SECURITY STANDARDS FOR CUSTOMER INFORMATION

FIL-22-2001
March 14, 2001

TO: CHIEF EXECUTIVE OFFICER AND COMPLIANCE OFFICER
SUBJECT: *Guidelines Establishing Standards for Safeguarding Customer Information*

The Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision have jointly approved and issued the attached guidelines establishing standards for safeguarding customer information as required by the Gramm-Leach-Bliley Act (GLBA).

GLBA requires the banking agencies to establish appropriate standards for financial institutions relating to the administrative, technical and physical safeguards of customer records and information. The standards' objectives are to:

- ensure the security and 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 result in substantial harm or inconvenience to any customer.

Information Security Program

The guidelines describe the agencies' expectations for creating, implementing and maintaining 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 guidelines also describe the oversight role of the institution's board of directors in this process and its continuing duty to evaluate and oversee the program's overall status. Institutions are required to:

- identify and assess the risks that may threaten customer information;
- develop a written plan containing policies and procedures to manage and control these risks;
- implement and test the plan; and
- adjust the plan on a continuing basis to account for changes in technology, sensitivity of customer information, and internal or external threats to information security.

Risk Assessment

The guidelines describe the elements of a comprehensive risk-management plan designed to control identified risks and achieve the overall objective of ensuring the security and confidentiality of customer information. They identify 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. The agencies intend that these elements will provide general parameters for institutions of varying sizes, scopes of operation and risk-management structures.

Involvement of the Board of Directors

The guidelines describe the responsibilities of the board of directors and management in developing and implementing an information security program. The board, or an appropriate board committee, is expected to:

- approve the institution's written information security program that complies with these guidelines; and
- oversee efforts to develop, implement and maintain an effective information security program, including regularly reviewing reports filed by management.

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, an institution should exercise appropriate due diligence in managing and monitoring its outsourcing arrangements.

For more information, please contact Jeffrey M. Kopchik (202-898-3872) or Thomas J. Tuzinski (202-898-6748) in the FDIC's Division of Supervision, or Robert A. Patrick (202-898-3757) in the FDIC's Legal Division.

Michael J. Zamorski
Acting Director

Attachment: Feb. 1, 2001, *Federal Register*, pages 8616-8641

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (800-276-6003 or 202-416-6940).

[Federal Register: February 1, 2001 (Volume 66, Number 22)]
[Rules and Regulations]
[Page 8615-8641]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr01fe01-9]

Part II

Department of the Treasury

Office of the Comptroller of the Currency

Office of Thrift Supervision

Federal Reserve System

Federal Deposit Insurance Corporation

---

12 CFR Part 30, et al.

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

Soundness; Final Rule

[[Page 8616]]

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 30

[Docket No. 00-35]
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. 2000-112]
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 (OCC), Treasury; Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); and Office of Thrift Supervision (OTS), Treasury.

ACTION: Joint final rule.

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 publishing final Guidelines establishing standards for safeguarding customer information that 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. As described in the Act, these safeguards are 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). These final Guidelines implement the requirements described above.

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 are rescinding these guidelines.

Effective Date: The joint final rule is effective July 1, 2001.

Applicability date: The Year 2000 Standards for Safety and Soundness are no longer applicable as of March 5, 2001.

FOR FURTHER INFORMATION CONTACT:

OCC

John Carlson, Deputy Director for Bank Technology, (202) 874-5013; or Deborah Katz, Senior Attorney, Legislative and Regulatory Activities Division, (202) 874-5090.

Board

Heidi Richards, Assistant Director, Division of Banking Supervision and Regulation, (202) 452-2598; Stephanie Martin, Managing Senior Counsel, Legal Division, (202) 452-3198; or Thomas E. Scanlon, Senior Attorney, Legal Division, (202) 452-3594. 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

Jennifer Dickerson, Manager, Information Technology, Examination Policy, (202) 906-5631; 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:

IV. Regulatory Analysis
A. Paperwork Reduction Act
B. Regulatory Flexibility Act
C. Executive Order 12866
D. Unfunded Mandates Act of 1995

I. Background

On November 12, 1999, President Clinton signed the G-L-B Act (Pub. L. 106-102) into law. Section 501, titled ``Protection of Nonpublic Personal Information'', requires the Agencies, the National Credit Union Administration, the Securities and Exchange Commission, 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. As stated in section 501, these safeguards are 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.\2\

\1\ Section 39 applies only to insure 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 sections 501 and 505(b) of the G-L-B Act.

\2\ OTS has placed 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, OTS has adopted a regulatory requirement that the institutions OTS regulates comply with the proposed Guidelines. Because information security guidelines are similar to physical security procedures, OTS has included a provision in 12 CFR part 568, which covers primarily physical security procedures, requiring compliance with the Guidelines in appendix B to part 570.

[[Page 8617]]

II. Overview of Comments Received

On June 26, 2000, the Agencies published for comment the proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness in the Federal Register (65 FR 39472). The public comment

period closed August 25, 2000. The Agencies collectively received a total of 206 comments in response to the proposal, although many commenters sent copies of the same letter to each of the Agencies. Those combined comments included 49 from banks, 7 from savings associations, 60 from financial institution holding companies; 50 from financial institution trade associations; 33 from other business entities; and four from state regulators. The Federal Reserve also received comments from three Federal Reserve Banks.

The Agencies invited comment on all aspects of the proposed Guidelines, including whether the rules should be issued as guidelines or as regulations. Commenters overwhelmingly supported the adoption of guidelines, with many commenters offering suggestions for ways to improve the proposed Guidelines as discussed below. Many commenters cited the benefits of flexibility and the drawbacks of prescriptive requirements that could become rapidly outdated as a result of changes in technology.

The Agencies also requested comments on the impact of the proposal on community banks, recognizing that community banks operate with more limited resources than larger institutions and may present a different risk profile. In general, community banks urged the Agencies to issue guidelines that are not prescriptive, that do not require detailed policies or reporting by banks that share little or no information outside the bank, and that provide flexibility in the design of an information security program. Some community banks indicated that the Guidelines are unnecessary because they already have information security programs in place. Others requested clarification of the impact of the Guidelines on banks that do not share any information in the absence of a customer's consent.

In light of the comments received, the Agencies have decided to adopt the Guidelines, with several changes as discussed below to respond to the commenters' suggestions. The respective texts of the Agencies' Guidelines are substantively identical. In directing the Agencies to issue standards for the protection of customer records and information, Congress provided that the standards apply to all financial institutions, regardless of the extent to which they may disclose information to affiliated or nonaffiliated third parties, electronically transfer data with customers or third parties, or record data electronically. Because the requirements of the Act apply to a broad range of financial institutions, the Agencies believe that the Guidelines must establish appropriate standards that allow each institution the discretion to design an information security program that suits its particular size and complexity and the nature and scope of its activities. In many instances, financial institutions already will have information security programs that are consistent with these Guidelines, because key components of the Guidelines were derived from security-related supervisory guidance previously issued by the Agencies and the Federal Financial Institutions Examination Council (FFIEC). In such situations, little or no modification to an institution's program will be required.

Below is a section-by-section analysis of the final Guidelines.

III. Section-by-Section Analysis

The discussion that follows applies to each Agency's Guidelines.

I. Introduction

Paragraph I. of the proposal set forth the general purpose of the 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 set forth the statutory authority for the 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)). The Agencies received no comments on this paragraph, and have adopted it as proposed.

I.A. Scope

Paragraph I.A. of the proposal described the scope of the Guidelines. Each Agency defined specifically those entities within its particular scope of coverage in this paragraph of the Guidelines.

The Agencies received no comments on the issue of which entities are covered by the Guidelines, and have adopted paragraph I.A. as proposed.

I.B. Preservation of Existing Authority

Paragraph I.B. of the proposal made clear that in issuing these 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. As noted in the preamble to the proposal, 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. The Agencies received no comments on this paragraph, and have adopted paragraph I.B. as proposed.

I.C.1. Definitions

Paragraph I.C. set forth the definitions of various terms for purposes of the Guidelines.\3\ It also stated that terms used in the Guidelines have the same meanings as set forth in sections 3 and 39 of the FDI Act (12 U.S.C. 1813 and 1831p-1).

\3\ In addition to the definitions discussed below, the Board's Guidelines in 12 CFR parts 208 and 225 contain a definition of ``subsidiary'', which described the state member bank and bank holding company subsidiaries that are subject to the Guidelines.

The Agencies received several comments on the proposed definitions, and have made certain changes as discussed below. The Agencies also have reordered proposed paragraph I.C. so that the statement concerning the reliance on sections 3 and 39(a) of the FDI Act is now in paragraph I.C.1., with the definitions appearing in paragraphs I.C.2.a.-e. The defined terms have been placed in alphabetical order in the final Guidelines.

I.C.2.a. Board of Directors

The proposal defined ``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.\4\ The Agencies received no comments on this proposed definition, and have adopted it without change.

\4\ The OTS version of the Guidelines does not include this

definition because OTS does not regulate foreign institutions. Paragraph I of the OTS Guidelines has been renumbered accordingly.

I.C.2.b. Customer

The proposal defined ``customer'' in the same way as that term is defined in section __.3(h) of the Agencies' rule captioned ``Privacy of Consumer Financial Information'' (Privacy Rule).\5\

[[Page 8618]]

The Agencies proposed to use this definition in the Guidelines because section 501(b) refers to safeguarding the security and confidentiality of ``customer'' information. Given that Congress used the same term for both the 501(b) standards and for the sections concerning financial privacy, the Agencies have concluded that it is appropriate to use the same definition in the Guidelines that was adopted in the Privacy Rule.

\6\ See 65 FR 35162 (June 1, 2000). Citations to the interagency Privacy Rule in this preamble are to sections only, leaving blank the citations to the part numbers used by each agency.

Under 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. ``Customer'' does not include a business, nor does it include a consumer who has not established an ongoing relationship with a financial institution (e.g., an individual who merely uses an institution's ATM or applies for a loan). See sections__.3(h) and (i) of the Privacy Rule. The Agencies solicited comment on whether the definition of ``customer'' should be broadened to provide a common information security program for all types of records under the control of a financial institution.

The Agencies received many comments on this definition, almost all of which agreed with the proposed definition. Although a few commenters indicated they would apply the same security program to both business and consumer records, the vast majority of commenters supported the use of the same definition of ``customer'' in the Guidelines as is used in the Privacy Rule. They observed that the use of the term ``customer'' in section 501 of the G-L-B Act, when read in the context of the definitions of ``consumer'' and ``customer relationship'' in section 509, reflects the Congressional intent to distinguish between certain kinds of consumers for the information security standards and the other privacy provisions established under subtitle A of Title V.

