



OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: FFIEC Information Security Booklet

Description: Information Security
Guidance

TO: Chief Executive Officers of All National Banks, Federal Branches and Agencies, Technology Service Providers and Software Vendors, Department and Division Heads, and All Examining Personnel

The Federal Financial Institutions Examination Council (FFIEC) has released updated information security guidance in the form of a new Information Security Booklet. The Information Security Booklet is the first in a series of booklets that will completely update and replace the *1996 FFIEC Information Systems Examination Handbook*.

Reliance on technology in all aspects of banking by bankers, consumers, and corporations has increased both the potential for, and likely impact of, security threats to national banks. Widespread adoption of effective security processes can help ensure that the banking industry maintains effective safeguards against such threats and, by doing so, helps preserve the public trust. The Information Security Booklet provides a comprehensive security framework for national banks and their technology service providers. The framework focuses on implementing a security risk management process that identifies risks, develops and implements a security strategy, tests key controls, and monitors the risk environment. This framework also stresses the important roles that senior management and boards of directors play in this process by emphasizing their responsibility to recognize security risks in their banks and to assign appropriate roles and responsibilities to their managers and employees.

To facilitate clear communication of various key points, action summaries are incorporated throughout the narrative to highlight high-level control considerations applicable to all banks. The booklet also makes clear that financial institutions or technology service providers that outsource some or all information processing are expected to incorporate the oversight of their service providers into this process to ensure that they implement a similar risk management process. Examiners will use the booklet's workprogram as expanded examination procedures, as appropriate, based on the risk and complexity of the bank or technology service provider's operations.

The booklet also consolidates guidance from prior issuances and rescinds the following:

- Chapter 14, Security – Physical and Data, 1996 FFIEC IT Examination Handbook
- OCC Bulletin 99-9 – Infrastructure Threats from Cyberterrorists
- Banking Circular 229 – Information Security

The attached FFIEC press release describes the handbook update process and provides the following link <http://www.ffiec.gov/guides> to an electronic version of the Information Security Booklet. To accommodate banks with limited access to the Internet, the OCC will also include the booklet in the next release of e-files, the CD-based library of OCC publications provided to all national banks. Any bank that is not able to download the booklet may order a printed copy. Please send your request to the Office of the Comptroller of the Currency, 250 E Street, SW, Mail Stop 4-8, Washington, DC 20219. If you need assistance, please contact the OCC's Communications Division at (202) 874-4700.

Questions regarding this booklet should be directed to your supervisory office or the Bank Technology Division at (202) 874-5920.

Ralph E. Sharpe
Deputy Comptroller for Technology

Attachment