Office of Audits

Report No. AUD-07-010
September 2007

Division of Resolutions and Receiverships Protection of Electronic Records

Background and Purpose of Audit

Key to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding the sensitive information it collects when conducting resolution and receivership activities at FDIC-insured financial institutions. Such information includes, for example, reports on potential financial institution failures and sensitive personally identifiable information (PII) for institution depositors, borrowers, and employees.

Much of the sensitive information handled by the FDIC falls within the scope of several statutes and regulations intended to protect such information from unauthorized disclosure. These statutes and regulations include the Privacy Act of 1974; the Federal Information Security Management Act of 2002; and the FDIC's Rules and Regulations--Parts 309, *Disclosure of Information*, and 310, *Privacy Act Regulations*.

The audit objective was to evaluate the design and implementation of selected controls established by the Division of Resolutions and Receiverships (DRR) for safeguarding sensitive electronic information collected and maintained as a result of resolution and receivership activities at FDIC-insured financial institutions.

Results of Audit

DRR established a number of important controls to safeguard the sensitive electronic information it collects and maintains as a result of resolution and receivership activities at FDIC-insured financial institutions. Such controls include policies, guidelines, and business rules for protecting sensitive electronic information and an Information Security Manager to promote compliance with FDIC and DRR security policies, procedures, and guidelines. However, access to sensitive resolution and receivership information (including PII) stored on the FDIC's internal network was not adequately protected. In addition, sensitive information stored on portable information technology equipment was not encrypted as prescribed by FDIC policy and DRR guidelines. Further, DRR's guidelines for safeguarding sensitive information did not address e-mail communications. These deficiencies increased the risk of unauthorized use of sensitive information.

Recommendations and Management Response

DRR and Division of Information Technology (DIT) security officials took prompt action to restrict access to the vulnerable sensitive information that we identified during the audit and were taking additional steps to safeguard sensitive resolution and receivership information at the close of our audit. The report contains four recommendations addressed to the DRR Director to implement appropriate security control measures to address the security control deficiencies referenced above. The DRR Director concurred with all four recommendations.

This report addresses issues associated with information security. Accordingly, we do not intend to make public release of the specific contents of the report.