The Agencies have concluded that the definition of ``customer'' used in the Guidelines should be consistent with the definition established in section__.3(h) of the Privacy Rule. The Agencies believe, therefore, that the most reasonable interpretation of the applicable provisions of subtitle A of Title V of the Act is that a financial institution is obligated to protect the security and confidentiality of the nonpublic personal information of its consumers with whom it has a customer relationship. As a practical manner, a financial institution may also design or implement its information security program in a manner that encompasses the records and information of its other consumers and its business clients.\6\

\6\ The Agencies recognize that ``customer'' is defined more broadly under Subtitle B of Title V of the Act, which, in general, makes it unlawful for any person to obtain or attempt to obtain customer information of a financial institution by making false, fictitious, or fraudulent statements. For the purpose of that subtitle, the term ``customer'' means ``any person (or authorized representative of a person) to whom the financial institution provides a product or service, including that of acting as a fiduciary.'' (See section 527(1) of the Act.) In light of the statutory mandate to ``prescribe such revisions to such regulations and guidelines as may be necessary to ensure that such financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information'' (section 525), the Agencies considered modifying these Guidelines to cover other customers, namely, business entities and individuals who obtain financial products and services for purposes other than personal, family, or household purposes. The Agencies have concluded, however, that defining ``customer'' to accommodate the range of objectives set forth in Title V of the Act is unnecessary. Instead, the Agencies have included a new paragraph III.C.1.a, described below, and plan to issue guidance and other revisions to the applicable regulations, as may be necessary, to satisfy the requirements of section 525 of the Act.

I.C.2.c. Customer Information

The proposal defined ``customer information'' as any records containing nonpublic personal information, as defined in section__.3(n) of the Privacy Rule, about a customer. This included records, data, files, or other information in paper, electronic, or other form that are maintained by any service provider on behalf of an institution. Although section 501(b) of the G-L-B Act refers to the protection of both customer ``records'' and ``information'', for the sake of simplicity, the proposed Guidelines used the term ``customer information'' to encompass both information and records.

The Agencies received several comments on this definition. The commenters suggested that the proposed definition was too broad because it included files ``containing'' nonpublic personal information. The Agencies believe, however, that a financial institution's security program must apply to files that contain nonpublic personal information in order to adequately protect the customer's information. In deciding what level of protection is appropriate, a financial institution may consider the fact that a given file contains very little nonpublic personal information, but that fact would not render the file entirely beyond the scope of the Guidelines. Accordingly, the Agencies have adopted a definition of ``customer record'' that is substantively the same as the proposed definition. The Agencies have, however, deleted the reference to ``data, files, or other information'' from the final Guidelines, since each is included in the term ``records'' and also is covered by the reference to ``paper, electronic, or other form''.

I.C.2.d. Customer Information System

The proposal defined ``customer information system'' to be electronic or physical methods used to access, collect, store, use, transmit, or protect customer information. The Agencies received a few comments on this definition, mostly from commenters who stated that it is too broad. The Agencies believe that the definition needs to be

sufficiently broad to protect all customer information, wherever the information is located within a financial institution and however it is used. Nevertheless, the broad scope of the definition of ``customer information system'' should not result in an undue burden because, in other important respects, the Guidelines allow a high degree of flexibility for each institution to design a security program that suits its circumstances.

For these reasons, the Agencies have adopted the definition of ``customer information system'' largely as proposed. However, the phrase ``electronic or physical'' in the proposal has been deleted because each is included in the term ``any methods''. The Agencies also have added a specific reference to records disposal in the definition of ``customer information system.'' This is consistent with the proposal's inclusion of access controls in the list of items a financial institution is to consider when establishing security policies and procedures (see discussion of paragraph III.C.1.a., below), given that inadequate disposal of records may result in identity theft or other misuse of customer information. Under the final Guidelines, a financial institution's responsibility to safeguard customer information continues through the disposal process.

I.C.2.e. Service Provider

The proposal defined a ``service provider'' as any person or entity that maintains or processes customer information for a financial institution, or is otherwise granted access to customer information through its provision of services to an institution. One commenter urged the Agencies to modify this definition so that it would not include a financial institution's attorneys, accountants, and appraisers. Others suggested deleting the phrase ``or

[[Page 8619]]

is otherwise granted access to customer information through its provision of services to an institution''.

The Agencies believe that the Act requires each financial institution to adopt a comprehensive information security program that is designed to protect against unauthorized access to or use of customers' nonpublic personal information. Disclosing information to a person or entity that provides services to a financial institution creates additional risks to the security and confidentiality of the information disclosed. In order to protect against these risks, a financial institution must take appropriate steps to protect information that it provides to a service provider, regardless of who the service provider is or how the service provider obtains access. The fact that an entity obtains access to customer information through, for instance, providing professional services does not obviate the need for the financial institution to take appropriate steps to protect the information. Accordingly, the Agencies have determined that, in general, the term ``service provider'' should be broadly defined to encompass a variety of individuals or companies that provide services to the institution.

This does not mean, however, that a financial institution's methods for overseeing its service provider arrangements will be the same for every provider. As explained in the discussion of paragraph III.D., a financial institution's oversight responsibilities will be shaped by the institution's analysis of the risks posed by a given service provider. If a service provider is subject to a code of conduct that imposes a duty to protect customer information consistent with the objectives of these Guidelines, a financial institution may take that

duty into account when deciding what level of oversight it should provide.

Moreover, a financial institution will be responsible under the final Guidelines for overseeing its service provider arrangements only when the service is provided directly to the financial institution. The Agencies clarified this point by amending the definition of ``service provider'' in the final Guidelines to state that it applies only to a person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the financial institution. Thus, for instance, a payment intermediary involved in the collection of a check but that has no correspondent relationship with a financial institution would not be considered a service provider of that financial institution under this rule. By contrast, a financial institution's correspondent bank would be considered its service provider. Nevertheless, the financial institution may take into account the fact that the correspondent bank is itself a financial institution that is subject to security standards under section 501(b) when it determines the appropriate level of oversight for that service provider.\7\

\7\ Similarly, in the case of a service provider that is not subject to these Guidelines but is subject to standards adopted by its primary regulator under section 501(b) of the G-L-B Act, a financial institution may take that fact into consideration when deciding what level of oversight is appropriate for that service provider.

In situations where a service provider hires a subservicer,\8\ the subservicer would not be a ``service provider'' under the final Guidelines. The Agencies recognize that it would be inappropriate to impose obligations on a financial institution to select and monitor subservicers in situations where the financial institution has no contractual relationship with that person or entity. When conducting due diligence in selecting its service providers (see discussion of paragraph III.D., below), however, a financial institution must determine that the service provider has adequate controls to ensure that the subservicer will protect the customer information in a way that meets the objectives of these Guidelines.

\8\ The term ``subservicer'' means any person who has access to an institution's customer information through its provision of services to the service provider and is not limited to mortgage subservicers.

II. Standards for Safeguarding Customer Information

II.A. Information Security Program

The proposed Guidelines described the Agencies' expectations for the creation, implementation, and maintenance of a comprehensive information security program. As noted in the proposal, 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.

Several commenters representing large and complex organizations were concerned that the term ``comprehensive information security

program'' required a single and uniform document that must apply to all component parts of the organization. In response, the Agencies note that a program that includes administrative, technical, and physical safeguards will, in many instances, be composed of more than one document. Moreover, use of this term does not require that all parts of an organization implement a uniform program. However, the Agencies will expect an institution to coordinate all the elements of its information security program. Where the elements of the program are dispersed throughout the institution, management should be aware of these elements and their locations. If they are not maintained on a consolidated basis, management should have an ability to retrieve the current documents from those responsible for the overall coordination and ongoing evaluation of the program.

The Board received comment on its proposal to revise the appendix to Regulation Y regarding the provision that would require a bank holding company to ensure that each of its subsidiaries is subject to a comprehensive information security program.\9\ This comment urged the Board to eliminate that provision and argued, in part, that the requirement assumes that a bank holding company has the power to impose such controls upon its subsidiary companies. These commenters recommended, instead, that the standards should be limited to customer information in the possession or control of the bank holding company.

\9\ The appendix provided that the proposed Guidelines would be applicable 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. See 65 FR 39484 (June 26, 2000).

Under the Bank Holding Company Act of 1956 and the Board's Regulation Y, a subsidiary is presumed to be controlled directly or indirectly by the holding company. 12 U.S.C. 1841(d); 12 CFR 225.2(o). Moreover, the Board believes that a bank holding company is ultimately responsible for ensuring that its subsidiaries comply with the standards set forth under these Guidelines. The Board recognizes, however, that a bank holding company may satisfy its obligations under section 501 of the GLB Act through a variety of measures, such as by including a subsidiary within the scope of its information security program or by causing the subsidiary to implement a separate information security program in accordance with these Guidelines.

II.B. Objectives

Paragraph II.B. of the proposed Guidelines described the objectives that each financial institution's information security program should be designed to achieve. These objectives tracked the objectives as stated in section 501(b)(1)-(3), adding only that the security

[[Page 8620]]

program is to protect against unauthorized access that could risk the safety and soundness of the institution. The Agencies requested comment on whether there are additional or alternative objectives that should be included in the Guidelines.

The Agencies received several comments on this proposed paragraph, most of which objected to language that, in the commenters' view, required compliance with objectives that were impossible to meet. Many

commenters stated, for instance, that no information security program can ensure that there will be no problems with the security or confidentiality of customer information. Others criticized the objective that required protection against any anticipated threat or hazard. A few commenters questioned the objective of protecting against unauthorized access that could result in inconvenience to a customer, while others objected to the addition of the safety and soundness standard noted above.

The Agencies do not believe the statute mandates a standard of absolute liability for a financial institution that experiences a security breach. Thus, the Agencies have clarified these objectives by stating that each security program is to be designed to accomplish the objectives stated. With the one exception discussed below, the Agencies have otherwise left unchanged the statement of the objectives, given that these objectives are identical to those set out in the statute.

In response to comments that objected to the addition of the safety and soundness standard, the Agencies have deleted that reference in order to make the statement of objectives identical to the objectives identified in the statute. The Agencies believe that risks to the safety and soundness of a financial institution may be addressed through other supervisory or regulatory means, making it unnecessary to expand the statement of objectives in this rulemaking.

Some commenters asked for clarification of a financial institution's responsibilities when a customer authorizes a third party to access that customer's information. For purposes of the Guidelines, access to or use of customer information is not ``unauthorized'' access if it is done with the customer's consent. When a customer gives consent to a third party to access or use that customer's information, such as by providing the third party with an account number, PIN, or password, the Guidelines do not require the financial institution to prevent such access or monitor the use or redisclosure of the customer's information by the third party. Finally, unauthorized access does not mean disclosure pursuant to one of the exceptions in the Privacy Rule.

III. Develop and Implement Information Security Program

III.A. Involve the Board of Directors

Paragraph III.A. of the proposal described the involvement of the board and management in the development and implementation of an information security program. As explained in the proposal, the board's responsibilities are to: (1) Approve the institution's written information security policy and program; and (2) oversee efforts to develop, implement, and maintain an effective information security program, including reviewing reports from management. The proposal also laid out management's responsibilities for developing, implementing, and maintaining the security program.

The Agencies received a number of comments regarding the requirement of board approval of the information security program. Some commenters stated that each financial institution should be allowed to decide for itself whether to obtain board approval of its program. Others suggested that approval by either a board committee or at the holding company level might be appropriate. Still others suggested modifying the Guidelines to require only that the board approve the initial information security program and delegate subsequent review and approval of the program to either a committee or an individual.

The Agencies believe that a financial institution's overall information security program is critical to the safety and soundness of the institution. Therefore, the final Guidelines continue to place

responsibility on an institution's board to approve and exercise general oversight over the program. However, the Guidelines allow the entire board of a financial institution, or an appropriate committee of the board to approve the institution's written security program. In addition, the Guidelines permit the board to assign specific implementation responsibilities to a committee or an individual.

