Independent Evaluation of the FDIC's Information Security Program-2004

(Report No. 04-046, September 30, 2004)

Summary

As required by the Federal Information Security Management Act of 2002 (FISMA), we have completed an independent evaluation of the Federal Deposit Insurance Corporation's (FDIC) information security program and practices. FISMA directs federal 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 Office of Management and Budget (OMB). FISMA states that the independent evaluation is to be performed by the agency Inspector General (IG) or an independent external auditor as determined by the IG. This is the fourth annual security evaluation that our office has performed pursuant to FISMA and its predecessor legislation, the Government Information Security Reform Act, which expired in November 2002.

The objective of the evaluation was to determine the effectiveness of the FDIC's information security program and practices, including its compliance with the requirements of FISMA and related information security policies, procedures, standards, and guidelines. In summary, we concluded that the Corporation had established and implemented management controls that provided limited assurance of adequate security over its information resources. As a result of focused efforts over the past several years, the FDIC has made considerable progress in improving its information security controls and practices. Notably, this is the first annual security evaluation wherein we identified no significant deficiencies as defined by OMB that warrant consideration as a potential material weakness. However, continued management attention was needed in several key security control areas to ensure that appropriate risk-based and cost-effective security controls are designed and in place to secure the FDIC's information resources and further the Corporation's security goals and objectives.

We issued a separate audit report containing responses to specific questions raised by OMB in its August 23, 2004 memorandum, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*.[1] Our responses to the OMB questions, together with the independent security evaluation report, satisfy our 2004 FISMA reporting requirements.

Steps to Improve Information Security

Similar to our prior year security evaluations, our report identified ten steps that the Corporation can take in the near term to improve its information security program and operations. Generally, the steps focused more on the implementation of the FDIC's security management controls, whereas the steps contained in our prior year evaluation

[1] Report entitled *Responses to Questions Raised in OMB's Fiscal Year 2004 FISMA Reporting Instructions*, dated September 30, 2004 (Report No. 04-047).

focused primarily on the establishment of security management controls. In many cases, the FDIC had already begun to address these steps during our evaluation field work. We will continue to work with the Corporation throughout the coming year to ensure that appropriate risk-based and cost-effective IT security controls are in place to secure corporate information resources and further corporate security goals and objectives.

Management Comments

We provided FDIC management with a draft report summarizing our FISMA evaluation results on September 3, 2004. 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.

This report contains sensitive information regarding information security. Accordingly, we have not made, nor do we intend to make, public release of the specific contents of the report.