DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 30

[Docket No. 00–13]

RIN 1557–AB84

FEDERAL RESERVE SYSTEM

12 CFR Parts 208, 211, 225, and 263

[Docket No. R–1073]

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Parts 308 and 364

RIN 3064–AC39

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR Parts 568 and 570

[Docket No. 2000–51]

RIN 1550–AB36

Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness

AGENCIES: The Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; and Office of Thrift Supervision, Treasury.

ACTION: Joint notice of proposed rule making.

SUMMARY: The Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision, (collectively, the Agencies) are requesting comment on proposed Guidelines establishing standards for safeguarding customer information published to implement sections 501 and 505(b) of the Gramm-Leach-Bliley Act (the G–L–B Act or Act).

Section 501 of the G–L–B Act requires the Agencies to establish appropriate standards for the financial institutions subject to their respective jurisdictions relating to administrative, technical, and physical safeguards for customer records and information. These safeguards are intended to: Insure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. The Agencies are to implement these standards in the same manner, to the extent practicable, as standards prescribed pursuant to section 39(a) of the Federal Deposit Insurance Act (FDI Act). The proposed Guidelines implement the requirements of the G–L–B Act.

The Agencies previously issued guidelines establishing Year 2000 safety and soundness standards for insured depository institutions pursuant to section 39 of the FDI Act. Since the events for which these guidelines were issued have passed, the Agencies have concluded that the guidelines are no longer necessary and propose to rescind the guidelines as part of this rulemaking.

DATES: Comments must be received not later than August 25, 2000.

ADDRESSES: Comments should be directed to: *Office of the Comptroller of the Currency (OCC):* Communications Division, Office of the Comptroller of the Currency, 250 E Street, SW., Third Floor, Washington, DC 20219, Attention: Docket No. 00–13; Fax number (202) 874–5274 or Internet address: *regs.comments@occ.treas.gov.* Comments may be inspected and photocopied at the OCC's Public Reference Room, 250 E Street, SW., Washington, D.C., between 9:00 a.m. and 5:00 p.m. on business days. You can make an appointment to inspect the comments by calling (202) 874–5043.

Board of Governors of the Federal Reserve System (Board): Comments, which should refer to Docket No. R–1073, may be mailed to Ms. Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, 20th and C Streets, NW, Washington, DC 20551 or mailed electronically to *regs.comments@federalreserve.gov.* Comments addressed to Ms. Johnson also may be delivered to the Board's mail room between 8:45 a.m. and 5:15 p.m. and to the security control room outside of those hours. Both the mail room and the security control room are accessible from the courtyard entrance on 20th Street between Constitution Avenue and C Street, NW. Comments may be inspected in Room MP–500 between 9 a.m. and 5 p.m., pursuant to § 261.12, except as provided in § 261.14, of the Board's Rules Regarding the Availability of Information, 12 CFR 261.12 and 261.14.

Federal Deposit Insurance Corporation (FDIC): Send written comments to Robert E. Feldman, Executive Secretary, Attention: Comments/OES, Federal Deposit Insurance Corporation, 550 17th Street, NW., Washington, DC 20429. Comments also may be mailed electronically to *comments@fdic.gov.* Comments may be hand delivered to the guard station at the rear of the 17th Street building (located on F Street) on business days between 7 a.m. and 5 p.m.; Fax number (202) 898–3838. Comments may be inspected and photocopied in the FDIC Public Information Center, Room 100, 801 17th Street, NW., Washington, DC 20429, between 9 a.m. and 5:00 p.m. on business days.

Office of Thrift Supervision (OTS): Send comments to Manager, Dissemination Branch, Information Management & Services Division, Office of Thrift Supervision, 1700 G Street, NW., lower level from 9:00 a.m. to 5:00 p.m. on business days. Send facsimile transmissions to Fax number (202) 906–7755 or (202) 906–6956 (if the comment is over 25 pages). Send email to *public.info@ots.treas.gov* and include your name and telephone number. Interested persons may inspect comments at 1700 G Street, NW., from 9 a.m. until 4 p.m. on Tuesdays and Thursdays.

FOR FURTHER INFORMATION CONTACT:

OCC: Mark Tenhundfeld, Assistant Director, Legislative and Regulatory Activities Division, (202) 874–5090; John Carlson, Acting Deputy Director for Bank Technology, (202) 874–5013; Deborah Katz, Senior Attorney, Legislative and Regulatory Activities Division, (202) 874–5090; or Jeffery Abrahamson, Attorney, Legislative and Regulatory Activities Division, (202) 874–5090.

Board: Heidi Richards, Manager, Division of Banking Supervision and Regulation, (202) 452–2598; or Stephanie Martin, Managing Senior Counsel, Legal Division, (202) 452–3198.

For the hearing impaired only, contact Janice Simms, Telecommunication Device for the Deaf (TDD) (202) 452–3544, Board of Governors of the Federal Reserve System, 20th and C Streets, NW., Washington, DC 20551.

FDIC: Thomas J. Tuzinski, Review Examiner, Division of Supervision, (202) 898–6748; Jeffrey M. Kopchik, Senior Policy Analyst, Division of Supervision, (202) 898–3872; or Robert A. Patrick, Counsel, Legal Division, (202) 898–3757.

OTS: Paul R. Reymann, Senior Project Manager, Technology Risk Management, (202) 906–5645; or Christine Harrington, Counsel, Banking and Finance,

Regulations and Legislation Division, (202) 906–7957.

SUPPLEMENTARY INFORMATION: The contents of this preamble are listed in the following outline:

I. Background
II. Section-by-Section Analysis
III. Regulatory Analysis
A. Paperwork Reduction Act
B. Regulatory Flexibility Act
C. Executive Order 12866
D. Unfunded Mandates Act of 1995
IV. Solicitation of Comments on Use of Plain Language

I. Background

On November 12, 1999, President Clinton signed the G–L–B Act (Pub. L. 106–102) into law. Section 501, entitled Protection of Nonpublic Personal Information, requires the Agencies and the Securities and Exchange Commission, the National Credit Union Administration, and the Federal Trade Commission to establish appropriate standards for the financial institutions subject to their respective jurisdictions relating to the administrative, technical, and physical safeguards for customer records and information. These safeguards are intended to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer.

Section 505(b) of the G–L–B Act provides that these standards are to be implemented by the Agencies in the same manner, to the extent practicable, as standards prescribed pursuant to section 39(a) of the FDI Act.[1] Section 39(a) of the FDI Act authorizes the Agencies to establish operational and managerial standards for insured depository institutions relative to, among other things, internal controls, information systems, and internal audit systems, as well as such other operational and managerial standards as the Agencies determine to be appropriate. These standards may be issued as guidelines or regulations. While this proposal is in the form of guidelines, the Agencies solicit comment on whether the final standards should be issued in the form of guidelines or as regulations.[2]

The proposed Guidelines apply to ''nonpublic personal information'' of ''customers'' as those terms are defined in the Agencies' privacy rules published in accordance with Title V of the G–L–B Act (the Privacy Rule). *See* Privacy of Consumer Financial Information, 65 FR 35162 (June 1, 2000).[3] Under section 503(b)(3) of the G–L–B Act and the Privacy Rule, financial institutions will be required to disclose their policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information as part of the initial and annual notices to their customers. Key components of the proposed Guidelines were derived from security-related supervisory guidance previously issued by the Agencies and the Federal Financial Institutions Examination Council (FFIEC).

The texts of the Agencies' proposed Guidelines are substantively identical. The Agencies request comment on all aspects of the proposed Guidelines as well as comment on the specific provisions and issues highlighted in the section-by-section analysis below. Those commenters who believe that the proposed Guidelines would impose undue burdens on financial institutions should identify which parts of the Guidelines they believe impose excessive burdens and describe the burdens. Those commenters should also discuss either: (1) Alternative methods that would accomplish the same purpose; or (2) why the intended purpose is unnecessary or should be modified.

The Agencies also seek comments on the impact of this proposal on community banks. The Agencies recognize that community banks operate with more limited resources than larger institutions and may present a different risk profile. Thus, in addition to reviewing comments, each Agency will endeavor to assess the potential impact and burden that the proposal may impose on community banks during the comment period. The Agencies also specifically request comment on the impact of this proposal on community banks' current resources and available personnel with the requisite expertise. Commenters should discuss whether (1) The standards are reasonable and realistic for community banks, and (2) whether the goals of the proposed regulation could be achieved, for community banks, through an alternative approach. Based on the comments received, the Agencies will consider whether there is a need to develop a compliance guide for community banks and other smaller institutions in conjunction with the final Guidelines.

As proposed, the Guidelines will appear as an appendix to each Agency's Standards for Safety and Soundness. For the OCC those regulations appear at 12 CFR part 30; for the Board at 12 CFR part 208; for the FDIC at 12 CFR part 364; and for the OTS at 12 CFR part 570. The Board is also amending 12 CFR parts 211 and 225 to apply the Guidelines to other institutions that it supervises.

The Agencies will apply the rules already in place to require the submission of a compliance plan in appropriate circumstances. For the OCC those regulations appear at 12 CFR part 30; for the Board at 12 CFR part 263; for the FDIC at 12 CFR part 308, subpart R; and for the OTS at 12 CFR part 570. This proposal makes conforming changes to the regulatory text of these parts.

Rescission of Year 2000 Standards for Safety and Soundness. The Agencies previously issued guidelines establishing Year 2000 safety and soundness standards for insured depository institutions pursuant to section 39 of the FDI Act. Because the events for which these guidelines were issued have passed, the Agencies have concluded that the guidelines are no longer necessary and propose to rescind the guidelines as part of this rulemaking. These guidelines appear for the OCC at 12 CFR part 30, appendix B and C; for the Board at 12 CFR part 208, appendix D–2; for the FDIC at 12 CFR part 364, appendix B; and for the OTS at 12 CFR part 570, appendix B. The Agencies request comment on whether the rescission of these appendices is appropriate.