One commenter suggested that the Guidelines be revised to provide that if a holding company develops, approves, and oversees the information security program that applies to its bank and nonbank subsidiaries, there should be no separate requirement for each subsidiary to do the same thing, as long as those subsidiaries agree to abide by the holding company's security program. The Agencies agree that subsidiaries within a holding company can use the security program developed at the holding company level. However, if subsidiary institutions choose to use a security program developed at the holding company level, the board of directors or an appropriate committee at each subsidiary institution must conduct an independent review to ensure that the program is suitable and complies with the requirements prescribed by the subsidiary's primary regulator. See 12 U.S.C. 505. Once the subsidiary institution's board, or a committee thereof, has approved the security program, it must oversee the institution's efforts to implement and maintain an effective program.

The Agencies also received comments suggesting that use of the term ``oversee'' conveyed the notion that a board is expected to be involved in day-to-day monitoring of the development, implementation, and maintenance of an information security program. The Agencies' use of the term ``oversee'' is meant to convey a board's conventional supervisory responsibilities. Day-to-day monitoring of any aspect of an information security program is a management responsibility. The final Guidelines reflect this by providing that the board must oversee the institution's information security program but may assign specific responsibility for its implementation.

The Agencies invited comment on whether the Guidelines should 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. The Agencies received a number of comments suggesting that the Agencies should not require the creation of a new position for this purpose. Some financial institutions also stated that hiring one or more additional staff for this purpose would impose a significant burden. The Agencies believe that a financial institution will not need to create a new position with a specific title for this purpose, as long as the institution has adequate staff in light of the risks to its customer information. Regardless of whether new staff are added, the lines of authority and responsibility for development, implementation, and administration of a financial institution's information security program need to be well defined and clearly articulated.\10\

\10\ The Agencies note that other regulations already require a financial institution to designate a security officer for different purposes. See 12 CFR 21.2; 12 CFR 208.61(b).

[[Page 8621]]

The proposal identified three responsibilities of management in the development of an information security program. They were to: (1)

Evaluate the impact on a financial institution's security program of changing business arrangements and changes to customer information systems; (2) document compliance with these Guidelines; and (3) keep the board informed of the overall status of the institution's information security program. A few commenters objected to the Agencies assigning specific tasks to management. These commenters did not object to the tasks per se, but suggested that the Agencies allow an institution's board and management to decide who within the institution is to carry out the tasks.

The Agencies agree that a financial institution is in the best position to determine who should be assigned specific roles in implementing the institution's security program. Accordingly, the Agencies have deleted the separate provision assigning specific roles to management. The responsibilities that were contained in this provision are now included in other paragraphs of the Guidelines.

III.B. Assess Risk

Paragraph III.B. of the proposal described the risk assessment process to be used in the development of the information security program. Under the proposal, a financial institution was to identify and assess the risks to customer information. As part of that assessment, the institution was to determine the sensitivity of the information and the threats to the institution's systems. The institution also was to assess the sufficiency of its policies, procedures, systems, and other arrangements in place to control risk. Finally, the institution was to monitor, evaluate, and adjust its risk assessment in light of changes in areas identified in the proposal.

The Agencies received several comments on these provisions, most of which focused on the requirement that financial institutions do a sensitivity analysis. One commenter noted that ``customer information'' is defined to mean ``nonpublic personal information'' as defined in the G-L-B Act, and that the G-L-B Act provides the same level of coverage for all nonpublic personal information. The commenter stated that it is therefore unclear how the level of sensitivity would affect an institution's obligations with respect to the security of this information.

While the Agencies agree that all customer information requires protection, the Agencies believe that requiring all institutions to afford the same degree of protection to all customer information may be unnecessarily burdensome in many cases. Accordingly, the final Guidelines continue to state that institutions should take into consideration the sensitivity of customer information. Disclosure of certain information (such as account numbers or access codes) might be particularly harmful to customers if the disclosure is not authorized. Individuals who try to breach the institution's security systems may be likely to target this type of information. When such information is housed on systems that are accessible through public telecommunications networks, it may require more and different protections, such as encryption, than if it were located in a locked file drawer. To provide flexibility to respond to these different security needs in the way most appropriate, the Guidelines confer upon institutions the discretion to determine the levels of protection necessary for different categories of information. Institutions may treat all customer information the same, provided that the level of protection is adequate for all the information.

Other commenters suggested that the risk assessment requirement be tied to reasonably foreseeable risks. The Agencies agree that the security program should be focused on reasonably foreseeable risks and have amended the final Guidelines accordingly.

The final Guidelines make several other changes to this paragraph to improve the order of the Guidelines and to eliminate provisions that were redundant in light of responsibilities outlined elsewhere. For instance, while the proposal stated that the risk assessment function included the need to monitor for relevant changes to technology, sensitivity of customer information, and threats to information security and make adjustments as needed, that function has been incorporated into the discussion of managing and controlling risk in paragraphs III.C.3. and III.E.

Thus, under the Guidelines as adopted, a financial institution should identify the reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. Next, the risk assessment should consider the potential damage that a compromise of customer information from an identified threat would have on the customer information, taking into consideration the sensitivity of the information to be protected in assessing the potential damage. Finally, 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.

III.C. Manage and Control Risk

Paragraph III.C. describes the steps an institution should take to manage and the control risks identified in paragraph III.B.

Establish policies and procedures (III.C.1.). Paragraph III.C.1 of the proposal described 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 identified eleven factors an institution should consider in evaluating the adequacy of its policies and procedures to effectively manage these risks.

The Agencies received a large number of comments on this paragraph. Most of the comments were based on a perception that every institution would have to adopt every security measure listed in proposed III.C.1.a.-k. as part of the institution's policies and procedures. In particular, a number of commenters were concerned that the proposed Guidelines would require the encryption of all customer data.

The Agencies did not intend for the security measures listed in paragraph III.C.1. to be seen as mandatory for all financial institutions and for all data. Rather, the Agencies intended only that an institution would consider whether the protections listed were appropriate for the institution's particular circumstances, and, if so, adopt those identified as appropriate. The Agencies continue to believe that these elements may be adapted by institutions of varying sizes, scope of operations, and risk management structures. Consistent with that approach, the manner of implementing a particular element may vary from institution to institution. For example, while a financial institution that offers Internet-based transaction accounts may conclude that encryption is appropriate, a different institution that processes all data internally and does not have a transactional web site may consider other kinds of access restrictions that are adequate to maintain the confidentiality of customer information. To underscore this point, the final Guidelines have been amended to state that each financial institution must consider whether the security elements discussed in paragraphs III.C.1.a.-h. are appropriate for the institution and, if so, adopt those

elements an institution concludes are appropriate.

The Agencies invited comment on the degree of detail that should be included in the Guidelines regarding the risk management program, including which elements should be specified in the Guidelines, and any other components of a risk management program that should be listed. With the exception of those commenters who thought some or all of the elements of the risk management program were intended to be mandatory for all financial institutions, the comments supported the level of detail conveyed in the proposed Guidelines. The Agencies have adopted the provision regarding management and control of risks with the changes discussed below. Comments addressing proposed security measures that have been adopted without change also are discussed below.

Access rights. The Agencies received a number of comments suggesting that the reference to ``access rights to customer information'' in paragraph III.C.1.a. of the proposal could be interpreted to mean providing customers with a right of access to financial information. The reference was intended to refer to limitations on employee access to customer financial information, not to customer access to financial information. However, this element has been deleted since limitations on employee access are covered adequately in other parts of paragraph III.C.1. (See discussion of ``access controls'' in paragraph III.C.1.a. of the final Guidelines, below.)

Access controls. Paragraph III.C.1.b. of the proposed Guidelines required a financial institution to consider appropriate access controls when establishing its information security policies and procedures. These controls were intended to address unauthorized access to an institution's customer information by anyone, whether or not employed by the institution.

The Agencies believe that this element sufficiently addresses the concept of unauthorized access, regardless of who is attempting to obtain access. This would cover, for instance, attempts through pretext calling to gather information about a financial institution's customers.\11\ The Agencies have amended the final Guidelines to refer specifically to pretext calling in new III.C.1.a. The Agencies do not intend for the final Guidelines to require a financial institution to provide its customers with access to information the institution has gathered. Instead, the provision in the final Guidelines addressing access is limited solely to the issue of preventing unauthorized access to customer information.

\11\ Pretext calling is a fraudulent means of obtaining an individual's personal information by persons posing as bank customers.

The Agencies have deleted the reference in the proposed paragraph III.C.1.b. to providing access to authorized companies. This change was made partly in response to commenters who objected to what they perceived to be an inappropriate expansion of the scope of the Guidelines to include company records and partly in recognition of the fact that access to records would be obtained, in any case, only through requests by individuals. The final Guidelines require an institution to consider the need for access controls in light of the institution's various customer information systems and adopt such controls as appropriate.

Dual control procedures. Paragraph III.C.1.f. of the proposed Guidelines stated that financial institutions should consider dual

control procedures, segregation of duties, and employee background checks for employees with responsibility for, or access to, customer information. Most of the comments on this paragraph focused on dual control procedures, which refers to a security technique that uses two or more separate persons, operating together to protect sensitive information. Both persons are equally responsible for protecting the information and neither can access the information alone.

According to one commenter, dual controls are part of normal audit procedures and did not need to be restated. Other commenters suggested that dual control procedures are not always necessary, implying that these procedures are not the norm. The Agencies recognize that dual-control procedures are not necessary for all activities, but might be appropriate for higher-risk activities. Given that the Guidelines state only that dual control procedures should be considered by a financial institution and adopted only if appropriate for the institution, the Agencies have retained a reference to dual control procedures in the items to be considered (paragraph III.C.1.e).

Oversight of servicers. Paragraph III.C.1.g. of the proposal was deleted. Instead, the final Guidelines consolidate the provisions related to service providers in paragraph III.D.

Physical hazards and technical failures. The paragraphs of the proposed Guidelines addressing protection against destruction due to physical hazards and technological failures (paragraphs III.C.1.j. and k., respectively, of the proposal) have been consolidated in paragraph III.C.1.h. of the final Guidelines. The Agencies believe that this change improves clarity and recognizes that disaster recovery from environmental and technological failures often involve the same considerations.

Training (III.C.2.). Paragraph III.C.2. of the proposed Guidelines provided that an institution's information security program should include a training component designed to train employees to recognize, respond to, and report unauthorized attempts to obtain customer information. The Agencies received several comments suggesting that this provision directed staff of financial institutions to report suspected attempts to obtain customer information to law enforcement agencies rather than to the management of the financial institution. The Agencies did not intend that result, and note that nothing in the Guidelines alters other applicable requirements and procedures for reporting suspicious activities. For purposes of these Guidelines, the Agencies believe that, as part of a training program, staff should be made aware both of federal reporting requirements and an institution's procedures for reporting suspicious activities, including attempts to obtain access to customer information without proper authority.

