(e) *Can I comply with this AD in any other way?* You may use an alternative method of compliance or adjust the compliance time if:

(1) Your alternative method of compliance provides an equivalent level of safety; and

(2) The Manager, Wichita Aircraft Certification Office (ACO), approves your alternative. Send your request through an FAA Principal Maintenance Inspector, who may add comments and then send it to the Manager, Wichita ACO.

Note: This AD applies to each airplane identified in paragraph (a) of this AD, regardless of whether it has been modified, altered, or repaired in the area subject to the requirements of this AD. For airplanes that have been modified, altered, or repaired so that the performance of the requirements of this AD is affected, the owner/operator must request approval for an alternative method of compliance in accordance with paragraph (e) of this AD. You should include in the request an assessment of the effect of the modification, alteration, or repair on the unsafe condition addressed by this AD; and, if you have not eliminated the unsafe condition, specific actions you propose to address it.

(f) *Where can I get information about any already-approved alternative methods of compliance?* Contact Paul C. DeVore, Aerospace Engineer, FAA, Wichita Aircraft Certification Office, 1801 Airport Road, Mid-Continent Airport, Wichita, Kansas 67209; telephone: (316) 946–4142; facsimile: (316) 946–4407.

(g) *What if I need to fly the airplane to another location to comply with this AD?* The FAA can issue a special flight permit under sections 21.197 and 21.199 of the Federal Aviation Regulations (14 CFR 21.197 and 21.199) to operate your airplane to a location where you can do the requirements of this AD.

(h) *How do I get copies of the documents referenced in this AD?* You may get the service information referenced in the AD from Raytheon Aircraft Company, P.O. Box 85, Wichita, Kansas 67201–0085; telephone: (800) 429–5372 or (316) 676–3140; or on the Internet at <http://www.raytheon.com/rac/servinfo/27-3013.pdf>. This file is in Adobe Portable Document Format. The Acrobat Reader is available at <http://www.adobe.com/>. You may read this document at FAA, Central Region, Office of the Regional Counsel, 901 Locust, Room 506, Kansas City, Missouri 64106.

Issued in Kansas City, Missouri, on August 31, 2000.

Carolanne L. Cabrini,

Acting Manager, Small Airplane Directorate, Aircraft Certification Service.

[FR Doc. 00–22909 Filed 9–6–00; 8:45 am]

BILLING CODE 4910–13–P

FEDERAL TRADE COMMISSION

16 CFR Part 313

Privacy of Customer Financial Information—Security

AGENCY: Federal Trade Commission.

ACTION: Advance notice of proposed rulemaking and request for comment.

SUMMARY: In this document, the Federal Trade Commission (the ''Commission'' or ''FTC'') requests comment on developing the administrative, technical, and physical information Safeguards Rule that the Commission is required to establish pursuant to section 501(b) of the Gramm-Leach-Bliley Act (the ''G–L–B Act'' or ''Act'') for the financial institutions under its jurisdiction, as set forth in section 505(a)(7). After reviewing the comments received in response to this document and request for comment, the Commission will issue a notice of proposed rulemaking.

DATES: Comments must be received on or before October 10, 2000.

ADDRESSES: Written comments should be addressed to: Secretary, Federal Trade Commission, Room H–159, 600 Pennsylvania Avenue, NW., Washington, DC 20580. The Commission requests that commenters submit the original plus five copies, if feasible. Comments should also be submitted, if possible, in electronic form, on either a 5¼ or 3½ inch computer disk, with a disk label stating the name of the commenter and the name version of the word processing program used to create the document. (Programs based on DOS or Windows are preferred. Files from other operating systems should be submitted in ASCII format.) Alternatively, the Commission will accept comments submitted to the following e-mail address: *GLB501Rule@ftc.gov.* Those commenters submitting comments by e-mail are advised to confirm receipt by consulting the postings on the Commission's website at www.ftc.gov. In addition, commenters submitting comments by e-mail are requested to indicate whether they are also providing their comments in other formats. Individual members of the public filing comments need not submit multiple copies or comments in electronic form. All submissions should be captioned ''Gramm-Leach-Bliley Act Privacy Safeguards Rule, 16 CFR Part 313–Comment.''

FOR FURTHER INFORMATION CONTACT: Laura Berger, Attorney, Division of Financial Practices, Federal Trade Commission, Washington, DC 20580, 202–326–3224.