II. Section-by-Section Analysis

The discussion that follows applies to each of the Agencies' proposed Guidelines.

[1] Section 39 applies only to insured depository institutions, including insured branches of foreign banks. The Guidelines, however, will also apply to certain uninsured institutions, such as bank holding companies, certain nonbank subsidiaries of bank holding companies and insured depository institutions, and uninsured branches and agencies of foreign banks. *See* section 501 and 505(b) of the G–L–B Act.

[2] The OTS proposes to place its information security guidelines in Appendix B to 12 CFR part 570, with the provisions implementing section 39 of the FDI Act. At the same time, the OTS proposes a regulatory requirement that the institutions the OTS regulates comply with the proposed guidelines. Because information security guidelines are similar to physical security procedures, the OTS proposes including a provision in 12 CFR part 568, which covers primarily physical security procedures, requiring compliance with the guidelines in Appendix B to part 570.

[3] Where the Supplementary Information refers to a section of the Privacy Rule, it will preface the common section number with ''__'', as each Agency has a different part number.

Appendix __ to Part __—Interagency Guidelines Establishing Standards for Safeguarding Customer Information

I. Introduction

Proposed paragraph I. sets forth the general purpose of the proposed Guidelines, which is to provide guidance to each financial institution in establishing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. This paragraph also sets forth the statutory authority for the proposed Guidelines, including section 39(a) of the FDI Act (12 U.S.C. 1831p–1) and sections 501 and 505(b) of the G–L–B Act (15 U.S.C. 6801 and 6805(b)).

I.A. Scope

Paragraph I.A. describes the scope of the proposed Guidelines. Each Agency defines specifically those entities within its particular scope of coverage in this paragraph of the proposed Guidelines. [4]

I.B. Preservation of Existing Authority

Paragraph I.B. makes clear that in issuing these proposed Guidelines none of the Agencies is, in any way, limiting its authority to address any unsafe or unsound practice, violation of law, unsafe or unsound condition, or other practice, including any condition or practice related to safeguarding customer information. Any action taken by any Agency under section 39(a) of the FDI Act and these Guidelines may be taken independently of, in conjunction with, or in addition to any other enforcement action available to the Agency.

I.C. Definitions

Paragraph I.C. sets forth the definitions of various terms for purposes of the proposed Guidelines. [5]

I.C.1. In General

Paragraph I.C.1. provides that terms used in the proposed Guidelines have the same meanings as set forth in sections 3 and 39(a) of the FDI Act (12 U.S.C. 1813 and 1831p–1), except to the extent that the definition of the term is modified in the proposed Guidelines or where the context requires otherwise.

I.C.2. Customer Information

Proposed paragraph I.C.2. defines customer information. Customer information includes any records, data, files, or other information containing nonpublic personal information, as defined in section __.3(n) of the Privacy Rule, about a customer. This includes records in paper, electronic, or any other form that are within the control of a financial institution or that are maintained by any service provider on behalf of an institution. Although the G–L–B Act uses both the terms ''records'' and ''information,'' for the sake of simplicity, in the proposed Guidelines the term ''customer information'' encompasses all customer records.

Section 501(b) refers to safeguarding the security and confidentiality of ''customer'' information. The term ''customer'' is also used in other sections of Title V of the G–L–B Act and has been defined by the Agencies in the Privacy Rule interpreting these sections to include those consumers who have a customer relationship with the institution. This term does not cover business customers, or consumers who have not established an ongoing relationship with a financial institution (*e.g.* those that merely use an institution's ATM or apply for a loan). *See* sections __.3(h) and (i) of the Privacy Rule.

The Agencies propose defining ''customer'' for purposes of the Guidelines consistently with the Privacy Rule. However, the Agencies have considered whether the scope of the Guidelines should apply to records regarding all consumers, the institution's consumer and business clients, or all of an institution's records. The Agencies solicit comment on whether a broader definition would change the information security program that an institution would implement, or, whether, as a practical matter, institutions would respond to the Guidelines by implementing an information security program for all types of records under their control rather than segregating ''customer'' records for special treatment.

I.C.3. Customer

Proposed paragraph I.C.3. defines customer. Customer would include any customer of an institution as defined in section __.3(h) of the Privacy Rule. A customer is a consumer who has established a continuing relationship with an institution under which the institution provides one or more financial products or services to the consumer to be used primarily for personal, family or household purposes.

I.C.4. Service Provider

Proposed paragraph I.C.4. defines a service provider as any person or entity that maintains or processes customer information on behalf of an institution, or is otherwise granted access to customer information through its provision of services to an institution.

I.C.5. Board of Directors

Proposed paragraph I.C.5. defines board of directors to mean, in the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency. [6]

I.C.6. Customer Information System

Proposed paragraph I.C.6. defines customer information system to be electronic or physical methods used to access, collect, store, use, transmit and protect customer information.

II. Standards for Safeguarding Customer Information

II.A. Information Security Program

The proposed Guidelines describe the Agencies' expectations for the creation, implementation, and maintenance of an information security program. This program must include administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. The proposed Guidelines describe the oversight role of the board of directors in this process and management's continuing duty to evaluate and report to the board on the overall status of this program. The four steps in this process require an institution to: (1) Identify and assess the risks that may threaten customer information; (2) develop a written plan containing policies and procedures to manage and control these risks; (3) implement and test the plan; and (4) adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security. The proposed Guidelines also set forth an institution's responsibility for overseeing outsourcing arrangements.

II.B. Objectives

Proposed paragraph II.B. describes the objectives for an information security program to ensure the security and

[4] While the OTS generally regulates savings and loan holding companies under the Home Owners Loan Act (12 U.S.C. 1461 *et seq.*), a different Federal functional regulator, a state insurance authority, or the Federal Trade Commission may establish standards for safeguarding customer information as to that holding company under section 505 of the G–L–B Act, depending on the nature of the holding company's activities.

[5] In addition to the definitions discussed below, the Board's guidelines in 12 CFR parts 208 and 225 contain a definition of ''subsidiary,'' which describes the state member bank and bank holding company subsidiaries that are subject to the Guidelines.

[6] The OTS version of the guidelines does not include this definition because the OTS does not regulate foreign institutions. Section I of the OTS guidelines has been renumbered accordingly.

confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of customer information that could either: (1) Result in substantial harm or inconvenience to any customer; or (2) present a safety and soundness risk to the institution. For purposes of the Guidelines, unauthorized access to or use of customer information does not include access to or use of customer information with the customer's consent. The Agencies request comment on whether there are additional or alternative objectives that should be included in the Guidelines.

III. Develop and Implement Information Security Program

III.A. Involve the Board of Directors and Management

Proposed paragraph III.A. describes the involvement of the board and management in the development and implementation of an information security program. The board's responsibilities are to: (1) Approve the institution's written information security policy and program that complies with these Guidelines; and (2) oversee efforts to develop, implement, and maintain an effective information security program, including the regular review of management reports.

The three responsibilities for management in the development of an information security program are to: (1) Evaluate the impact on the institution's security program of changing business arrangements (*e.g.* mergers and acquisitions, alliances and joint ventures, outsourcing arrangements), and changes to customer information systems; (2) document compliance with these Guidelines; and (3) keep the board informed of the current status of the institution's information security program, *e.g.,* report to the board on a regular basis on the overall status of the information security program, including material matters related to: Risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements to the information security program.

The Agencies specifically invite comment regarding the appropriate frequency of reports to the board. Should the Guidelines specify reporting intervals—monthly, quarterly, annually? How regularly should management report to the board regarding the institution's information security program and why are these intervals appropriate? Should the Guidelines require that the board designate a Corporate Information Security Officer or other responsible individual who would have the authority, subject to the board's approval, to develop and administer the institution's information security program?

III.B. Assess Risk

Proposed paragraph III.B. describes the risk assessment process that should be developed as part of the information security program in order to meet the objectives of the Guidelines. First, a financial institution should identify and assess risks that may threaten the security, confidentiality, or integrity of customer information, whether in storage, processing, or transit. The risk assessment should be made in light of an institution's size, scope of operations, and technology. Institutions should determine the sensitivity of customer information to be protected as part of this analysis.

Next, a financial institution should conduct an assessment of the sufficiency of existing policies, procedures, customer information systems, and other arrangements intended to control the risks it has identified. Finally, the financial institution should monitor, evaluate, and adjust its risk assessment, taking into consideration any technological or other changes or the sensitivity of the information.

III.C. Manage and Control Risk

Proposed paragraph III.C. describes the elements of a comprehensive risk management plan designed to control identified risks and to achieve the overall objective of ensuring the security and confidentiality of customer information. It identifies the factors an institution should consider in evaluating the adequacy of its policies and procedures to effectively manage these risks commensurate with the sensitivity of the information as well as the complexity and scope of the institution and its activities. In establishing the policies and procedures, each institution should consider appropriate:

a. Access rights to customer information;

b. Access controls on customer information systems, including controls to authenticate and grant access only to authorized individuals and companies;

c. Access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities;

d. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

e. Procedures to confirm that customer information system modifications are consistent with the institution's information security program;

f. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

g. Contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by service providers;

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

i. Response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected;

j. Protection against destruction of customer information due to potential physical hazards, such as fire and water damage; and

k. Response programs to preserve the integrity and security of customer information in the event of computer or other technological failure, including, where appropriate, reconstructing lost or damaged customer information.

The Agencies intend that these elements accommodate institutions of varying sizes, scope of operations, and risk management structures. The Agencies invite comment on the degree of detail that should be included in the Guidelines regarding the risk management program, which elements should be specified in the Guidelines, and any other components of a risk management program that should be included.

The Guidelines also provide that an institution's information security program should include a training component designed to teach employees to recognize and respond to fraudulent attempts to obtain customer information and, where appropriate, to report any attempts to regulatory and law enforcement agencies.