The final Guidelines amend the provision governing training to state that a financial institution's information security program should include a training component designed to implement the institution's information security policies and procedures. The Agencies believe that the appropriate focus for the training should be on compliance with the institution's security program generally and not just on the limited aspects identified in proposed III.C.2. The provisions governing reporting have been moved to paragraph III.C.1.g., which addresses response programs in general.

Testing (III.C.3.). Paragraph III.C.3. of the proposed Guidelines provided that an information security program should include regular testing of key controls, systems, and procedures. The proposal provided that the frequency and nature of the testing should be determined by the risk assessment and adjusted as necessary to reflect changes in both internal and external conditions. The proposal also provided that the tests are to be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the

security program. Finally, the proposal stated that test results are to be reviewed by independent third parties or staff independent of those that

[[Page 8623]]

conducted the test. The Agencies requested comment on whether specific types of security tests, such as penetration tests or intrusion detection tests, should be required.

The most frequent comment regarding testing of key controls was that the Agencies should not require specific tests. Commenters noted that because technology changes rapidly, the tests specified in the Guidelines will become obsolete and other tests will become the standard. Consequently, according to these commenters, the Guidelines should identify areas where testing may be appropriate without requiring a financial institution to implement a specific test or testing procedure. Several commenters noted that periodic testing of information security controls is a sound idea and is an appropriate standard for inclusion in these Guidelines.

The Agencies believe that a variety of tests may be used to ensure the controls, systems, and procedures of the information security program work properly and also recognize that such tests will progressively change over time. The Agencies believe that the particular tests that may be applied should be left to the discretion of management rather than specified in advance in these Guidelines. Accordingly, the final Guidelines do not require a financial institution to apply specific tests to evaluate the key control systems of its information security program.

The Agencies also invited 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. The proposal asked whether the tests or reviews of tests be conducted by persons who are not employees of the financial institution. The proposal also asked whether employees may conduct the testing or may review test results, and what measures, if any, are appropriate to assure their independence.

Some commenters interpreted the proposal as requiring three separate teams of people to provide sufficient independence to control testing: one team to operate the system; a second team to test the system; and a third team to review test results. This approach, they argued, would be too burdensome and expensive to implement. The Agencies believe that the critical need for independence is between those who operate the systems and those who either test them or review the test results. Therefore, the final Guidelines now require that tests should be conducted or reviewed by persons who are independent of those who operate the systems, including the management of those systems.

Whether a financial institution should use third parties to either conduct tests or review their results depends upon a number of factors. Some financial institutions may have the capability to thoroughly test certain systems in-house and review the test results but will need the assistance of third party testers to assess other systems. For example, an institution's internal audit department may be sufficiently trained and independent for the purposes of testing certain key controls and providing test results to decision makers independent of system managers. Some testing may be conducted by third parties in connection with the actual installation or modification of a particular program. In each instance, management needs to weigh the benefits of testing and test review by third parties against its own resources in this area, both in terms of expense and reliability.

Ongoing adjustment of program. Paragraph III.C.4. of the proposal required an institution to 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. This provision was previously located in the paragraph titled ``Manage and Control Risk''. While there were no comments on this provision, the Agencies wanted to highlight this concept and clarify that this provision is applicable to an institutions' entire information security program. Therefore, this provision is now separately identified as new paragraph III.E. of the final Guidelines, discussed below.

III.D. Oversee Service Provider Arrangements

The Agencies' proposal addressed service providers in two provisions. The Agencies provided that an institution should consider contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by service providers as one of the proposed elements to be considered in establishing risk management policies and procedures (proposed paragraph III.C.1.g.). Additionally, proposed paragraph III.D. provided that, when an institution uses an outsourcing arrangement, the institution would continue to be responsible for safeguarding customer information that it gives to the service provider. That proposed paragraph also provided that the institution must use due diligence in managing and monitoring the outsourcing arrangement to confirm that its service providers would protect customer information consistent with the Guidelines.

The Agencies requested comment on the appropriate treatment of outsourcing arrangements, such as whether industry best practices are available regarding effective monitoring of service provider security precautions, whether service providers accommodate requests for specific contract provisions regarding information security, and, to the extent that service providers do not accommodate these requests, whether financial institutions implement effective information security programs. The Agencies also requested comment on whether institutions would find it helpful if the Guidelines contained specific contract provisions requiring service provider performance standards in connection with the security of customer information.

The Agencies received one example of best practices, but the commenter did not recommend that they be included in the Guidelines. While some commenters suggested that the Guidelines include best practices, other commenters stated that, given the various types of financial institutions, there could be a variety of best industry practices. Another commenter stated that best practices could become minimum requirements that result in inappropriate burdens. The Agencies recognize that information security practices are likely to evolve rapidly, and thus believe that it is inappropriate to include best practices in the final Guidelines.

Commenters were mixed as to whether service providers are receptive to contract modifications to protect customer information. Commenters were uniform, however, in stating that an institution's obligation to monitor service providers should not include on-site audits by the institution or its agent. The commenters stated that, in addition to the expense for financial institutions, the procedure would place an inordinate burden on many service providers that process customer information for multiple institutions. Several commenters noted that the service providers often contract for audits of their systems and that institutions should be able to rely upon those testing procedures. Some commenters recommended that an institution's responsibility for information given to service providers require only that the

institution enter into appropriate contractual arrangements. However, commenters also indicated that requiring specific

[[Page 8624]]

contract provisions would not be consistent with the development of flexible Guidelines and recommended against the inclusion of specific provisions.

The Agencies believe that financial institutions should enter into appropriate contracts, but also believe that these contracts, alone, are not sufficient. Therefore, the final Guidelines, in paragraph III.D., include provisions relating to selecting, contracting with, and monitoring service providers.

The final Guidelines require that an institution exercise appropriate due diligence in the selection of service providers. Due diligence should include a review of the measures taken by a service provider to protect customer information. As previously noted in the discussion of ``service provider'', it also should include a review of the controls the service provider has in place to ensure that any subservicer used by the service provider will be able to meet the objectives of these Guidelines.

The final Guidelines also require that a financial institution have a contract with each of its service providers that requires each provider to implement appropriate measures designed to meet the objectives of these Guidelines (as stated in paragraph II.B.). This provision does not require a service provider to have a security program in place that complies with each paragraph of these Guidelines. Instead, by stating that a service provider's security measures need only achieve the objectives of these Guidelines, the Guidelines provide flexibility for a service provider's information security measures to differ from the program that a financial institution implements. The Agencies have provided a two-year transition period during which institutions may bring their outsourcing contracts into compliance. (See discussion of paragraph III.F.) The Agencies have not included model contract language, given our belief that the precise terms of service contracts are best left to the parties involved.

Each financial institution must also exercise an appropriate level of oversight over each of its service providers to confirm that the service provider is implementing the provider's security measures. The Agencies have amended the Guidelines as proposed to include greater flexibility with regard to the monitoring of service providers. A financial institution need only monitor its outsourcing arrangements if such oversight is indicated by an institution's own risk assessment. The Agencies recognize that not all outsourcing arrangements will need to be monitored or monitored in the same fashion. Some service providers will be financial institutions that are directly subject to these Guidelines or other standards promulgated by their primary regulator under section 501(b). Other service providers may already be subject to legal and professional standards that require them to safeguard the institution's customer information. Therefore, the final Guidelines permit an institution to do a risk assessment taking these factors into account and determine for themselves which service providers will need to be monitored.

Even where monitoring is warranted, the Guidelines do not require on-site inspections. Instead, the Guidelines state that this monitoring can be accomplished, for example, through the periodic review of the service provider's associated audits, summaries of test results, or equivalent measures of the service provider. The Agencies expect that institutions will arrange, when appropriate, through contracts or otherwise, to receive copies of audits and test result information

sufficient to assure the institution that the service provider implements information security measures that are consistent with its contract provisions regarding the security of customer information. The American Institute of Certified Public Accountants Statement of Auditing Standards No. 70, captioned ``Reports on the Processing of Transactions by Service Organizations'' (SAS 70 report), is one commonly used external audit tool for service providers. Information contained in an SAS 70 report may enable an institution to assess whether its service provider has information security measures that are consistent with representations made to the institution during the service provider selection process.

III.E. Adjust the Program

Paragraphs III.B.3 and III.C.4. of the proposed Guidelines both addressed a financial institution's obligations when circumstances change. Both paragraph III.B.3. (which set forth management's responsibilities with respect to its risk assessment) and paragraph III.C.4. (which focused on the adequacy of an institution's information security program) identified the possible need for changes to an institution's program in light of relevant changes to technology, the sensitivity of customer information, and internal or external threats to the information security.

The Agencies received no comments objecting to the statements in these paragraphs of the need to adjust a financial institution's program as circumstances change. While the Agencies have not changed the substance of these provisions in the final Guidelines, we have, however, made a stylistic change to simplify the Guidelines. The final Guidelines combine, in paragraph III.E., the provisions previously stated separately. Consistent with the proposal, this paragraph provides that each financial institution must monitor, evaluate, and adjust its information security program in light of relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the institution's own changing business arrangements. This would include an analysis of risks to customer information posed by new technology (and any needed program adjustments) before a financial institution adopts the technology in order to determine whether a security program remains adequate in light of the new risks presented.\12\

\12\ For additional information concerning how a financial institution should identify, measure, monitor, and control risks associated with the use of technology, see OCC Bulletin 98-3 concerning technology risk management, which may be obtained on the Internet at http://www.occ.treas.gov/ftp/bulletin/98-3.txt.; Federal Reserve SR Letter 98-9 on Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations, April 20, 1998, http://www.federalreserve.gov/boarddocs/SRLETTERS/1998/SR9809.HTM; FDIC FIL 99-68 concerning risk assessment tools and practices for information security systems at http://www.fdic.gov/news/news/financial/1999/fil9968.html.; OTS's CEO Letter 70, Statement on Retail On-Line Personal Computer Banking, (June 23, 1997), available at http://www.ots.treas.gov/docs/25070.pdf.

III.F. Report to the Board

Paragraph III.A.2.c. of the proposal set out management's

responsibilities for reporting to its board of directors. As previously discussed, the final Guidelines have removed specific requirements for management, but instead allow a financial institution to determine who within the organization should carry out a given responsibility. The board reporting requirement thus has been amended to require that a financial institution report to its board, and that this report be at least annual. Paragraph III.F. of the final Guidelines sets out this requirement.

The Agencies invited comment regarding the appropriate frequency of reports to the board, including whether reports should be monthly, quarterly, or annually. The Agencies received a number of comments recommending that no specific frequency be mandated by the Guidelines and that each financial institution be permitted to establish its own reporting period.

[[Page 8625]]

Several commenters stated that if a reporting period is required, then it should be not less than annually unless some material event triggers the need for an interim report.

The Agencies expect that in all cases, management will provide its board (or the appropriate board committee) a written report on the information security program consistent with the Guidelines at least annually. Management of financial institutions with more complex information systems may find it necessary to provide information to the board (or a committee) on a more frequent basis. Similarly, more frequent reporting will be appropriate whenever a material event affecting the system occurs or a material modification is made to the system. The Agencies expect that the content of these reports will vary for each financial institution, depending upon the nature and scope of its activities as well as the different circumstances that it will confront as it implements and maintains its program.

III.G. Implement the Standards

Paragraph III.E. of the proposal described the timing requirements for the implementation of these standards. It provided that each financial institution is to take appropriate steps to fully implement an information security program pursuant to these Guidelines by July 1, 2001.

