Office of Audits
OIG

Report No. 05-016
March 2005

Security Controls Over the FDIC's Electronic Mail (E-mail) Infrastructure

Background and Purpose of Audit

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with International Business Machines (IBM) Business Consulting Services to audit and report on the effectiveness of security controls over the FDIC's electronic mail (e-mail) infrastructure. The results of this audit support the OIG in fulfilling its evaluation and reporting responsibilities under the Federal Information Security Management Act of 2002.

The FDIC uses e-mail to conduct much of its official business and share sensitive information such as open bank data, contract negotiations, personnel data, and legal matters. E-mail servers are one of the most frequent targets of attacks. In addition, e-mail messages and their attachments have proven to be effective in introducing viruses, worms, and other types of malicious code into networks. Therefore, e-mail servers and related infrastructure components must be properly secured.

The objective of the audit was to evaluate the adequacy of security controls over the FDIC's e-mail infrastructure that were designed to ensure the appropriate confidentiality, integrity, and availability of information. As part of the audit, IBM evaluated the FDIC's management, operational, and technical security controls related to the e-mail infrastructure for consistency with federal standards and guidelines.

Results of Audit

IBM found that the FDIC had established and implemented many of the e-mail security controls recommended in federal standards and guidelines such as e-mail encryption, software patch management, and a network architecture that protects e-mail servers. While these actions were positive, the FDIC needed to take additional steps to ensure that security controls for the e-mail infrastructure provided adequate confidentiality, integrity, and availability of information.

Recommendations and Management Response

IBM recommended that the FDIC:

- take additional measures to ensure that users encrypt e-mail communications when appropriate;
- strengthen technical security controls over the e-mail infrastructure;
- improve the vulnerability scanning process for e-mail servers; and
- strengthen controls for ensuring that electronic records, including e-mails, are retained when employees leave the Corporation.

The Corporation's response adequately addressed our concerns.

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.