The information security program also should include regular testing of systems to confirm that an institution and its service providers control identified risks and achieve the objectives to ensure the security and confidentiality of customer information. The tests should be verified by an independent third party or staff independent of those who conducted the test. Tests should be documented.

The frequency and nature of the testing should be determined by the risk assessment and adjusted as necessary to reflect changes in the internal and external conditions. The Agencies request comment on whether specific types of security tests, such as penetration tests or intrusion detections tests, should be required.

The Agencies invite comment regarding the appropriate degree of independence that should be specified in the Guidelines in connection with the testing of information security systems and the review of test results. Should the tests or reviews of tests be conducted by persons who are not employees of the financial institution? If employees may conduct the testing or may review test results, what measures, if any, are appropriate to assure their independence?

Finally, the Guidelines describe the need for an ongoing process of monitoring, evaluation, and adjustment of the information security program in light of any relevant changes in technology, the sensitivity of customer information, and internal or external threats to information security.

III.D. Oversee Outsourcing Arrangements

Proposed paragraph III.D. addresses outsourcing. An institution should exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect customer information and customer information systems consistent with these Guidelines.

The Agencies welcome comments on the appropriate treatment of outsourcing arrangements. For example, are industry best practices available regarding effective monitoring of service provider security precautions? Do service providers accommodate requests for specific contract provisions regarding information security? To the extent that service providers do not accommodate these requests, how do financial institutions implement effective information security programs? Should these Guidelines contain specific contract provisions requiring service provider performance standards in connection with the security of customer information?

III.E. Implement the Standards

Proposed paragraph III.E. describes the timing requirements for the implementation of these standards. Each financial institution is to take appropriate steps to fully implement an information security program pursuant to these Guidelines by July 1, 2001.

III. Regulatory Analysis

A. Paperwork Reduction Act

FDIC: The FDIC has determined that the proposed rule does not contain any information collections as defined by the Paperwork Reduction Act (44 U.S.C. 3501, *et seq*.).

B. Regulatory Flexibility Act

OCC: The Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA) requires an agency to either provide an Initial Regulatory Flexibility Analysis with a proposed rule or certify that the proposed rule will not have a significant economic impact on a substantial number of small entities (defined for purposes of the RFA to include banks with less than $ 100 million in assets).

A. Reasons for Proposed Rule

The proposed Guidelines implement section 501(b) of the G–L–B Act. Section 501(b) requires the OCC to publish standards for financial institutions subject to its jurisdiction relating to administrative, technical, and physical standards to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

The OCC does not expect that this rule, if adopted, would have the threshold impact on small entities. The rule would adopt guidelines that are to be implemented by each institution within the OCC's primary jurisdiction in a way that is appropriate for that institution. Thus, the burden stemming from this rule is likely to be less on small institutions. Moreover, institutions regulated by the OCC, regardless of size, likely already have in place certain policies and procedures that would satisfy at least some of the guidelines. However, the OCC invites comment on the burden that likely will result on small institutions from this rulemaking, and has prepared the following analysis.

B. Statement of Objectives and Legal Basis

The objectives of the proposed Guidelines are described in the **SUPPLEMENTARY INFORMATION** section. The legal bases for the proposed rule are 12 U.S.C. 93a, 1818, 1831p–1, and 3102(b), and 15 U.S.C. 6801 and 6805(b)(1).

C. Description of Small Entities to Which the Rule Will Apply

The proposed rule would apply to all national banks, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities with assets under $100 million.

D. Projected Reporting, Recordkeeping and Other Compliance Requirements

The OCC does not believe that the proposed rule imposes any reporting or any specific recordkeeping requirements within the meaning of the RFA. The proposed rule requires all covered institutions to develop an information security program to safeguard customer information. An institution must assess risks to customer information, establish policies, procedures and training to control risks, test the program's effectiveness, and manage and monitor its service providers. These requirements will apply to all institutions subject to the OCC's jurisdiction, regardless of their size.

Because the information security program described in the proposed Guidelines reflects existing supervisory guidance already issued by the OCC and the FFIEC, as well as sound business practices, the OCC believes that most institutions already have such a program in place. Accordingly, the OCC believes that most covered institutions will already have the expertise to develop, implement, and maintain the program, including the skills of computer security professionals and lawyers. However, some institutions may need to formalize or enhance their information security programs. The OCC is concerned about the potential impact of the proposed Guidelines on community banks and will be reviewing current information security practices at smaller institutions. The OCC invites comment on the costs of establishing and operating an information security program.

E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules

The OCC is unable to identify any statutes or rules which would overlap or conflict with the requirement to develop and implement an information security program. The OCC seeks comment and information about any such statutes or rules, as well as any other state, local, or industry rules or policies that require a covered institution to implement business practices that would comply with the requirements of the proposed rule.

F. Discussion of Significant Alternatives

The G–L–B Act requires that the Agencies issue standards to safeguard customer information. However, the G–L–B Act also states that the standards should be implemented in the same manner, to the extent practicable, as standards issued under section 39(a) of the FDI Act. Therefore, the standards have been issued as Guidelines and in a form that resembles all of the other standards prescribed by the Agencies thus far under section 39(a).

In addition, the G–L–B Act requires that standards be developed for all institutions, without exception. Therefore, the proposed Guidelines apply to institutions of all sizes, including those with assets of $100 million or less. However, the standards in the proposed Guidelines are flexible, so that each institution may develop an information security program tailored to its size and the nature of its operations. The OCC welcomes comment on any significant alternatives, consistent with the G–L–B Act, that would minimize the impact on small entities.

Board: The Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA) requires an agency either to publish an initial regulatory flexibility analysis with a proposed rule or certify that the proposed rule would not have a significant economic impact on a substantial number of small entities. The Board cannot at this time determine whether the proposed Guidelines would have significant economic impact on a substantial number of small entities as defined by the RFA. Therefore, pursuant to subsections 603(b) and (c) of the RFA, the Board provides the following initial regulatory flexibility analysis.

A. Reasons for Proposed Rule

The Board is requesting comment on the proposed interagency Guidelines published pursuant to section 501 of the G–L–B Act. Section 501 requires the Agencies to publish standards for financial institutions relating to administrative, technical, and physical standards to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

B. Statement of Objectives and Legal Basis

The objectives of the proposed Guidelines are described in the Supplementary Information section above. The legal basis for the proposed Guidelines is the G–L–B Act, sections 501 and 505 (15 U.S.C. 6801 and 6805).

C. Description/Estimate of Small Entities to Which the Rule Applies

The proposed Guidelines would apply to approximately 9,500 institutions, including state member banks and certain of their subsidiaries, bank holding companies and certain of their subsidiaries, state-licensed uninsured branches and agencies of foreign banks, and Edge and agreement corporations. The Board estimates that over 4,500 of the covered institutions are small institutions with assets less than $100 million.

D. Projected Reporting, Recordkeeping and Other Compliance Requirements

The G–L–B Act and the proposed Guidelines require a covered institution to develop an information security program to safeguard customer information. The Guidelines will apply to all covered institutions regardless of size. Development of an information security program involves assessing risks to customer information, establishing policies, procedures, and training to control risks, testing the program's effectiveness, and managing and monitoring service providers. A covered institution may require professional skills to develop an information security program, including the skills of computer security professionals and lawyers.

The Board believes that the establishment of information security programs is a sound business practice for the covered institutions that is already addressed by existing supervisory procedures. Although some institutions may need to establish or enhance information security programs to comply with the proposed Guidelines, the cost of doing so is not known. Neverthless, the Board is concerned about the potential impact on community banks and will be reviewing current information security practices at smaller institutions during the comment period. The Board seeks any information or comment on the costs of establishing information security programs as detailed in the proposed Guidelines, particularly for smaller institutions. The Board welcomes comment on the appropriate level of detail and degree of flexibility in the proposed Guidelines and on the potential cost of particular provisions in the proposed Guidelines.

The Board does not believe that there are information collection requirements imposed by the proposed Guidelines.

E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules

The Board is unable to identify any statutes or rules which would overlap or conflict with the requirement to develop and implement an information security program. The Board seeks comment and information about any such statutes or rules, as well as any other state, local, or industry rules or policies that require a covered institution to implement business practices that would overlap or conflict with the requirements of the proposed Guidelines.

F. Discussion of Significant Alternatives

The proposed Guidelines attempt to clarify the statutory requirements for all covered entities, including small entities. The proposed Guidelines are intended to provide substantial flexibility so that any institution, regardless of size, may adopt an information security program tailored to its individual needs. Neverthless, the Board is concerned about the potential impact on community banks and will be reviewing current information security practices at smaller institutions during the comment period. The Board seeks comment on elements that would be most useful in a Compliance Guide to be issued in conjunction with the final Guidelines. In addition, the Board welcomes comment on any significant alternatives to the proposed Guidelines that would provide adequate guidance regarding expectations for compliance with the G–L–B Act. The Board seeks any information or comment on cost-effective, sound information security programs and practices implemented by financial institutions, including community banks.

FDIC: The Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA) requires an agency to publish an initial regulatory flexibility analysis with a proposed rule whenever the agency is required to publish a general notice of proposed rulemaking for a proposed rule, except to the extent provided in the RFA. Pursuant to section 603 of the RFA, the FDIC provides the following initial regulatory flexibility analysis.

A. Reasons for Proposed Rule

The FDIC is requesting comment on the proposed interagency Guidelines published pursuant to section 501 of the G–L–B Act. Section 501 requires the Agencies to publish standards for financial institutions relating to administrative, technical, and physical standards to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any

anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. The proposed standards do not represent any change in the policies of the FDIC; rather they implement the G–L–B Act requirement to provide appropriate standards relating to the security and confidentiality of customer records. The FDIC requests comment on whether small entities would be required to amend their operations in order to comply with the proposed standards and the costs for such compliance.

B. Statement of Objectives and Legal Basis

The **SUPPLEMENTARY INFORMATION** section above contains this information. The legal basis for the proposed rule is the G–L–B Act.