The Agencies received several comments suggesting that the proposed effective date be extended for a period of 12 to 18 months because financial institutions are currently involved in efforts to meet the requirements of the final Privacy Rule by the compliance deadline, July 1, 2001. The Agencies believe that the dates for full compliance with these Guidelines and the Privacy Rule should coincide. Financial institutions are required, as part of their initial privacy notices, to disclose their policies and practices with respect to protecting the confidentiality and security of nonpublic personal information. See Sec. __.6(a)(8). Each Agency has provided in the appendix to its Privacy Rule that a financial institution may satisfy this disclosure requirement by advising its customers that the institution maintains physical, electronic, and procedural safeguards that comply with federal standards to guard customers' nonpublic personal information. See appendix A-7. The Agencies believe that this disclosure will be meaningful only if the final Guidelines are effective when the disclosure is made. If the effective date of these Guidelines is extended beyond July 1, 2001, then a financial institution may be placed in the position of providing an initial notice regarding confidentiality and security and thereafter amending the privacy policy

to accurately refer to the federal standards once they became effective. For these reasons, the Agencies have retained July 1, 2001, as the effective date for these Guidelines.

However, the Agencies have included a transition rule for contracts with service providers. The transition rule, which parallels a similar provision in the Privacy Rule, provides a two-year period for grandfathering existing contracts. Thus a contract entered into on or before the date that is 30 days after publication of the final Guidelines in the Federal Register satisfies the provisions of this part until July 1, 2003, even if the contract does not include provisions delineating the servicer's duties and responsibilities to protect customer information described in paragraph III.D.

Location of Guidelines: These guidelines have been published 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 also is 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. The final rules make 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 standards were issued have passed, the Agencies have concluded that the guidelines are no longer necessary and proposed to rescind the standards as part of this rulemaking. The Agencies requested comment on whether rescission of these standards is appropriate. Those commenters responding to this request were unanimous in recommending the rescission of the Year 2000 Standards, and the Agencies have rescinded these standards. These standards appeared 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. Accordingly, the Agencies hereby rescind the Year 2000 Standards for Safety and Soundness, effective thirty (30) days after the publication date of this notice of the joint final rule.

IV. Regulatory Analysis

A. Paperwork Reduction Act

The Agencies have determined that this rule does not involve a collection of information pursuant to the provisions of the Paperwork Reduction Act (44 U.S.C. 3501 et seq.).

B. Regulatory Flexibility Act

OCC: Under the Regulatory Flexibility Act (RFA), the OCC must either provide a Final Regulatory Flexibility Analysis (FRFA) with these final Guidelines or certify that the final Guidelines ``will not, if promulgated'', have a significant economic impact on a substantial number of small entities.\13\ The OCC has evaluated the effects of these Guidelines on small entities and is providing the following FRFA.

\13\ The RFA defines the term ``small entity'' in 5 U.S.C. 601

by reference to a definition published by the Small Business Administration (SBA). The SBA has defined a ``small entity'' for banking purposes as a national or commercial bank, or savings institution with less than $100 million in assets. See 13 CFR 121.201.

Although the OCC specifically sought comment on the costs to small entities of establishing and operating information security programs, no commenters provided specific cost information. Instead, commenters confirmed the OCC's conclusion that most if not all institutions already have information security programs in place, because the standards reflect good business practices and existing OCC and FFIEC guidance. Some comments indicated, however, that institutions will have to formalize or enhance their information security programs. Accordingly, the OCC considered certifying, under section 605(b) of the RFA, that these Guidelines will not have a significant economic impact on a substantial number of small entities. However, given that the guidance previously issued by the OCC and the FFIEC is not completely identical to the Guidelines being adopted in this rulemaking, the Guidelines are likely to have some impact on all affected institutions. While the OCC believes that this impact will not be substantial in the case of most small entities, we nevertheless have prepared the following FRFA.

[[Page 8626]]

1. Reasons for Final Action

The OCC is issuing these Guidelines under 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.

2. Objectives of and Legal Basis for Final Action

The objectives of the Guidelines are described in the Supplementary Information section above. The legal bases for the Guidelines are: 12 U.S.C. 93a, 1818, 1831p-1, and 3102(b) and 15 USC 6801 and 6805(b)(1).

3. Small Entities to Which the Rule Will Apply

The OCC's final Guidelines will apply to approximately 2300 institutions, including national banks, federal branches and federal agencies of foreign banks, and certain subsidiaries of such entities. The OCC estimates that approximately 1125 of these institutions are small institutions with assets less than $100 million.

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

The Guidelines do not require any reports to the OCC, however, they require all covered institutions to develop and implement a written information security program comprised of several elements. Institutions must assess the risks to their customer information and adopt appropriate measures to control those risks. Institutions must then test these security measures and adjust their information security programs in light of any relevant changes. In addition, institutions must use appropriate due diligence in selecting service providers, and require service providers, by contract, to implement appropriate security measures. The Guidelines also require institutions to monitor their service providers, where appropriate, to confirm they have met

their contractual obligations. Finally, the Guidelines require the board of directors or an appropriate committee of the board of each institution to approve the institution's information security program and to oversee its implementation. To facilitate board oversight, the institution must provide to the board or to the board committee a report, at least annually, describing the overall status of the institution's information security program and the institution's compliance with the Guidelines.

Because the information security program described above reflects existing supervisory guidance, the OCC believes that most institutions already have the expertise to develop, implement, and maintain the program. However, if they have not already done so, institutions will have to retain the services of someone capable of assessing threats to the institution's customer information. Institutions that lack an adequate information security program also will have to have personnel capable of developing, implementing and testing security measures to address these threats. Institutions that use service providers may require legal skills to draft appropriate language for contracts with service providers.

5. Public Comment and Significant Alternatives

The OCC did not receive any public comment on its initial regulatory flexibility analysis, although it did receive comments on the proposed Guidelines, and on the impact of the Guidelines on small entities in particular. The comments received by the OCC and the other Agencies are discussed at length in the supplementary information above. While some commenters suggested that the OCC exempt small institutions altogether, the OCC has no authority under the statute to do so. The discussion below reviews the changes adopted in the final Guidelines that will minimize the economic impact of the Guidelines on all businesses.

The OCC carefully considered comments from small entities that encouraged the Agencies to issue guidelines that are not overly prescriptive, that provide flexibility in the design of an information security program, but that still provide small entities with some guidance. After considering these comments, the OCC determined that it is appropriate to issue the standards as Guidelines that allow each institution the discretion to design an information security program that suits its particular size and complexity and the nature and scope of its activities. The OCC considered issuing broader Guidelines that would only identify objectives to be achieved while leaving it up to each institution to decide what steps it should take to ensure that it meets these objectives. However, the OCC concluded that such broad guidance ultimately would be less helpful than would be guidelines that combine the flexibility sought by commenters with meaningful guidance on factors that an institution should consider and steps that the institution should take. The OCC also considered the utility of more prescriptive guidelines, but rejected that approach out of concern that it likely would be more burdensome, could interfere with innovation, and could impose requirements that would be inappropriate in a given situation. While the Guidelines are not overly detailed, they provide guidance by establishing the process an institution will need to follow in order to protect its customer information and by identifying security measures that are likely to have the greatest applicability to national banks in general.

Most commenters supported the use of the more narrow definition of ``customer'' in the Guidelines as is used in the Privacy Rule rather than a broad definition that would apply to all records under the control of a financial institution. Commenters maintained that two different definitions would be confusing and also inconsistent with the use of the term ``customer'' in section 501 of the G-L-B Act. The OCC

considered using the broader definition, but determined that information security could be addressed more broadly through other vehicles. For the sake of consistency, the final Guidelines adopt the narrower definition and apply only to records of consumers who have 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, the definition used in the Privacy Rule.

Many commenters criticized the list of proposed objectives for each financial institution's information security program which generally reflected the statutory objectives in section 501(b). According to these comments, the objectives were stated in a manner that made them absolute, unachievable, and therefore burdensome. The final Guidelines have been drafted to clarify these objectives by stating that each security program is to be ``designed'' to accomplish the objectives stated.

Commenters wanted board involvement in the development and implementation of an information security program left to the discretion of the financial institution. Commenters also asked the OCC to clarify that the board may delegate to a committee responsibility for involvement in the

[[Page 8627]]

institution's security program. While the final Guidelines as drafted continue to place responsibility on an institution's board to approve and exercise general oversight over the program, they now clarify that a committee of the board may approve the institution's written security program. In addition, the Guidelines permit the board to assign specific implementation responsibilities to a committee or an individual.

The OCC considered requiring an institution to designate a Corporate Security Officer. However, the agency agreed with commenters that a financial institution is in the best position to determine who should be assigned specific roles in implementing the institution's security program. Therefore, the Guidelines do not include this requirement.

The proposal identifying various security measures that an institution should consider in evaluating the adequacy of its policies and procedures was criticized by many commenters. These commenters misinterpreted the list of measures and believed each measure to be mandatory. Small entities commented that these measures were overly comprehensive and burdensome. As discussed previously in the preamble, the OCC did not intend to suggest that every institution must adopt every one of the measures. To highlight the OCC's intention that an institution must determine for itself which measures will be appropriate for its own risk profile, the final Guidelines now clearly state that each financial institution must consider whether the security elements listed are appropriate for the institution and, if so, adopt those elements an institution concludes are appropriate.

Commenters noted that testing could be burdensome and costly, especially for small entities. The OCC considered mandating specific tests, but determined that with changes in technology, such tests could become obsolete. Therefore, the final Guidelines permit management to exercise its discretion to determine the frequency and types of tests that need to be conducted. The OCC considered required testing or the review of tests to be conducted by outside auditors. The OCC determined that these duties could be performed effectively by an institution's own staff, if staff selected is sufficiently independent. Therefore, the Guidelines permit financial institutions to determine for

themselves whether to use third parties to either conduct tests or review their results or to use staff independent of those that develop or maintain the institution's security program.

Many commenters objected to provisions in the proposal requiring institutions to monitor their service providers. Commenters asserted that it would be burdensome to require them to monitor the activities of their service providers and that information security of service providers should be handled through contractual arrangements. The final Guidelines include greater flexibility with regard to the monitoring of service providers than was provided in the proposal. The final Guidelines recognize that some service providers will be financial institutions that are directly subject to these Guidelines or other standards promulgated under section 501(b) and that other service providers may already be subject to legal and professional standards that require them to safeguard the institution's customer information. Therefore, the final Guidelines permit an institution to do a risk assessment taking these factors into account and to determine for themselves which service providers will need to be monitored. Where monitoring is warranted, the Guidelines now specify that monitoring can be accomplished, for example, through the periodic review of the service provider's associated audits, summaries of test results, or equivalent measures of the service provider.

In addition, after considering the comments about contracts with service providers and the effective date of the Guidelines, the OCC also adopted a transition rule, similar to a provision in the Privacy Rule, that grandfathers existing contracts for a two-year period.

One commenter requested that smaller community banks be given additional time to comply with the Guidelines because having to comply with the new Privacy Rule and these Guidelines will put a strain on the resources of smaller banks. The OCC considered this request but did not change the effective date of the Guidelines given the importance of safeguarding customer information. In addition, most institutions already have information security programs in place, and the OCC has addressed this concern by adding flexibility to the final Guidelines in a variety of other areas as described above.

