency Inspector General (IG) or an independent external auditor as determined by the IG. The FISMA permanently re-authorized and strengthened the information security program, evaluation, and reporting requirements established by the former Government Information Security Reform Act (GISRA), which expired in November 2002. Prior to the enactment of the FISMA, our office completed two evaluations of the FDIC's information security program and practices as required by the GISRA.*

The objective of our review was to evaluate the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with the requirements of the FISMA and related information security policies, procedures, standards, and guidelines. The evaluation focused on the FDIC's efforts to improve its information security program relative to the baseline established in our 2002 security evaluation report. As part of our evaluation, we relied on information security-related audit, review, and evaluation reports issued by our office, the U.S. General Accounting Office, the FDIC, and others.

We concluded that although the Corporation made significant progress in improving its information security operations in recent years, additional actions were needed to ensure that corporate information resources were adequately protected. Our evaluation report contains specific steps intended to further the Corporation's efforts to develop and implement information security controls that provide assurance of adequate security for its information resources.

Management Comments

We provided FDIC management with a draft report summarizing our FISMA evaluation results on August 25, 2003. We subsequently discussed the report with management officials and made a number of changes to address their concerns and comments. Because the draft report did not contain formal recommendations, no written response was required from the Corporation.

* We issued reports entitled *Independent Evaluation of the FDIC's Information Security Program Required by the Government Information Security Reform Act*, dated September 20, 2001, and *Independent Evaluation of the FDIC's Information Security Program—2002*, dated September 11, 2002.

This report addresses issues associated with information security. Accordingly, we have not made, nor do we intend to make, public release of the specific contents of the report.