C. Description /Estimate of Small Entities to Which the Rule Applies

The proposed Guidelines would apply to all FDIC-insured state nonmember banks, approximately 3,700 of which are small entities as defined by the RFA.

D. Projected Reporting, Recordkeeping and Other Compliance Requirements

The FDIC does not believe that there are new reporting or recordkeeping requirements imposed by the proposed rule as defined by the Regulatory Flexibility Act (5 U.S.C. 603). Other compliance requirements of the proposed guidelines are applicable to all financial institutions subject to the jurisdiction of the FDIC and are discussed in the **SUPPLEMENTARY INFORMATION** section above. The G–L–B Act and the proposed Guidelines require all financial institutions subject to the jurisdiction of the FDIC to develop an information security program to safeguard customer information. The Guidelines will apply to all such covered institutions regardless of size. Development of an information security program involves assessing risks to customer information, establishing policies, procedures, and training to control risks, testing the program's effectiveness, and managing and monitoring service providers. A covered institution may require professional skills to develop an information security program, including the skills of computer security professionals and lawyers.

The FDIC believes that the establishment of information security programs is a sound business practice for the covered institutions that is already addressed by existing supervisory procedures. Although some institutions may need to enhance information security programs, the cost of doing so is not known. The FDIC seeks any information or comment on the costs of establishing information security programs.

E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules

The FDIC is unable to identify any statutes or rules that would overlap or conflict with the requirement to develop and implement an information security program. The FDIC seeks comment and information about any such statutes or rules, as well as any other state, local, or industry rules or policies that require a financial institution subject to its jurisdiction to implement business practices that would comply with the requirements of the proposed Guidelines.

F. Discussion of Significant Alternatives

As previously noted, the G–L–B Act requires the FDIC to establish appropriate standards for financial institutions under its jurisdiction relating to the security and confidentiality of customer records. These proposed Guidelines attempt to clarify the statutory requirements for all covered entities, including small entities. These proposed Guidelines also provide substantial flexibility so that any institution, regardless of size, may adopt an information security program tailored to its individual needs. The FDIC welcomes comment on any significant alternatives, consistent with the G–L–B Act that would minimize the impact on small entities.

OTS: The Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA) requires OTS to publish an initial regulatory flexibility analysis with this proposed rule unless OTS can certify that the proposed rule would not have a significant economic impact on a substantial number of small entities. Because OTS cannot at this time determine what impact this proposal would have on small entities, OTS provides the following initial regulatory flexibility analysis.

A. Reasons for Proposed Action

OTS makes this proposal pursuant to section 501 of the G–L–B Act. Section 501 requires OTS to publish standards for the thrift industry relating to administrative, technical, and physical safeguards to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

B. Objectives of and Legal Basis for Proposal

The **SUPPLEMENTARY INFORMATION** section above contains this information. The legal bases for the proposed action are: section 501 of the G–L–B Act; section 39 of the FDIA; and sections 2, 4, and 5 of the Home Owners' Loan Act (12 U.S.C. 1462, 1463, and 1464).

C. Description of Entities to Which Proposal Would Apply

This proposal would apply to all savings associations whose deposits are FDIC insured, and subsidiaries of such savings associations, except subsidiaries that are brokers, dealers, persons providing insurance, investment companies, and investment advisers.[7] There are approximately 487 such small savings associations, approximately 97 of which have subsidiaries.

D. Projected Reporting, Recordkeeping, and Other Compliance Requirements; Skills Required

The proposed rule does not contain any specific reporting requirements. However, it would require institutions to maintain certain records documenting compliance with the proposed rule, as detailed more specifically above.

The statute and the proposed rule require a covered institution to develop an information security program to safeguard customer information. Developing such a program involves assessing risks to customer information, establishing policies, procedures, and training to control risks, testing the program's effectiveness, and managing and monitoring service providers. OTS believes that establishing an information security program is a sound business practice for covered institutions. However, some institutions may need to establish or enhance information security programs. The cost of doing so is unknown. OTS seeks information and comment on the costs of establishing and operating information security programs.

Compliance with the proposed rule would require professional skills, especially skills of computer hardware and software professionals. Professional skills would be necessary to assess information security needs, design and

[7] For purposes of the Regulatory Flexibility Act, a small savings association is one with less that $100 million in assets. 13 CFR 121.201 (Division H).

implement an information security program, and to monitor service providers. The particular skills needed will depend on the nature of each institution's customer information systems. Institutions with sophisticated and extensive computerization would need far more skills to comply with the proposed rules than would institutions with little computerization. As a result, small entities are likely to have less burdensome compliance needs than large entities.

E. Significant Alternatives

The G–L–B Act requires OTS to establish standards for information security standards, but does not mandate the specific form that those standards must take. OTS has considered different alternatives for these standards, considering the burden on small institutions. OTS considered exempting small institutions entirely from the requirement to implement any information security standards. However, OTS does not believe that Congress has authorized OTS to exempt small institutions. Section 501(b) of the G–L–B Act requires OTS to establish standards for the institutions within OTS's jurisdiction, without regard to the institution's size.

OTS has also considered an alternative of publishing standards using language the same, or nearly the same, as that in section 501(b) of the G–L–B Act. The statutory language is broad and general. This alternative would give institutions maximum flexibility in implementing information security protections. It would also ensure that institutions would not be at a competitive disadvantage with other types of financial institutions not subject to the Agencies' information security standards. This alternative has disadvantages, however. Because the statutory language is very general, this alternative would not give institutions information about what risks need to be addressed or what types of protections are appropriate. Small institutions in particular may need guidance in this area. OTS welcomes comments on whether the proposed guidelines have too much or too little detail. How would changing the level of detail affect institutions' security practices?

OTS has proposed guidelines that would describe appropriate steps institutions must take to ensure the security of their customer information. While describing appropriate steps, OTS proposes flexible guidelines to let each institution design individual information standards appropriate for the institution's particular circumstances.

OTS is considering whether to adopt the proposed information security standards as guidance or as a regulation. OTS solicits comments on whether the regulatory burden on small entities would differ depending on the form of the standards. If so, how and to what extent?

OTS welcomes comments on the appropriateness of its approach, and on any other alternatives that would satisfy the objectives of this proposal.

F. Federal Rules That Duplicate, Overlap, or Conflict With the Proposal

OTS is unaware of any statutes or rules that would overlap or conflict with the requirement to develop and implement an information security program. OTS seeks comment and information about any such statutes or rules, as well as other rules or policies that require covered institutions to implement business practices that would comply with the proposed guidelines.

C. Executive Order 12866

OCC: The Comptroller of the Currency has determined that this proposed rule, if adopted as a final rule, does not constitute a ''significant regulatory action'' for the purposes of Executive Order 12866. The OCC issued the proposed Guidelines in accordance with the requirements of Sections 501 and 505(b) of the G–L–B Act and not under its own authority. The standards established by the Guidelines reflect good business practices and guidance previously issued by the OCC and the FFIEC. Accordingly, the OCC believes that most institutions already have information security programs in place.

Nevertheless, the OCC acknowledges that the proposed Guidelines may impose costs on some institutions by requiring them to formalize or enhance their existing information security programs. Therefore, the OCC invites institutions and the public to provide any cost estimates and related data that they think would be useful to the agency in evaluating the overall costs of the proposed Guidelines. The OCC will review any comments and cost data provided carefully and will revisit the cost aspects of the proposed Guidelines in developing the final rule.

OTS: OTS has determined that this proposed rule, if adopted as a final rule, would not constitute a ''significant regulatory action'' for the purposes of Executive Order 12866. OTS issued the proposed guidelines as required by sections 501 and 505(b) of the G–L–B Act and not under its own authority. The guidelines reflect good business practices that many institutions already follow. Further, OTS believes that any costs of complying with the guidelines would be below the thresholds prescribed in the Executive Order. Nevertheless, OTS acknowledges that the proposed guidelines may impose costs on some institutions by requiring them to formalize or enhance their existing information security programs. Therefore, OTS invites institutions and the public to provide any cost estimates and related data that they think would be useful to the agency in evaluating the overall costs of the proposed guidelines. OTS will carefully review any comments and cost data provided and will revisit the cost aspects of the proposed guidelines in developing the final rule.

D. Unfunded Mandates Act of 1995

OCC: Section 202 of the Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1532 (Unfunded Mandates Act), requires that an agency prepare a budgetary impact statement before promulgating any rule likely to result in a federal mandate that may result in the expenditure by state, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year. If a budgetary impact statement is required, section 205 of the Unfunded Mandates Act also requires the agency to identify and consider a reasonable number of regulatory alternatives before promulgating the rule. However, an agency is not required to assess the effects of its regulatory actions on the private sector to the extent that such regulations incorporate requirements specifically set forth in law. 2 U.S.C. 1531.

The OCC believes that most institutions have already established an information security program because it is a sound business practice that also has been addressed in existing supervisory guidance. Therefore, the OCC has determined that this proposed rule is unlikely to result in expenditures by state, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year. Accordingly, the OCC has not prepared a budgetary impact statement or specifically addressed the regulatory alternatives considered.

OTS: Section 202 of the Unfunded Mandates Act requires that an agency prepare a budgetary impact statement before promulgating any rule likely to result in a federal mandate that may result in the expenditure by state, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year. If a budgetary impact statement is required, section 205 of the Unfunded Mandates Act also

requires the agency to identify and consider a reasonable number of regulatory alternatives before promulgating the rule. However, an agency is not required to assess the effects of its regulatory actions on the private sector to the extent that such regulations incorporate requirements specifically set forth in law. 2 U.S.C. 1531.

OTS has determined that this proposed rule is unlikely to result in expenditures by state, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year. Accordingly, the OTS has not prepared a budgetary impact statement or specifically addressed the regulatory alternatives, except as described in the OTS's initial regulatory flexibility analysis earlier in this preamble.