Board: The Regulatory Flexibility Act (5 U.S.C. 604) requires an agency to publish a final regulatory flexibility analysis when promulgating a final rule that was subject to notice and comment.

Need for and objectives of Guidelines: As discussed above, these Guidelines implement section 501 of the GLB Act. The objective of the Guidelines is to establish standards for financial institutions that are subject to the Board's jurisdiction to protect the security and confidentiality of their customers' information. In particular, the Guidelines require those financial institutions to implement a comprehensive written information security program that includes:

(1) Assessing the reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information;

(2) Adopting security measures that the financial institution concludes are appropriate for it; and

(3) Overseeing its arrangements with its service provider(s).

Comments on the initial regulatory flexibility analysis: Although few commenters addressed the initial regulatory flexibility analysis specifically, many commenters addressed the regulatory burdens that were discussed in that analysis. Several commenters noted that certain aspects of the proposal may tax the comparatively limited resources of small institutions, yet few commenters quantified the potential costs of compliance. The comments received by the Board and the other Agencies were discussed in the supplementary information above. Those comments that are closely related to regulatory burden are highlighted

below:

The Board requested comment on the scope of the term ``customer'' for purposes of the Guidelines. Many commenters opposed expanding the proposed scope of the Guidelines to apply to information about business customers and consumers who have not established continuing relationships with the financial institution. The commenters stated that an expanded scope would impose higher costs of developing an information security program and would be inconsistent with the use of the term ``customer'' in section 501 of the GLB Act and the Agencies' Privacy Rule. As explained in the supplementary information above, the Board has defined ``customer'' in the final Guidelines in the same way as that term is defined in section __.3(h) of the Agencies' Privacy Rule.

Many commenters urged the Board to reduce the level of detail about the kinds of measures that would be required to implement an information security program under the proposed Guidelines. Commenters argued, for instance, that requiring particular testing procedures of security systems would make the standards too onerous for those institutions for which other kinds of tests and audits would be more suitable. In a similar vein, some commenters proposed that the Board

[[Page 8628]]

should issue examples that would illustrate the kinds of security measures that, if adopted, would constitute compliance with the Guidelines.

The Board believes that many commenters may have misinterpreted the intent of the original proposal regarding the particular safeguards that would be expected. The provision that requires each financial institution to consider a variety of security measures has been redrafted in an effort to clarify that the institution must determine for itself which measures will be appropriate to its own risk profile. Although an institution is required to consider each of the security measures listed in paragraph III.C.1., it is not obligated to incorporate any particular security measures or particular testing procedures into its information security program. Rather, the institution may adopt those measures and use those tests that it concludes are appropriate. The Board is mindful that institutions' operations will vary in their complexity and scope of activities and present different risk profiles to their customer information. Accordingly, the Board has not established definitive security measures that, if adopted, would constitute compliance with the Guidelines.

The Board asked for comments on several issues related to the appropriate security standards pertaining to an institution's arrangements with its service providers. As discussed above, many comments addressed these issues and, notably, objected to a provision that would require an institution to monitor its service providers through on-site audits. Several commenters noted that the service providers often contract for audits of their systems and argued that an institution should be able to rely upon those testing procedures. Commenters also recommended that an institution's responsibility for information given to service providers require only that the institution enter into appropriate contractual arrangements. The Board has modified the Guidelines to clarify an institution's responsibilities with respect to service providers. The Board has not designed a standard that would require a financial institution to conduct an on-site audit of its service provider's security program. Instead, the Board adopted a standard that requires an institution to monitor its service provider to confirm that it has satisfied its contractual obligations, depending upon the institution's risk

assessment. In the course of conducting its risk assessment and determining which service providers will need to be monitored, an institution may take into account the fact that some of its service providers may be financial institutions that are directly subject to these Guidelines or other standards promulgated by their primary regulator under section 501(b). Furthermore, after considering the comments about contracts with service providers and the effective date of the Guidelines, the Board also adopted a transition rule, which parallels a similar provision in the Privacy Rule, that provides a two-year period for grandfathering existing contracts.

Many commenters addressed the burdens that would be imposed by the proposal due to the effective date and urged the Board to extend the proposed July 1, 2001, effective date for period ranging from one to two years. Most of these commenters argued that complying with the proposed Guidelines by July 1, 2001, would place a considerable burden on their businesses, particularly because the Guidelines would mandate changes to computer software, employee training, and compliance systems. As discussed above, the Board believes that the dates for full compliance with these Guidelines and the Privacy Rule should coincide. Financial institutions are required, as part of their initial privacy notices, to describe their policies and practices with respect to protecting the confidentiality and security of nonpublic personal information (12 CFR 216.6). The Board believes that if the effective date of these Guidelines is extended beyond July 1, 2001, then a financial institution may be placed in the position of providing an initial notice regarding confidentiality and security and thereafter amending the privacy policy to accurately refer to the federal standards once they became effective. Accordingly, the Board has adopted the proposed effective date of July 1, 2001.

Institutions covered. The Board's final Guidelines will apply to approximately 9,500 institutions, including state member banks, bank holding companies and certain of their nonbank subsidiaries or affiliates, state uninsured branches and agencies of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge and Agreement corporations. The Board estimates that over 4,500 of the institutions are small institutions with assets less than $100 million.

New compliance requirements. The final Guidelines contain new compliance requirements for all covered institutions, many of which are contained in existing supervisory guidance and examination procedures. Nonetheless, each must develop and implement a written information security program. As part of that program, institutions will be required to assess the reasonably foreseeable risks, taking into account the sensitivity of customer information, and assess the sufficiency of policies and procedures in place to control those risks. Institutions that use third party service providers to process customer information must exercise appropriate due diligence in selecting them, require them by contract to implement appropriate measures designed to meet the objectives of these Guidelines, and depending upon the institution's risk assessment, monitor them to confirm that they have satisfied their contractual obligations. As part of its compliance measures, an institution may need to train its employees or hire individuals with professional skills suitable to implementing the policies and procedures of its information security program, such as those skills necessary to test or review tests of its security measures. Some institutions may already have programs that meet these requirements, but others may not.

Minimizing impact on small institutions. The Board believes the requirements of the Act and these Guidelines may create additional burden for some small institutions. The Guidelines apply to all covered

institutions, regardless of size. The Act does not provide the Board with the authority to exempt a small institution from the requirement of implementing administrative, technical, and physical safeguards to protect the security and confidentiality of customer information. Although the Board could develop different guidelines depending on the size and complexity of a financial institution, the Board believes that differing treatment would not be appropriate, given that one of the stated purposes of the Act is to protect the confidentiality and security of customers' nonpublic personal information.

The Board believes that the compliance burden is minimized for small institutions because the Guidelines expressly allow institutions to develop security measures that are ``appropriate to the size and complexity of the [institution]''. The Guidelines do not mandate any particular policies, procedures, or security measures for any institution other than general requirements, such as to ``train staff'' or ``monitor its service providers to confirm that they have satisfied their [contractual] obligations''. The Board believes that the final Guidelines vest a small institution with a broad degree of discretion to design and implement an

[[Page 8629]]

information security program that suits its own organizational structure and risk profile.

FDIC: The Regulatory Flexibility Act (5 U.S.C. 601-612) (RFA) requires, subject to certain exceptions, that federal agencies prepare an initial regulatory flexibility analysis (IRFA) with a proposed rule and a final regulatory flexibility analysis (FRFA) with a final rule, unless the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities.\14\ At the time of issuance of the proposed Guidelines, the FDIC could not make such a determination for certification. Therefore, the FDIC issued an IRFA pursuant to section 603 of the RFA. After reviewing the comments submitted in response to the proposed Guidelines, the FDIC believes that it does not have sufficient information to determine whether the final Guidelines would have a significant economic impact on a substantial number of small entities. Hence, pursuant to section 604 of the RFA, the FDIC provides the following FRFA.

\14\ The RFA defines the term ``small entity'' in 5 U.S.C. 601 by reference to definitions published by the Small Business Administration (SBA). The SBA has defined a ``small entity'' for banking purposes as a national or commercial bank, or savings institution with less than $100 million in assets. See 13 CFR 121.201.

This FRFA incorporates the FDIC's initial findings, as set forth in the IRFA; addresses the comments submitted in response to the IRFA; and describes the steps the FDIC has taken in the final rule to minimize the impact on small entities, consistent with the objectives of the Gramm-Leach-Bliley Act (G-L-B Act). Also, in accordance with section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996 (Public Law 104-121), in the near future the FDIC will issue a compliance guide to assist small entities in complying with these Guidelines.

Small Entities to Which the Guidelines Will Apply

The final Guidelines will apply to all FDIC-insured state-nonmember banks, regardless of size, including those with assets of under $100 million. As of September 2000, there were 3,331 small banks out of a total of 5,130 FDIC-insured state-nonmember banks with assets of under $100 million. Title V, Subtitle A, of the GLBA does not provide either an exception for small banks or statutory authority upon which the FDIC could provide such an exception in the Guidelines.

Statement of the Need and Objectives of the Rule

The final Guidelines implement the provisions of Title V, Subtitle A, Section 501 of the GLBA addressing standards for safeguarding customer information. Section 501 requires the Agencies to publish standards for financial institutions relating to administrative, technical, and physical standards 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.

Protect against unauthorized access to or use of such records or information, which could result in substantial harm or inconvenience to any customer.

The final Guidelines 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.

Summary of Significant Issues Raised by the Public Comments; Description of Steps the Agency Has Taken in Response to the Comments to Minimize the Significant Economic Impact on Small Entities.

In the IRFA, the FDIC specifically requested information on whether small entities would be required to amend their operations in order to comply with the final Guidelines and the costs for such compliance. The FDIC also requested comment or information on the costs of establishing information security programs. The FDIC also sought comment on any significant alternatives, consistent with the G-L-B Act that would minimize the impact on small entities. The FDIC received a total of 63 comment letters. However, none of the comment letters specifically addressed the initial regulatory flexibility act section of the proposed Guidelines. Instead, many commenters, representing banks of various sizes, addressed the regulatory burdens in connection with their discussion of specific Guideline provisions.

The FDIC has sought to minimize the burden on all businesses, including small entities, in promulgating this final Guidelines. The statute does not authorize the FDIC to create exemptions from the G-L-B Act based on an institution's asset size. However, the FDIC carefully considered comments regarding alternatives designed to minimize the economic and overall burden of complying with the final Guidelines. The discussion below reviews some of the significant changes adopted in the final Guidelines to accomplish this purpose.

1. Issue the Rule as Guidelines or Regulations. The FDIC sought comment on whether to issue the rule as Guidelines or as regulations. All the comment letters stated that the rule should be issued in the form of Guidelines. Some community banks stated that the Guidelines were unnecessary because they already have information security programs in place but would prefer Guidelines to regulations. The commentary supported the use of Guidelines because guidelines typically provide more flexibility than regulations. Since technology changes rapidly, Guidelines would allow institutions to adapt to a changing

environment more quickly than regulations, which may become outdated. The FDIC has issued these standards as Guidelines. The final Guidelines establish standards that will allow each institution the flexibility to design an information security program to accommodate its particular level of complexity and scope of activities.

