Security Controls Over the FDIC's Wireless Data Communications

March 2006
Report No. 06-012

SUMMARY OF AUDIT REPORT

Background and Purpose of Audit

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to audit and report on the security of the FDIC's wireless data communications. The results of this audit support the FDIC OIG in fulfilling its evaluation and reporting responsibilities under the Federal Information Security Management Act (FISMA) of 2002.

Wireless technology offers federal agencies a number of important benefits, such as increased employee productivity and ease of network installation. However, this technology also presents a number of potentially significant security risks to the confidentiality, availability, and integrity of sensitive information. Such risks include the interception of communications not intended for public disclosure, denial of service attacks, and unauthorized deployment of wireless-enabled devices.

The audit objective was to determine whether the FDIC has established and implemented security controls that provide reasonable assurance that its wireless data communications are adequately protected.

Results of Audit

The FDIC established and implemented security controls for its wireless data communications that were generally consistent with the National Institute of Standards and Technology's recommended practices. Such controls include policies to govern the deployment of wireless-enabled devices connected to the FDIC's corporate network, security software to authenticate wireless users to the corporate network and protect the confidentiality of their communications, and procedures to assess wireless security activities. However, additional controls are needed to provide reasonable assurance of adequate security

Recommendations and Management Response

KPMG recommended that the FDIC's Chief Information Officer (CIO):

- enhance the Corporation's wireless security policies and awareness training; and
- restrict access to critical software programs designed to safeguard wireless data communications.

The CIO provided written comments that were responsive to the report's recommendations. Because this report addresses issues associated with information security, we do not intend to make public release of the specific contents of the report.