IV. Solicitation of Comments on Use of Plain Language

Section 722 of the G–L–B Act requires the federal banking agencies to use plain language in all proposed and final rules published after January 1, 2000. We invite your comments on how to make this proposal easier to understand. For example:

- Have we organized the material to suit your needs? If not, how could this material be better organized?
- Are the requirements in the Guidelines clearly stated? If not, how could the Guidelines be more clearly stated?
- Do the Guidelines contain technical language or jargon that is not clear? If so, which language requires clarification?
- Would a different format (grouping and order of sections, use of headings, paragraphing) make the Guidelines easier to understand? If so, what changes to the format would make the Guidelines easier to understand?
- Would more, but shorter, sections be better? If so which sections should be changed?
- What else could we do to make the Guidelines easier to understand?

List of Subjects

12 CFR Part 30

Banks, banking, Consumer protection, National banks, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 208

Banks, banking, Consumer protection, Federal Reserve System, Foreign banking, Holding companies, Information, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 211

Exports, Federal Reserve System, Foreign banking, Holding companies, Investments, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 225

Administrative practice and procedure, Banks, banking, Federal Reserve System, Holding companies, Privacy, Reporting and recordkeeping requirements, securities.

12 CFR Part 263

Administrative practice and procedure, Claims, Crime, Equal access in justice, Federal Reserve System, Lawyers, Penalties.

12 CFR Part 308

Administrative practice and procedure, Banks, banking, Claims, Crime, Equal access of justice, Lawyers, Penalties, State nonmember banks.

12 CFR Part 364

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and soundness.

12 CFR Part 568

Reporting and recordkeeping requirements, Savings associations, Security measures.

12 CFR Part 570

Consumer protection, Privacy, Savings associations.

Office of the Comptroller of the Currency

12 CFR Chapter I

Authority and Issuance

For the reasons set forth in the joint preamble, part 30 of the chapter I of title 12 of the Code of Federal Regulations is proposed to be amended as follows:

PART 30—SAFETY AND SOUNDNESS STANDARDS

1. The authority citation for part 30 is revised to read as follows:

Authority: 12 U.S.C. 93a, 1818, 1831p–1, 3102(b); 15 U.S.C. 6801, 6805(b)(1).

2. Revise § 30.1 to read as follows:

§ 30.1 Scope.

(a) This rule and the standards set forth in appendices A and B to this part apply to national banks and federal branches of foreign banks, that are subject to the provisions of section 39 of the Federal Deposit Insurance Act (section 39) (12 U.S.C. 1831p–1).

(b) The standards set forth in appendix B to this part also apply to uninsured national banks, federal branches and federal agencies of foreign banks, and the subsidiaries of any national bank, federal branch or federal agency of a foreign bank (except brokers, dealers, persons providing insurance, investment companies and investment advisers). Violation of these standards may be an unsafe and unsound practice within the meaning of 12 U.S.C. 1818.

3. In § 30.2, revise the last sentence to read as follows:

§ 30.2 Purpose.

* * * The Interagency Guidelines Establishing Standards for Safety and Soundness are set forth in appendix A to this part, and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information are set forth in appendix B to this part.

4. In § 30.3, revise paragraph (a) to read as follows:

§ 30.3 Determination and notification of failure to meet safety and soundness standard.

(a) *Determination.* The OCC may, based upon an examination, inspection, or any other information that becomes available to the OCC, determine that a bank has failed to satisfy the safety and soundness standards contained in the Interagency Guidelines Establishing Standards for Safety and Soundness set forth in appendix A to this part, and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth in appendix B to this part.

* * * * *

5. Revise Appendix B to part 30 to read as follows:

Appendix B to Part 30—Interagency Guidelines Establishing Standards For Safeguarding Customer Information

Table of Contents

I. Introduction
A. Scope
B. Preservation of Existing Authority
C. Definitions
II. Standards for Safeguarding Customer Information
A. Information Security Program
B. Objectives
III. Development and Implementation of Customer Information Security Program
A. Involve the Board of Directors and Management
B. Assess Risk
C. Manage and Control Risk
D. Oversee Outsourcing Arrangements
E. Implement the Standards

I. Introduction

The Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12

U.S.C. 1831p–1), and sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

A. Scope. The Guidelines apply to customer information maintained by or on behalf of entities over which the OCC has authority. Such entities, referred to as ''the bank,'' are national banks, federal branches and federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

B. Preservation of Existing Authority. Neither section 39 nor these Guidelines in any way limit the authority of the OCC to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. The OCC may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the OCC.

C. Definitions. For purposes of the Guidelines, the following definitions apply:

1. In general. For purposes of the Guidelines, except as modified in the Guidelines or unless the context otherwise requires, the terms used have the same meanings as set forth in sections 3 and 39 of the Federal Deposit Insurance Act (12 U.S.C. 1813 and 1831p–1).

2. *Customer information* means any records, data, files, or other information containing nonpublic personal information, as defined in § 40.3(n) of this chapter, about a customer, whether in paper, electronic or other form, that are maintained by or on behalf of the bank.

3. *Customer* means any customer of the bank as defined in § 40.3(h) of this chapter.

4. *Service provider* means any person or entity that maintains or processes customer information on behalf of the bank, or is otherwise granted access to customer information through its provision of services to the bank.

5. *Board of directors,* in the case of a branch or agency of a foreign bank means the managing official in charge of the branch or agency.

6. *Customer information systems* means the electronic or physical methods used to access, collect, store, use, transmit and protect customer information.

II. Standards for Safeguarding Customer Information

A. Information Security Program. Each bank shall implement a comprehensive information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities.

B. Objectives. A bank's information security program shall:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer or risk to the safety and soundness of the bank.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors and Management.

1. The board of directors of each bank shall:

a. Approve the bank's written information security policy and program that complies with these Guidelines; and

b. Oversee efforts to develop, implement, and maintain an effective information security program.

2. The bank's management shall develop, implement, and maintain an effective information security program. In conjunction with its responsibility to implement the bank's information security program, management of each bank shall regularly:

a. Evaluate the impact on the bank's security program of changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems;

b. Document its compliance with these Guidelines; and

c. Report to the board on the overall status of the information security program, including material matters related to the following: risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements in the information security program.

B. Assess Risk. To achieve the objectives of its information security program, each bank shall:

1. Identify and assess the risks that may threaten the security, confidentiality, or integrity of customer information systems. As part of the risk assessment, a bank shall determine the sensitivity of customer information and the internal or external threats to the bank's customer information systems.

2. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

3. Monitor, evaluate, and adjust its risk assessment in light of any relevant changes to technology, the sensitivity of customer information, and internal or external threats to information security.

C. Manage and Control Risk. As part of a comprehensive risk management plan, each bank shall:

1. Establish written policies and procedures that are adequate to control the identified risks and achieve the overall objectives of the bank's information security program. Policies and procedures shall be commensurate with the sensitivity of the information as well as the complexity and scope of the bank and its activities. In establishing the policies and procedures, each bank should consider appropriate:

a. Access rights to customer information;

b. Access controls on customer information systems, including controls to authenticate and grant access only to authorized individuals and companies;

c. Access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities;

d. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

e. Procedures to confirm that customer information system modifications are consistent with the bank's information security program;

f. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

g. Contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by service providers;

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

i. Response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected;

j. Protection against destruction of customer information due to potential physical hazards, such as fire and water damage; and

k. Response programs to preserve the integrity and security of customer information in the event of computer or other technological failure, including, where appropriate, reconstructing lost or damaged customer information.

2. Train staff to recognize, respond to, and, where appropriate, report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain customer information.

3. Regularly test the key controls, systems and procedures of the information security program to confirm that they control the risks and achieve the overall objectives of the bank's information security program. The frequency and nature of such tests should be determined by the risk assessment, and adjusted as necessary to reflect changes in internal and external conditions. Tests shall be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs. Test results shall be reviewed by independent third parties or staff independent of those that conducted the test.

4. Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information security.

D. Oversee Outsourcing Arrangements. The bank continues to be responsible for safeguarding customer information even when it gives a service provider access to that

information. The bank must exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect customer information and customer information systems consistent with these Guidelines.

E. Implement the Standards. Each bank is to take appropriate steps to fully implement an information security program pursuant to these Guidelines by July 1, 2001.

Dated: June 5, 2000.

John D. Hawke, Jr.,

Comptroller of the Currency.

Federal Reserve System

12 CFR Chapter II

Authority and Issuance

For the reasons set forth in the joint preamble, parts 208, 211, 225, and 263 of chapter II of title 12 of the Code of Federal Regulations are proposed to be amended as follows:

PART 208—MEMBERSHIP OF STATE BANKING INSTITUTIONS IN THE FEDERAL RESERVE SYSTEM (REGULATION H)

1. The authority citation for 12 CFR part 208 is revised to read as follows:

Authority: 12 U.S.C. 24, 36, 92a, 93a, 248(a), 248(c), 321–338a, 371d, 461, 481–486, 601, 611, 1814, 1816, 1818, 1820(d)(9), 1823(j), 1828(o), 1831, 1831o, 1831p–1, 1831r–1, 1835a, 1882, 2901–2907, 3105, 3310, 3331–3351, and 3906–3909; 15 U.S.C. 78b, 78*l*(b), 78*l*(g), 78l(i), 78o–4(c)(5), 78q, 78q–1, 78w, 6801, and 6805; 31 U.S.C. 5318; 42 U.S.C. 4012a, 4104a, 4104b, 4106, and 4128.

2. Amend § 208.3 to revise paragraph (d)(1) to read as follows:

§ 208.3 Application and conditions for membership in the Federal Reserve System.

* * * * *

(d) *Conditions of membership.* (1) *Safety and soundness.* Each member bank shall at all times conduct its business and exercise its powers with due regard to safety and soundness. Each member bank shall comply with the Interagency Guidelines Establishing Standards for Safety and Soundness prescribed pursuant to section 39 of the FDI Act (12 U.S.C. 1831p–1), set forth in appendix D–1 to this part, and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information prescribed pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805), set forth in appendix D–2 to this part.