2. Definition of Customer. In the proposed Guidelines, the FDIC defined ``customer'' in the same manner as in the Privacy Rule. A ``customer'' is defined as 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. This definition does not include a business or a consumer who does not have an ongoing relationship with a financial institution. Almost all of the comments received by the FDIC agreed with the proposed definition and agreed that the definition should not be expanded to provide a common information security program for all types of records under the control of a financial institution. The Guidelines will apply only to consumer records as defined by the Privacy Rule, not business records. This will allow for a consistent interpretation of the term ``customer'' between the Guidelines and the Privacy Rule.

3. Involvement of the Bank's Board of Directors. The FDIC sought comment on how frequently management should report to the board of directors concerning the bank's information security program. Most of the comment letters stated that the final Guidelines should not dictate how frequently the bank reports to the board of directors and that the bank should have discretion in this regard. The comment letters clearly conveyed a preference to not have a reporting requirement. However, if there was to be one, commenters suggested that it be annual.

[[Page 8630]]

The Agencies have amended the Guidelines to require that a bank report at least annually to its board of directors. However, more frequent reporting will be necessary if a material event affecting the information security system occurs or if material modifications are made to the system.

4. Designation of Corporate Information Security Officer. The Agencies considered whether the Guidelines should require that the bank's board of directors designate a ``Corporate Information Security Officer'' with the responsibility to develop and administer the bank's information security program. Most of the comment letters requested that this requirement not be adopted because adding a new personnel position would be financially burdensome. The FDIC agrees that a new position with a specific title is not necessary. The final Guidelines do, however, require that the authority for the development, implementation, and administration of the bank's information security program be clearly expressed although not assigned to a particular individual.

5. Managing and Controlling Risk. Many comments focused on the eleven factors in the proposed Guidelines that banks should consider when evaluating the adequacy of their information security programs. The Agencies did not intend to mandate the security measures listed in section III.C. of the proposed Guidelines for all banks and all data. Instead the Agencies believe the security measures should be followed as appropriate for each bank's particular circumstances. Some concern was expressed that the proposed Guidelines required encryption of all customer information. The FDIC believes that a bank that has Internet-based transaction accounts or a transactional Web site may decide that encryption is appropriate, but a bank that processes all data internally may need different access restrictions. While a bank is to

consider each element in section III.C. in the design of its information security program, this is less burdensome than a requirement to include each element listed that section.

The proposed Guidelines provided that institutions train employees to recognize, respond to, and report suspicious attempts to obtain customer information directly to law enforcement agencies and regulatory agencies. Some comment letters stated that suspicious activity should be reported to management, not directly to law enforcement agencies and regulatory agencies. The FDIC believes employees should be made aware of federal reporting requirements and an institution's procedures for reporting suspicious activity. However, the Guidelines have been amended to allow financial institutions to decide who is to file a report to law enforcement agencies, consistent with other applicable regulations.

A significant number of comments stated that the FDIC should not require specific tests to ensure the security and confidentiality of customer information. Some comments stated that periodic testing is appropriate. The final Guidelines do not specify particular tests but provide that management should decide on the appropriate testing. Also, the final Guidelines require tests to be conducted or reviewed by people independent of those who operate the systems. Further, banks must review their service provider's security program to determine that it is consistent with the Guidelines. However, the final Guidelines do not require on-site inspections.

6. Effective Date. The effective date for the final Guidelines is July 1, 2001. As discussed in the section-by-section analysis, many of the comment letters urged the FDIC to extend the effective date of the Guidelines, particularly since this is the effective date for complying with the Privacy Rule. Several of the comments suggested the proposed effective date be extended for 12 to 18 months. However, the FDIC believes that the effective date for the Guidelines and the Privacy Rule should coincide. The Privacy Rule requires a financial institution to disclose to its customers that the bank maintains physical, electronic, and procedural safeguards to protect customers' nonpublic personal information. Appendix A of the Privacy Rule provides that this disclosure may refer to these federal guidelines. This is only meaningful if the final Guidelines for safeguarding customer information are effective when the disclosure is made. The Guidelines do provide a transition rule for contracts with service providers--essentially allowing a two-year compliance period for service provider contracts. A contract entered into on or before March 5, 2001, satisfies the provisions of this part until July 1, 2003, even if the contract does not include provisions delineating the servicer's duties and responsibilities to protect customer information described in section III.D. This additional time will allow financial institutions to make all necessary changes to service provider contracts and to comply with this segment of the Guidelines.

Summary of the Agency Assessment of Issues Raised in Public Comments

Most of the comment letters did not discuss actual compliance costs for implementing the provisions of the Guidelines. Some commenters stated that their bank has an established information security program and that information security is a customary business practice. The new compliance and reporting requirements will create additional costs for some institutions. These costs include: (1) Training staff; (2) monitoring outsourcing agreements; (3) performing due diligence before contracting with a service provider; (4) testing security systems; and (5) adjusting security programs due to technology changes. The comments

did not provide data from which the FDIC could quantify the cost of implementing the requirements of the GLBA. The compliance costs will vary among institutions.

Description/Estimate of Small Entities To Which the Guidelines Will Apply

The Guidelines will apply to approximately 3,300 FDIC insured State nonmember banks that are small entities (assets less than $100 million) as defined in the RFA.

Description of Projected Reporting, Record-Keeping, and Other Compliance Requirements

The final Guidelines contain standards for the protection of customer records and information that apply to all FDIC-insured state-nonmember banks. Institutions will be required to report annually to the bank's board of directors concerning the bank's information security program. Institutions will need to develop a training program that is designed to implement the institution's information security policies and procedures. An institution's information security system will be tested to ensure the controls and procedures of the program work properly. However, the final Guidelines do not specify what particular tests the bank should undertake. The final Guidelines state that the tests are to be conducted or reviewed by persons who are independent of those who operate the systems. Institutions will have to exercise due diligence in the selection of service providers to ensure that the bank's customer information will be protected consistent with these Guidelines. And institutions will have to monitor these service provider arrangements to confirm that the institution's customer information is protected, which may be accomplished by reviewing service provider audits

[[Page 8631]]

and summaries of test results. Also, institutions will need to adjust their security program as technology changes.

The types of professional skills within the institution necessary to prepare the report to the board would include an understanding of the institution's information security program, a level of technical knowledge of the hardware and software systems to evaluate test results recommending substantial modifications; and the ability to evaluate and report on the institution's steps to oversee service provider arrangements.

OTS: The Regulatory Flexibility Act (RFA),\15\ requires OTS to prepare a final regulatory flexibility analysis with these final Guidelines unless the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities. OTS has evaluated the effects these Guidelines will have on small entities. In issuing proposed Guidelines, OTS specifically sought comment on the costs of establishing and operating information security programs, but no commenters provided specific cost information. Institutions cannot yet know how they will implement their information security programs and therefore have difficulty quantifying the associated costs. The Director of OTS considered certifying, under section 605(b) of the RFA, that these guidelines will not have a significant economic impact on a substantial number of small entities. However, because OTS cannot quantify the impact the Guidelines will have on small entities, and in the interests of thoroughness, OTS does not certify that the Guidelines will not have a significant economic

impact on a substantial number of small entities. Instead, OTS has prepared the following final regulatory flexibility analysis.

\15\ U.S.C. 604(a).

A. Reasons for Final Action

OTS issues these Guidelines pursuant to section 501 of the G-L-B Act. As described in this preamble and in the notice of proposed action, 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 the substantial harm or inconvenience to any customer.

B. Objectives of and Legal Basis for Final Action

The objectives of the Guidelines are described in the Supplementary Information section above. The legal bases for the final action are: section 501 of the G-L-B Act; section 39 of the FDI Act; 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 Final Action Will Apply

These Guidelines will 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.\16\

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

The Guidelines do not require any reports to OTS. As discussed more fully above, they do require institutions to have a written information security program, and to make an appropriate report to the board of directors, or a board committee, at least annually. The Guidelines require institutions to establish an information security program, if they do not already have one. The Guidelines require institutions to assess the risks to their customer security and to adopt appropriate measures to control those risks. Institutions must also test the key controls, commensurate with the risks. Institutions must use appropriate due diligence in selecting outside service providers, and require service providers, by contract, to implement appropriate security measures. Finally, where appropriate, the Guidelines require institutions to monitor their service providers.

\16\ For purposes of the Regulatory Flexibility Act, a small savings association is one with less than $100 million in assets. 13 CFR 121.201 (Division H). There are approximately 487 such small savings associations, approximately 97 of which have subsidiaries.

Professional skills, such as skills of computer hardware and software, will be necessary to assess information security needs, and

to design and implement an information security program. The particular skills needed will be commensurate with the nature of each institution's system, i.e. more skills will be needed in institutions with sophisticated and extensive computerization. As a result, small entities with less extensive computerization are likely to have less burdensome compliance needs than large entities. Institutions that use outside service providers may require legal skills to draft appropriate language for contracts with service providers.

E. Public Comment and Significant Alternatives

OTS did not receive any public comment on its initial regulatory flexibility analysis, although it did receive comments on the proposal in general, and on the Guidelines' impact on small entities in particular. OTS addresses these below.

OTS has considered publishing standards using only the broad language in section 501(b) of the G-L-B Act, as supported by one commenter. The Agencies rejected this alternative in favor of more comprehensive Guidelines. Using only the general statutory language would permit institutions maximum flexibility in implementing information security protections and would not put institutions at a competitive disadvantage with respect to institutions not subject to the same security standards. However, using the statutory language alone would not provide enough guidance to institutions about what risks need to be addressed or what types of protections are appropriate. Small institutions in particular may need guidance in this area. One trade association that represents community banks commented that institutions need guidance to determine what level of information security the Agencies will look for, and that community banks in particular need guidance in this area. OTS believes that the alternative it chose, more comprehensive standards, provides helpful guidance without sacrificing flexibility.

OTS has also considered the alternative of defining ``service provider'' more narrowly than in the proposed Guidelines to reduce regulatory burden. The Guidelines require a financial institution to take appropriate steps to protect customer information provided to a service provider. Due to limited resources, small institutions may need to outsource a disproportionately larger number of functions than large institutions outsource, and accordingly have a greater need for service providers. Thus, the burdens associated with service providers may fall more heavily on small institutions than on large institutions. But the risks to information security do not necessarily vary depending on a service provider's identity. Rather, they vary depending on the type and volume of information to which a service provider has access, the safeguards it has in place, and what the service provider does with the

information. Basing the requirements as to service providers on a service provider's identity would not necessarily focus protections on areas of risk. For this reason, the final Guidelines focus the protections regarding service providers on the risks involved rather than on the service provider's identity. This approach should provide the necessary protections without unnecessary burden on small institutions.

OTS reviewed the alternative of requiring an institution's board of directors to designate a Corporate Information Security Officer who would have authority, with approval by the board, to develop and administer the institution's information security program. However, ultimately, the agencies rejected the idea of having financial

institutions create a new position to fulfill this purpose. Instead, the Guidelines allow financial institutions the flexibility to determine who should be assigned specific roles in implementing the institution's security program. As a result, small institutions will be relieved of a potential burden.

