employees with responsibilities for or access to customer information;

f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

2. Train staff to implement the bank's information security program.

3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

D. *Oversee Service Provider Arrangements.* Each bank shall:

1. Exercise appropriate due diligence in selecting its service providers;

2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and

3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. *Adjust the Program.* Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. *Report to the Board.* Each bank shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank's compliance with these Guidelines. The report, which will vary depending upon the complexity of each bank's program should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations, and management's responses; and recommendations for changes in the information security program.

G. *Implement the Standards.* 1. *Effective date.* Each bank must implement an information security program pursuant to these Guidelines by July 1, 2001.

2. *Two-year grandfathering of agreements with service providers.* Until July 1, 2003, a contract that a bank has entered into with a service provider to perform services for it or functions on its behalf, satisfies the provisions of paragraph III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of customer information as long as the bank entered into the contract on or before March 5, 2001.

[66 FR 8638, Feb. 1, 2001]

PART 365—REAL ESTATE LENDING STANDARDS

Sec.
365.1 Purpose and scope.
365.2 Real estate lending standards.
APPENDIX A TO PART 365—INTERAGENCY GUIDELINES FOR REAL ESTATE LENDING POLICIES

AUTHORITY: 12 U.S.C. 1828(o).

SOURCE: 57 FR 62896, 62900, Dec. 31, 1992, unless otherwise noted.

§ 365.1 Purpose and scope.

This part, issued pursuant to section 304 of the Federal Deposit Insurance Corporation Improvement Act of 1991, 12 U.S.C. 1828(o), prescribes standards for real estate lending to be used by insured state nonmember banks (including state-licensed insured branches of foreign banks) in adopting internal real estate lending policies.

§ 365.2 Real estate lending standards.

(a) Each insured state nonmember bank shall adopt and maintain written policies that establish appropriate limits and standards for extensions of credit that are secured by liens on or interests in real estate, or that are made for the purpose of financing permanent improvements to real estate.

(b)(1) Real estate lending policies adopted pursuant to this section must:

(i) Be consistent with safe and sound banking practices;

(ii) Be appropriate to the size of the institution and the nature and scope of its operations; and