* * * * *

3. Revise appendix D–2 to read as follows:

Appendix D–2 To Part 208—Interagency Guidelines Establishing Standards For Safeguarding Customer Information

Table of Contents

I. Introduction
A. Scope
B. Preservation of Existing Authority
C. Definitions
II. Standards for Safeguarding Customer Information
A. Information Security Program
B. Objectives
III. Development and Implementation of Customer Information Security Program
A. Involve the Board of Directors and Management
B. Assess Risk
C. Manage and Control Risk
D. Oversee Outsourcing Arrangements
E. Implement the Standards

I. Introduction

These Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805), in the same manner, to the extent practicable, as standards prescribed pursuant to section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1). These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

A. Scope. The Guidelines apply to customer information maintained by or on behalf of state member banks (banks) and their nonbank subsidiaries, except for brokers, dealers, persons providing insurance, investment companies, and investment advisors. Pursuant to §§ 211.9 and 211.24 of this chapter, these guidelines also apply to customer information maintained by or on behalf of Edge corporations, agreement corporations, and uninsured state-licensed branches or agencies of a foreign bank.

B. Preservation of Existing Authority. Neither section 39 nor these Guidelines in any way limit the authority of the Board to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. The Board may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the Board.

C. Definitions. For purposes of the Guidelines, the following definitions apply:

1. *In general.* For purposes of the Guidelines, except as modified in the Guidelines or unless the context otherwise requires, the terms used have the same meanings as set forth in sections 3 and 39 of the Federal Deposit Insurance Act (12 U.S.C. 1813 and 1831p–1).

2. *Customer information* means any records, data, files, or other information containing nonpublic personal information, as defined in § 216.3(n) of this chapter, about a customer, whether in paper, electronic or other form, that are maintained by or on behalf of the bank.

3. *Customer* means any customer of the bank as defined in § 216.3(h) of this chapter.

4. *Service provider* means any person or entity that maintains or processes customer information on behalf of the bank, or is otherwise granted access to customer information through its provision of services to the bank.

5. *Board of directors,* in the case of a branch or agency of a foreign bank means the managing official in charge of the branch or agency.

6. *Customer information systems* means the electronic or physical methods used to access, collect, store, use, transmit and protect customer information.

7. *Subsidiary* means any company controlled by a bank, except a broker, dealer, person providing insurance, investment company, investment advisor, insured depository institution, or subsidiary of an insured depository institution.

II. Standards for Safeguarding Customer Information

A. Information Security Program. Each bank shall implement a comprehensive information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. A bank also shall ensure that each of its subsidiaries is subject to a comprehensive information security program. The bank may fulfill this requirement either by including a subsidiary within the scope of the bank's comprehensive information security program or by causing the subsidiary to implement a separate comprehensive information security program in accordance with the standards and procedures in sections II and III of this appendix that apply to banks.

B. Objectives. A bank's information security program shall:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer or risk to the safety and soundness of the bank.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors and Management.

1. The board of directors of each bank shall:

a. Approve the bank's written information security policy and program that complies with these Guidelines; and

b. Oversee efforts to develop, implement, and maintain an effective information security program.

2. The bank's management shall develop, implement, and maintain an effective information security program. In conjunction with its responsibility to implement the bank's information security program, management of each bank shall regularly:

a. Evaluate the impact on the bank's security program of changing business arrangements, such as mergers and acquisitions, alliances and joint ventures,

outsourcing arrangements, and changes to customer information systems;

b. Document its compliance with these Guidelines; and

c. Report to the board on the overall status of the information security program, including material matters related to: risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements in the information security program.

B. Assess Risk. To achieve the objectives of its information security program, each bank shall:

1. Identify and assess the risks that may threaten the security, confidentiality, or integrity of customer information systems. As part of the risk assessment, a bank shall determine the sensitivity of customer information and the internal or external threats to the bank's customer information systems.

2. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risk.

3. Monitor, evaluate, and adjust its risk assessment in light of any relevant changes to technology, the sensitivity of customer information, and internal or external threats to information security.

C. Manage and Control Risk. As part of a comprehensive risk management plan, each bank shall:

1. Establish written policies and procedures that are adequate to control the identified risks and achieve the overall objectives of the bank's information security program. Policies and procedures shall be commensurate with the sensitivity of the information as well as the complexity and scope of the bank and its activities. In establishing the policies and procedures, each bank should consider appropriate:

a. Access rights to customer information;

b. Access controls on customer information systems, including controls to authenticate and grant access only to authorized individuals and companies;

c. Access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities;

d. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

e. Procedures to confirm that customer information system modifications are consistent with the bank's information security program;

f. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

g. Contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by service providers;

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

i. Response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected;

j. Protection against destruction of customer information due to potential physical hazards, such as fire and water damage; and

k. Response programs to preserve the integrity and security of customer information in the event of computer or other technological failure, including, where appropriate, reconstructing lost or damaged customer information.

2. Train staff to recognize, respond to, and, where appropriate, report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain customer information.

3. Regularly test the key controls, systems and procedures of the information security program to confirm that they control the risks and achieve the overall objectives of the bank's information security program. The frequency and nature of such tests should be determined by the risk assessment, and adjusted as necessary to reflect changes in internal and external conditions. Tests shall be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs. Test results shall be reviewed by independent third parties or staff independent of those that conducted the test.

4. Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information security.

D. Oversee Outsourcing Arrangements. The bank continues to be responsible for safeguarding customer information even when it gives a service provider access to that information. The bank must exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect customer information and customer information systems consistent with these Guidelines.

E. Implement the Standards. Each bank is to take appropriate steps to fully implement an information security program pursuant to these Guidelines by July 1, 2001.

PART 211—INTERNATIONAL BANKING OPERATIONS (REGULATION K)

4. The authority citation for part 211 is revised to read as follows:

Authority: 12 U.S.C. 221 *et seq.*, 1818, 1835a, 1841 *et seq.*, 3101 *et seq.*, and 3901 *et seq.*; 15 U.S.C. 6801 and 6805.

5. Add new § 211.9 to read as follows:

§ 211.9 Protection of customer information.

An Edge or agreement corporation shall comply with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information prescribed pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805), set forth in appendix D–2 to part 208 of this chapter.

6. In § 211.24, add new paragraph (i) to read as follows:

§ 211.24 Approval of offices of foreign banks; procedures for applications; standards for approval; representative-office activities and standards for approval; preservation of existing authority; reports of crimes and suspected crimes; government securities sales practices.

* * * * *

(i) *Protection of customer information.* An uninsured state-licensed branch or agency of a foreign bank shall comply with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information prescribed pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805), set forth in appendix D–2 to part 208 of this chapter.

PART 225—BANK HOLDING COMPANIES AND CHANGE IN BANK CONTROL (REGULATION Y)

7. The authority citation for part 225 is revised to read as follows:

Authority: 12 U.S.C. 1817(j)(13), 1818, 1828(o), 1831i, 1831p–1, 1843(c)(8), 1844(b), 1972(1), 3106, 3108, 3310, 3331–3351, 3907, and 3909; 15 U.S.C. 6801 and 6805.

8. In § 225.1, add new paragraph (c)(16) to read as follows:

§ 225.1 Authority, purpose, and scope.

* * * * *

(c) * * *

(16) *Appendix F* contains the Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

9. In § 225.4, add new paragraph (g) to read as follows:

§ 225.4 Corporate practices.

* * * * *

(g) *Protection of nonpublic personal information.* A bank holding company, including a bank holding company that is a financial holding company, shall comply with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, as set forth in appendix F of this part, prescribed pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805).

10. Add new appendix F to read as follows:

Appendix F To Part 225—Interagency Guidelines Establishing Standards For Safeguarding Customer Information

Table of Contents

I. Introduction
A. Scope

B. Preservation of Existing Authority
C. Definitions
II. Standards for Safeguarding Customer Information
A. Information Security Program
B. Objectives
III. Development and Implementation of Customer Information Security Program
A. Involve the Board of Directors and Management
B. Assess Risk
C. Manage and Control Risk
D. Oversee Outsourcing Arrangements
E. Implement the Standards

I. Introduction

These Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805). These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

A. Scope. The Guidelines apply to customer information maintained by or on behalf of bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisors), for which the Board has supervisory authority.

B. Preservation of Existing Authority. These Guidelines do not in any way limit the authority of the Board to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. The Board may take action to enforce these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the Board.

C. Definitions. For purposes of the Guidelines, the following definitions apply:

1. *In general.* For purposes of the Guidelines, except as modified in the Guidelines or unless the context otherwise requires, the terms used have the same meanings as set forth in sections 3 and 39 of the Federal Deposit Insurance Act (12 U.S.C. 1813 and 1831p–1).

2. *Customer information* means any records, data, files, or other information containing nonpublic personal information, as defined in § 216.3(n) of this chapter, about a customer, whether in paper, electronic or other form, that are maintained by or on behalf of the bank holding company.

3. *Customer* means any customer of the bank holding company as defined in § 216.3(h) of this chapter.

4. *Service provider* means any person or entity that maintains or processes customer information on behalf of the bank holding company, or is otherwise granted access to customer information through its provision of services to the bank holding company.

5. *Board of directors,* in the case of a branch or agency of a foreign bank means the managing official in charge of the branch or agency.

6. *Customer information systems* means the electronic or physical methods used to access, collect, store, use, transmit and protect customer information.

7. *Subsidiary* means any company controlled by a bank holding company, except a broker, dealer, person providing insurance, investment company, investment advisor, insured depository institution, or subsidiary of an insured depository institution.