The final Guidelines incorporate new provisions not in the proposed Guidelines designed to add flexibility to assist all institutions, large and small. For example, the final Guidelines, unlike the proposal, do not specify particular tasks for management. Instead, the final Guidelines allow each institution the flexibility to decide for itself the most efficient allocation of its personnel. Similarly, the final Guidelines allow institutions to delegate board duties to board committees. Additionally, in the final guidelines the Agencies removed the requirement that information security programs ``shall * * * ensure'' the security and confidentiality of customer information. Instead, the guidelines say the program ``shall be designed to * * * ensure'' the security and confidentiality of customer information. The final Guidelines further incorporate more flexibility than the proposal concerning testing systems. The proposal required third parties of staff independent of those who maintain the program to test it, and required third parties or staff independent of the testers to review test results. To add flexibility, the final Guidelines more simply require staff or third parties independent of those who develop or maintain the programs to conduct or review the tests. These changes should serve to reduce the burden of the Guidelines.

C. Executive Order 12866

The Comptroller of the Currency and the Office of Thrift Supervision have determined that this rule does not constitute a ``significant regulatory action'' for the purposes of Executive Order 12866. The OCC and OTS are issuing the Guidelines in accordance with the requirements of Sections 501 and 505(b) of the G-L-B Act and not under their own authority. Even absent the requirements of the G-L-B Act, if the OCC and OTS had issued the rule under their own authority, the rule would not constitute a ``significant regulatory action'' for purposes of Executive Order 12866.

The standards established by the Guidelines are very flexible and allow each institution the discretion to have an information security program that suits its particular size , complexity and the nature and scope of its activities. Further, the standards reflect good business practices and guidance previously issued by the OCC, OTS, and the FFIEC. Accordingly, most if not all institutions already have information security programs in place that are consistent with the Guidelines. In such cases, little or no modification to an institution's program will be required.

D. Unfunded Mandates Act of 1995

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 and OTS believe that most institutions already have established an information security program because it is a sound business practice that also has been addressed in existing supervisory guidance. Therefore, the OCC and OTS have determined that the Guidelines will not 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 and OTS have not prepared a budgetary impact statement or specifically addressed the regulatory alternatives considered.

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. Consumer protection, Privacy, Savings associations.

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 amended as follows:

[[Page 8633]]

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, 1831-p, 3102(b); 15 U.S.C. 6801, 6805(b)(1).

2. Revise Sec. 30.1 to read as follows:

Sec. 30.1 Scope.

(a) The rules set forth in this part 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 Sec. 30.2, revise the last sentence to read as follows:

Sec. 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 Sec. 30.3, revise paragraph (a) to read as follows:

Sec. 30.3 Determination and notification of failure to meet safety and soundness standard and request for compliance plan.

(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

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. 1. Except as modified in the Guidelines, or unless the context otherwise requires, the terms used in these Guidelines 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. For purposes of the Guidelines, the following definitions apply:

a. 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.

b. Customer means any customer of the bank as defined in Sec. 40.3(h) of this chapter.

c. Customer information means any record containing nonpublic personal information, as defined in Sec. 40.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the bank.

d. Customer information systems means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

e. Service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank.

II. Standards for Safeguarding Customer Information

A. Information Security Program. Each bank shall implement a comprehensive written 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. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

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

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.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors. The board of directors or an appropriate committee of the board of each bank shall:

1. Approve the bank's written information security program; and

2. Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk. Each bank shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

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

C. Manage and Control Risk. Each bank shall:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized

individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

[[Page 8634]]

b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

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

d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;

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

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

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

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

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

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

D. Oversee Service Provider Arrangements. Each bank shall:

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

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

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

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

F. Report to the Board. Each bank shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank's compliance with these Guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control

decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

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

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

6. Appendix C to part 30 is removed.

Dated: December 21, 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 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, 78l(b), 78l(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 Sec. 208.3 to revise paragraph (d)(1) to read as follows:

Sec. 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

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 Secs. 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.

1. Except as modified in the Guidelines, or unless the context otherwise requires, the terms used in these Guidelines 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. For purposes of the Guidelines, the following definitions apply:

a. 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.

b. Customer means any customer of the bank as defined in Sec. 216.3(h) of this chapter.

c. Customer information means any record containing nonpublic personal information, as defined in Sec. 216.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the bank.

d. Customer information systems means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

e. Service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank.

f. 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 written 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. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated. 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 be designed to:

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.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors. The board of directors or an appropriate committee of the board of each bank shall:

1. Approve the bank's written information security program; and

2. Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk. Each bank shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

3. Assess the sufficiency of policies, procedures, customer

information systems, and other arrangements in place to control risks.

C. Manage and Control Risk. Each bank shall:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

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

d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;

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

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

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

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

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

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

D. Oversee Service Provider Arrangements. Each bank shall:

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

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

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

E. Adjust the Program. Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its

customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and

acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

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

G. Implement the Standards.

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

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

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 Sec. 211.9 to read as follows:

Sec. 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 Sec. 211.24, add new paragraph (i) to read as follows:

Sec. 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 Sec. 225.1, add new paragraph (c)(16) to read as follows:

Sec. 225.1 Authority, purpose, and scope.

* * * * *

(c) * * *

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

9. In Sec. 225.4, add new paragraph (h) to read as follows:

Sec. 225.4 Corporate practices.

* * * * *

(h) 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

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 under these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the Board.

C. Definitions. 1. Except as modified in the Guidelines, or unless the context otherwise requires, the terms used in these Guidelines 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. For purposes of the Guidelines, the following definitions apply:

a. 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.

b. Customer means any customer of the bank holding company as defined in Sec. 216.3(h) of this chapter.

c. Customer information means any record containing nonpublic personal information, as defined in Sec. 216.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the bank holding company.

d. Customer information systems means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

e. Service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank holding company.

f. 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 written 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. While all parts of the bank holding company are not required to implement a uniform set of policies, all elements of the information security program must be coordinated. 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 be designed to:

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.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors. The board of directors or an appropriate committee of the board of each bank holding company shall:

1. Approve the bank holding company's written information security program; and

2. Oversee the development, implementation, and maintenance of the bank holding company's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk. Each bank holding company shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

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

C. Manage and Control Risk. Each bank holding company shall:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank holding company's activities. Each bank holding company must consider whether the following security measures are appropriate for the bank holding company and, if so, adopt those measures the bank holding company concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

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

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

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

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

g. Response programs that specify actions to be taken when the

bank holding company suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

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

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

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

D. Oversee Service Provider Arrangements. Each bank holding company shall:

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

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

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

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

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

G. Implement the Standards.

1. Effective date. Each bank holding company must implement an information security program pursuant to these Guidelines by July 1, 2001.

2. Two-year grandfathering of agreements with service providers. Until July 1, 2003, a contract that a bank holding company has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of section III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of customer information, as long as the bank holding company entered into the contract on or before March 5, 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 Sec. 263.302 to revise paragraph (a) to read as follows:

Sec. 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.
* * * * *

[[Page 8638]]

By order of the Board of Governors of the Federal Reserve System, January 4, 2001.
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 Regulations are amended as follows:

PART 308--RULES OF PRACTICE AND PROCEDURE

1. The authority citation for part 308 is revised 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; 6801(b), 6805(b)(1), 28 U.S.C. 2461 note; 31 U.S.C. 330, 5321; 42 U.S.C. 4012a; Sec. 3100(s), Pub. L. 104-134, 110 Stat. 1321-358.

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

Sec. 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. 1819(Tenth), 1831p-1; 15 U.S.C. 6801(b), 6805(b)(1).

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

Sec. 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

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 Federal Deposit Insurance Corporation (FDIC) has authority. Such entities, referred to as ``the bank'' 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. 1. Except as modified in the Guidelines, or unless the context otherwise requires, the terms used in these Guidelines 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. For purposes of the Guidelines, the following definitions apply:

a. 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.

b. Customer means any customer of the bank as defined in Sec. 332.3(h) of this chapter.

c. Customer information means any record containing nonpublic personal information, as defined in Sec. 332.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the bank.

d. Customer information systems means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

e. Service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank.

II. Standards for Safeguarding Customer Information

A. Information Security Program. Each bank shall implement a comprehensive written 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. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

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

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.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors. The board of directors or an appropriate committee of the board of each bank shall:
1. Approve the bank's written information security program; and
2. Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.
B. Assess Risk.
Each bank shall:
1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

[[Page 8639]]

3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.
C. Manage and Control Risk. Each bank shall:
1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:
a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.
b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;
e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;
f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

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

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

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

D. Oversee Service Provider Arrangements. Each bank shall:

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

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

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

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

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

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

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

By order of the Board of Directors.

Dated at Washington, D.C., this 21st day of December, 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 amended as follows:

PART 568--SECURITY PROCEDURES

1. The authority citation of 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 Sec. 568.1 by revising paragraph (a) to read as follows:

Sec. 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 new Sec. 568.5 to read as follows:

Sec. 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 Sec. 570.1 by adding a sentence at the end of paragraph (a) and revising the last sentence of paragraph (b) to read as follows:

Sec. 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 Sec. 570.2 by revising paragraph (a) to read as follows:

[[Page 8640]]

Sec. 570.2 Determination and notification of failure to meet safety and soundness standards and request for compliance plan.

(a) Determination. OTS may, based upon an examination, inspection, or any other information that becomes available to 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

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 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 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. 1. Except as modified in the Guidelines, or unless the context otherwise requires, the terms used in these Guidelines 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. For purposes of the Guidelines, the following definitions apply:

a. Customer means any of your customers as defined in Sec. 573.3(h) of this chapter.

b. Customer information means any record containing nonpublic personal information, as defined in Sec. 573.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that you maintain or that is maintained on your behalf.

c. Customer information systems means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

d. Service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to you.

II. Standards for Safeguarding Customer Information

A. Information Security Program. You shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to your size and complexity and the nature and scope of your activities. While all parts of your organization are not required to implement a uniform set of policies, all elements of your information security program must be coordinated.

B. Objectives. Your information security program shall be designed to:

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.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors. Your board of directors or an appropriate committee of the board shall:

1. Approve your written information security program; and

2. Oversee the development, implementation, and maintenance of your information security program, including assigning specific responsibility for its implementation and reviewing reports from

management.

B. Assess Risk. You shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

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

C. Manage and Control Risk. You shall:

1. Design your information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of your activities. You must consider whether the following security measures are appropriate for you and, if so, adopt those measures you conclude are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

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

d. Procedures designed to ensure that customer information system modifications are consistent with your information security program;

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

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

g. Response programs that specify actions for you to take when you suspect or detect that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

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

2. Train staff to implement your information security program.

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

D. Oversee Service Provider Arrangements. You shall:

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

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

3. Where indicated by your risk assessment, monitor your service providers to confirm that they have satisfied their

obligations as required by paragraph D.2. As part of this monitoring, you should review audits, summaries of test results, or other equivalent evaluations of your service providers.

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

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

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

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

Dated: December 19, 2000.

By the Office of Thrift Supervision.
Ellen Seidman,
Director.
[FR Doc. 01-1114 Filed 1-31-01; 8:45 am]
BILLING CODE 4810-33-P; 6210-01-P; 6714-01-P; 6720-01-P