Evaluation of FDIC's Intrusion Detection and Incident Response Capability

(Report No. 04-009, February 13, 2004)

Summary

This report presents the results of a review by IBM Business Consulting Services (IBM), an independent professional services firm engaged by the Office of Inspector General (OIG) to support its efforts to satisfy reporting requirements related to the Federal Information Security Management Act of 2002.

The objective of the review was to evaluate the policies, procedures, and technical controls for the Federal Deposit Insurance Corporation's (FDIC) computer incident response capability. The scope of the review was specifically designed to focus on (1) intrusion identification and detection, (2) incident tracking and external reporting, and (3) incident investigation.

IBM concluded that the FDIC has made improvements in the incident response area, but additional work is needed to strengthen FDIC's controls for identifying and monitoring security incidents.

Recommendations

IBM made multiple recommendations to improve the intrusion detection and incident response capability at the FDIC.

Management Response

The FDIC's response adequately addressed all the conditions discussed in the report.

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.