II. Standards for Safeguarding Customer Information

A. Information Security Program. Each bank holding company shall implement a comprehensive information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank holding company and the nature and scope of its activities. A bank holding company also shall ensure that each of its subsidiaries is subject to a comprehensive information security program. The bank holding company may fulfill this requirement either by including a subsidiary within the scope of the bank holding company's comprehensive information security program or by causing the subsidiary to implement a separate comprehensive information security program in accordance with the standards and procedures in sections II and III of this appendix that apply to bank holding companies.

B. Objectives. A bank holding company's information security program shall:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer or risk to the safety and soundness of the bank holding company.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors and Management.

1. The board of directors of each bank holding company shall:

a. Approve the bank holding company's written information security policy and program that complies with these Guidelines; and

b. Oversee efforts to develop, implement, and maintain an effective information security program.

2. The bank holding company's management shall develop, implement, and maintain an effective information security program. In conjunction with its responsibility to implement the bank holding company's information security program, management of each bank holding company shall regularly:

a. Evaluate the impact on the bank holding company's security program of changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems;

b. Document its compliance with these Guidelines; and

c. Report to the board on the overall status of the information security program, including material matters related to: risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements in the information security program.

B. Assess Risk. To achieve the objectives of its information security program, each bank holding company shall:

1. Identify and assess the risks that may threaten the security, confidentiality, or integrity of customer information systems. As part of the risk assessment, a bank holding company shall determine the sensitivity of customer information and the internal or external threats to the bank holding company's customer information systems.

2. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks identified in section III.B.1 of this appendix.

3. Monitor, evaluate, and adjust its risk assessment in light of any relevant changes to technology, the sensitivity of customer information, and internal or external threats to information security.

C. Manage and Control Risk. As part of a comprehensive risk management plan, each bank holding company shall:

1. Establish written policies and procedures that are adequate to control the identified risks and achieve the overall objectives of the bank holding company's information security program. Policies and procedures shall be commensurate with the sensitivity of the information as well as the complexity and scope of the bank holding company and its activities. In establishing the policies and procedures, each bank holding company should consider appropriate:

a. Access rights to customer information;

b. Access controls on customer information systems, including controls to authenticate and grant access only to authorized individuals and companies;

c. Access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities;

d. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

e. Procedures to confirm that customer information system modifications are consistent with the bank holding company's information security program;

f. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

g. Contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by service providers;

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

i. Response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected;

j. Protection against destruction of customer information due to potential physical hazards, such as fire and water damage; and

k. Response programs to preserve the integrity and security of customer information in the event of computer or other technological failure, including, where appropriate, reconstructing lost or damaged customer information.

2. Train staff to recognize, respond to, and, where appropriate, report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain customer information.

3. Regularly test the key controls, systems and procedures of the information security program to confirm that they control the risks and achieve the overall objectives of the bank holding company's information security program. The frequency and nature of such tests should be determined by the risk assessment, and adjusted as necessary to reflect changes in internal and external conditions. Tests shall be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs. Test results shall be reviewed by independent third parties or staff independent of those that conducted the test.

4. Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information security.

D. Oversee Outsourcing Arrangements. The bank holding company continues to be responsible for safeguarding customer information even when it gives a service provider access to that information. The bank holding company must exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect customer information and customer information systems consistent with these Guidelines.

E. Implement the Standards. Each bank holding company is to take appropriate steps to fully implement an information security program pursuant to these Guidelines by July 1, 2001.

PART 263—RULES OF PRACTICE FOR HEARINGS

11. The authority citation for part 263 is revised to read as follows:

Authority: 5 U.S.C. 504; 12 U.S.C. 248, 324, 504, 505, 1817(j), 1818, 1828(c), 1831o, 1831p–1, 1847(b), 1847(d), 1884(b), 1972(2)(F), 3105, 3107, 3108, 3907, 3909; 15 U.S.C. 21, 78o–4, 78o–5, 78u–2, 6801, 6805; and 28 U.S.C. 2461 note.

12. Amend § 263.302 to revise paragraph (a) to read as follows:

§ 263.302 Determination and notification of failure to meet safety and soundness standard and request for compliance plan.

(a) *Determination.* The Board may, based upon an examination, inspection, or any other information that becomes available to the Board, determine that a bank has failed to satisfy the safety and soundness standards contained in the Interagency Guidelines Establishing Standards for Safety and Soundness or the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, set forth in appendices D–1 and D–2 to part 208 of this chapter, respectively.

* * * * *

By order of the Board of Governors of the Federal Reserve System, June 13, 2000.

Jennifer J. Johnson,

Secretary of the Board.

Federal Deposit Insurance Corporation

12 CFR Chapter III

Authority and Issuance

For the reasons set forth in the joint preamble, parts 308 and 364 of chapter III of title 12 of the Code of Federal Regulation are proposed to be amended as follows:

PART 308—RULES OF PRACTICE AND PROCEDURE

1. The authority citation for part 308 continues to read as follows:

Authority: 5 U.S.C. 504, 554–557; 12 U.S.C. 93(b), 164, 505, 1815(e), 1817, 1818, 1820, 1828, 1829, 1829b, 1831i, 1831o, 1831p–1, 1832(c), 1884(b), 1972, 3102, 3108(a), 3349, 3909, 4717; 15 U.S.C. 78(h) and (i), 78o–4(c), 78o–5, 78q–1, 78s, 78u, 78u–2, 78u–3 and 78w; 28 U.S.C. 2461 note; 31 U.S.C. 330, 5321; 42 U.S.C. 4012a; sec. 31001(s), Pub. L. 104–134, 110 Stat. 1321–358.

1. Amend § 308.302 to revise paragraph (a) to read as follows:

§ 308.302 Determination and notification of failure to meet a safety and soundness standard and request for compliance plan.

(a) Determination. The FDIC may, based upon an examination, inspection, or any other information that becomes available to the FDIC, determine that a bank has failed to satisfy the safety and soundness standards set out in part 364 of this chapter and in the Interagency Guidelines Establishing Standards for Safety and Soundness in appendix A and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information in appendix B to part 364 of this chapter.

* * * * *

PART 364—STANDARDS FOR SAFETY AND SOUNDNESS

2. The authority citation for part 364 is revised to read as follows:

Authority: 12 U.S.C. 1818 (Tenth), 1831p–1; 15 U.S.C. 6801(b), 6805(b)(1).

3. Amend § 364.101 to revise paragraph (b) to read as follows:

§ 364.101 Standards for safety and soundness.

* * * * *

(b) *Interagency Guidelines Establishing Standards for Safeguarding Customer Information.* The Interagency Guidelines Establishing Standards for Safeguarding Customer Information prescribed pursuant to section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1) and sections 501 and 505(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801, 6805(b)), as set forth in appendix B to this part, apply to all insured state nonmember banks, insured state licensed branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

4. Revise Appendix B to Part 364 to read as follows:

Appendix B to Part 364—Interagency Guidelines Establishing Standards for Safeguarding Customer Information

Table of Contents

I. Introduction
A. Scope
B. Preservation of Existing Authority
C. Definitions
II. Standards for Safeguarding Customer Information
A. Information Security Program
B. Objectives
III. Development and Implementation of Customer Information Security Program
A. Involve the Board of Directors and Management
B. Assess Risk
C. Manage and Control Risk
D. Oversee Outsourcing Arrangements
E. Implement the Standards

I. Introduction

The Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12 U.S.C. 1831p–1), and sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

A. Scope. The Guidelines apply to customer information maintained by or on behalf of entities for which the Federal Deposit Insurance Corporation (FDIC) has authority. Such entities are referred to in this appendix as ''the bank.'' These are banks insured by the FDIC (other than members of the Federal Reserve System), insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

B. Preservation of Existing Authority. Neither section 39 nor these Guidelines in any way limit the authority of the FDIC to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. The FDIC may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the FDIC.

C. Definitions. For purposes of the Guidelines, the following definitions apply:

1. *In general.* For purposes of the Guidelines, except as modified in the Guidelines or unless the context otherwise requires, the terms used have the same meanings as set forth in sections 3 and 39 of the Federal Deposit Insurance Act (12 U.S.C. 1813 and 1831p–1).

2. *Customer information* means any records, data, files, or other information containing nonpublic personal information, as defined in § 332.3(n) of this chapter (the Privacy Rule), about a customer, whether in paper, electronic or other form, that are maintained by or on behalf of the bank.

3. *Customer* means any customer of the bank as defined in § 332.3(h) of this chapter.

4. *Service provider* means any person or entity that maintains or processes customer information on behalf of the bank, or is otherwise granted access to customer information through its provision of services to the bank.

5. *Board of directors,* in the case of a branch or agency of a foreign bank means the managing official in charge of the branch or agency.

6. *Customer information systems* means the electronic or physical methods used to access, collect, store, use, transmit and protect customer information.

II. Standards for Safeguarding Customer Information

A. *Information Security Program.* Each bank shall implement a comprehensive information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities.

B. *Objectives.* A bank's information security program shall:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer or risk to the safety and soundness of the bank.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors and Management.

1. The board of directors of each bank shall:

a. Approve the bank's written information security policy and program that complies with these Guidelines; and

b. Oversee efforts to develop, implement, and maintain an effective information security program.

2. The bank's management shall develop, implement, and maintain an effective information security program. In conjunction with its responsibility to implement the bank's information security program, management of each bank shall regularly:

a. Evaluate the impact on the bank's security program of changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems;

b. Document its compliance with these Guidelines; and

c. Report to the board on the overall status of the information security program, including material matters related to: risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements in the information security program.

B. Assess Risk. To achieve the objectives of its information security program, each bank shall:

1. Identify and assess the risks that may threaten the security, confidentiality, or integrity of customer information systems. As part of the risk assessment, a bank shall determine the sensitivity of customer information and the internal or external threats to the bank's customer information systems.

2. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

3. Monitor, evaluate, and adjust its risk assessment in light of any relevant changes to technology, the sensitivity of customer information, and internal or external threats to information security.

C. *Manage and Control Risk.* As part of a comprehensive risk management plan, each bank shall:

1. Establish written policies and procedures that are adequate to control the identified risks and achieve the overall objectives of the bank's information security program. Policies and procedures shall be commensurate with the sensitivity of the information as well as the complexity and scope of the bank and its activities. In establishing the policies and procedures, each bank should consider appropriate:

a. Access rights to customer information;

b. Access controls on customer information systems, including controls to authenticate and grant access only to authorized individuals and companies;

c. Access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities;

d. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

e. Procedures to confirm that customer information system modifications are consistent with the bank's information security program;

f. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

g. Contract provisions and oversight mechanisms to protect the security of

customer information maintained or processed by service providers;

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

i. Response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected;

j. Protection against destruction of customer information due to potential physical hazards, such as fire and water damage; and

k. Response programs to preserve the integrity and security of customer information in the event of computer or other technological failure, including, where appropriate, reconstructing lost or damaged customer information.

2. Train staff to recognize, respond to, and, where appropriate, report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain customer information.

3. Regularly test the key controls, systems and procedures of the information security program to confirm that they control the risks and achieve the overall objectives of your information security program. The frequency and nature of such tests should be determined by the risk assessment, and adjusted as necessary to reflect changes in internal and external conditions. Tests shall be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs. Test results shall be reviewed by independent third parties or staff independent of those that conducted the test.

4. Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information security.

D. Oversee Outsourcing Arrangements. The bank continues to be responsible for safeguarding customer information even when it gives a service provider access to that information. The bank must exercise appropriate due diligence in managing and monitoring your outsourcing arrangements to confirm that your service providers have implemented an effective information security program to protect customer information and customer information systems consistent with these Guidelines.

E. Implement the Standards. Each bank is to take appropriate steps to fully implement an information security program pursuant to these Guidelines by July 1, 2001.

By order of the Board of Directors.

Dated at Washington, D.C., this 6th day of June, 2000.

Federal Deposit Insurance Corporation.

Robert E. Feldman,

Executive Secretary.

Office of Thrift Supervision

12 CFR Chapter V

Authority and Issuance

For the reasons set forth in the joint preamble, parts 568 and 570 of chapter V of title 12 of the Code of Federal regulations are proposed to be amended as follows:

PART 568—SECURITY PROCEDURES

1. The authority citation for part 568 is revised to read as follows:

Authority: Secs. 2–5, 82 Stat. 294–295 (12 U.S.C. 1881–1984); 12 U.S.C. 1831p–1; 15 U.S.C. 6801, 6805(b)(1).

2. Amend § 568.1 to revise paragraph (a) to read as follows:

§ 568.1 Authority, purpose, and scope.

(a) This part is issued by the Office of Thrift Supervision (''OTS'') pursuant to section 3 of the Bank Protection Act of 1968 (12 U.S.C. 1882), and sections 501 and 505(b)(1) of the Gramm-Leach-Bliley Act (12 U.S.C. 6801, 6805(b)(1). This part is applicable to savings associations. It requires each savings association to adopt appropriate security procedures to discourage robberies, burglaries, and larcenies and to assist in the identification and prosecution of persons who commit such acts. Section 568.5 of this part is applicable to savings associations and their subsidiaries (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). Section 568.5 of this part requires covered institutions to establish and implement appropriate administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

* * * * *

3. Add § 568.5 to read as follows:

§ 568.5 Protection of customer information.

Savings associations and their subsidiaries (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) must comply with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information prescribed pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805), set forth in appendix B to part 570 of this chapter.

PART 570—SUBMISSION AND REVIEW OF SAFETY AND SOUNDNESS COMPLIANCE PLANS AND ISSUANCE OF ORDERS TO CORRECT SAFETY AND SOUNDNESS DEFICIENCIES

4. Amend § 570.1 to add a sentence to the end of paragraph (a) and revise the last sentence of paragraph (b) to read as follows:

§ 570.1 Authority, purpose, scope and preservation of existing authority.

(a) * * * Appendix B to this part is further issued under sections 501(b) and 505 of the Gramm-Leach-Bliley Act (Pub. L. 106–102, 113 Stat. 1338 (1999)).

(b) * * * Interagency Guidelines Establishing Standards for Safeguarding Customer Information are set forth in appendix B to this part.

5. Amend § 570.2 to revise paragraph (a) to read as follows:

§ 570.2 Determination and notification of failure to meet safety and soundness stnadards and request for compliance plan.

(a) *Determination.* The OTS may, based upon an examination, inspection, or any other information that becomes available to the OTS, determine that a savings association has failed to satisfy the safety and soundness standards contained in the Interagency Guidelines Establishing Standards for Safety and Soundness as set forth in appendix A to this part or the Interagency Guidelines Establishing Standards for Safeguarding Customer Information as set forth in appendix B to this part.

* * * * *

6. Revise Appendix B to Part 570 to read as follows:

Appendix B to Part 570—Interagency Guidelines Establishing Standards for Safeguarding Customer Information

Table of Contents

I. Introduction
A. Scope
B. Preservation of Existing Authority
C. Definitions
II. Standards for Safeguarding Customer Information
A. Information Security Program
B. Objectives
III. Development and Implementation of Customer Information Security Program
A. Involve the Board of Directors and Management
B. Assess Risk
C. Manage and Control Risk
D. Oversee Outsourcing Arrangements
E. Implement the Standards

I. Introduction

The Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12 U.S.C. 1831p–1), and sections 501 and

505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

A. *Scope.* The Guidelines apply to customer information maintained by or on behalf of entities for which OTS has authority. For purposes of this appendix, these entities are savings associations whose deposits are FDIC-insured and any subsidiaries of such savings associations, except brokers, dealers, persons providing insurance, investment companies, and investment advisers. This appendix refers to such entities as ''you.''

B. *Preservation of Existing Authority.* Neither section 39 nor these Guidelines in any way limit the OTS's authority to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. OTS may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to OTS.

C. *Definitions.* For purposes of the Guidelines, the following definitions apply:

1. *In general.* For purposes of the Guidelines, except as modified in the Guidelines or unless the context otherwise requires, the terms used have the same meanings as set forth in sections 3 and 39 of the Federal Deposit Insurance Act (12 U.S.C. 1813 and 1831p–1).

2. *Customer information* means any records, data, files, or other information containing nonpublic personal information, as defined in 12 CFR 573.3(n), about a customer, whether in paper, electronic or other form, that you maintain or that are maintained on your behalf.

3. *Customer* means any of your customers, as defined in 12 CFR 573.3(h).

4. *Service provider* means any person or entity that maintains or processes customer information on your behalf, or is otherwise granted access to customer information through its provision of services to you.

5. *Customer information systems* means the electronic or physical methods used to access, collect, store, use, transmit and protect customer information.

II. Standards for Safeguarding Customer Information

A. *Information Security Program.* You shall implement a comprehensive information security program that includes administrative, technical, and physical safeguards appropriate to your size and complexity and the nature and scope of your activities.

B. *Objectives.* Your information security program shall:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer or risk to your safety and soundness.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors and Management.

1. Your board of directors shall:

a. Approve your written information security policy and program that complies with these Guidelines; and

b. Oversee efforts to develop, implement, and maintain an effective information security program.

2. Your management shall develop, implement, and maintain an effective information security program. In conjunction with its responsibility to implement your information security program, your management shall regularly:

a. Evaluate the impact on your security program of changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems;

b. Document its compliance with these Guidelines; and

c. Report to your board on the overall status of the information security program, including material matters related to; risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements in the information security program.

B. *Assess Risk.* To achieve the objectives of its information security program, you shall:

1. Identify and assess the risks that may threaten the security, confidentiality, or integrity of customer information systems. As part of the risk assessment, you shall determine the sensitivity of customer information and the internal or external threats to your customer information systems.

2. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

3. Monitor, evaluate, and adjust your risk assessment in light of any relevant changes to technology, the sensitivity of customer information, and internal or external threats to information security.

C. *Manage and Control Risk.* As part of a comprehensive risk management plan, you shall:

1. Establish written policies and procedures that are adequate to control the identified risks and achieve the overall objectives of your information security program. Policies and procedures shall be commensurate with the sensitivity of the information as well as the complexity and scope of you and your activities. In establishing the policies and procedures, you should consider appropriate:

a. Access rights to customer information;

b. Access controls on customer information systems, including controls to authenticate and grant access only to authorized individuals and companies;

c. Access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities;

d. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

e. Procedures to confirm that customer information system modifications are consistent with your information security program;

f. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

g. Contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by service providers;

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

i. Response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected;

j. Protection against destruction of customer information due to potential physical hazards, such as fire and water damage; and

k. Response programs to preserve the integrity and security of customer information in the event of computer or other technological failure, including, where appropriate, reconstructing lost or damaged customer information.

2. Train staff to recognize, respond to, and, where appropriate, report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain customer information.

3. Regularly test the key controls, systems and procedures of the information security program to confirm that they control the risks and achieve the overall objectives of your information security program. The frequency and nature of such tests should be determined by the risk assessment, and adjusted as necessary to reflect changes in internal and external conditions. Tests shall be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs. Test results shall be reviewed by independent third parties or staff independent of those that conducted the test.

4. Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information security.

D. *Oversee Outsourcing Arrangements.* You continue to be responsible for safeguarding customer information even when you give a service provider access to that information. You must exercise appropriate due diligence in managing and monitoring your outsourcing arrangements to confirm that your service providers have implemented an effective information security program to protect customer information and customer information systems consistent with these Guidelines.

E. *Implement the Standards.* You are to take appropriate steps to fully implement an information security program pursuant to these Guidelines by July 1, 2001.

Dated: June 9, 2000.

By the Office of Thrift Supervision.

Ellen Seidman,

Director.

[FR Doc. 00–15798 Filed 6–23–00; 8:45 am]

BILLING CODE 4810–33–P, 6210–01–P, 6714–01–P, 6720–01–P