SUPPLEMENTARY INFORMATION

Section A. Background

On November 12, 1999, President Clinton signed the G–L–B Act (Pub. L. 106–102) into law. Subtitle A of Title V of the Act, captioned Disclosure of Nonpublic Personal Information, limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose to all of its customers the institution's privacy policies and practices with respect to information sharing with both affiliates and nonaffiliated third parties. Title V also requires the Commission to establish by rule appropriate standards for the financial institutions subject to its jurisdiction relating to administrative, technical, and physical safeguards (hereinafter ''Safeguards Rule'') to insure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

On May 12, 2000, the Commission issued a final rule implementing the requirements of Subtitle A that relate to the disclosure of nonpublic personal information about a consumer to nonaffiliated third parties and the disclosure to all customers of the institution's privacy policies and practices with respect to information sharing with both affiliates and nonaffiliated third parties (hereinafter ''Privacy Rule'').[1] As required by section 504 of Subtitle A, the Commission worked with other federal government agencies and authorities (hereinafter ''the agencies'') [2] to ensure that the Privacy Rule was consistent and comparable with the regulations prescribed by the agencies. The Privacy Rule will take effect on November 13, 2000, and full compliance is required on or before July 1, 2001.

The Act does not require the Commission (or other agencies) to coordinate in developing a Safeguards Rule, and permits the agencies, with the exception of the SEC and the Commission, to develop their safeguards standards by issuing guidelines.

[1] The rule was published in the **Federal Register** at 65 FR 33646 (May 24, 2000).

[2] The Office of the Comptroller of the Currency (''OCC''); the Board of Governors of the Federal Reserve System (''Board''); the Federal Deposit Insurance Corporation (''FDIC''); the Office of Thrift Supervision (''OTS''); the National Credit Union Administration (''NCUA''); the Secretary of the Treasury (''Treasury''); and the Securities and Exchange Commission (''SEC''). Section 504 required these agencies to prescribe, within six months of the Act's date of enactment (by May 12, 2000), ''such regulations as may be necessary to carry out the purposes of [Subtitle A] with respect to financial institutions subject to their jurisdiction under section 505.''

On June 26, 2000, the OCC, Board, OTC, and FDIC published a joint **Federal Register** notice containing proposed Guidelines establishing standards for safeguarding customer information (hereinafter ''proposed Interagency Guidelines''), but requested comment as to whether a rule would be preferable to guidelines. 65 FR 39,471 (June 26, 2000). As proposed, the Interagency Guidelines will appear as an appendix to each Agency's Standards for Safety and Soundness. The NCUA published a **Federal Register** notice containing proposed safeguards guidelines on June 14, 2000. 65 FR 37,302. The NCUA's guidelines, as proposed, will be issued as an amendment to the NCUA's existing regulation governing security programs in federally-insured credit unions. As with the Privacy Rule, Treasury will not be issuing a separate rule. On June 22, 2000, the SEC adopted a final safeguards rule as part of its Privacy of Consumer Financial Information Final rule. See *www.sec.gov/rules/final34–42974.htm.*

The SEC's safeguards rule restates the objectives of section 501(b), and passes along to financial institutions the requirement to develop policies and procedures that are ''reasonably designed'' to meet these goals.

Prior to issuing a proposed Safeguards Rule, the Commission seeks public comment on the following questions concerning the scope and potential requirements of such a rule. In formulating a proposed rule, the Commission will consider the costs and benefits of the proposed rule's requirements.

Section B. Questions as to Scope of the Commission's Safeguards Rule

In order to develop the Safeguards Rule the Commission is required to implement, the Commission seeks comment on several issues relevant to the proper scope of the rule.

1. Range of Information Subject to the Safeguards Rule

The Commission requests comment on the range of information that should be subject to the Safeguards Rule. The privacy provisions of Subtitle A of Title V of the Act require that financial institutions provide certain notices of their privacy policies to individuals, but vary these requirements according to whether the individual is a ''customer'' or a ''consumer'' of the financial institution. Section 502 (a) & (b) (consumers); Section 503 (customers). Respecting consumers, the G–L–B Act generally prohibits a financial institution from disclosing nonpublic personal information about a consumer to a nonaffiliated third party without first notifying the consumer and providing an opportunity to opt out of the disclosure. Section 502 (a) & (b). Customers, however, are entitled to notice of a financial institution's privacy policies at the time that a customer relationship is established, and annually thereafter during the continuation of the relationship, regardless of whether nonpublic personal information will be shared with nonaffiliated third parties. Section 503.

In contrast to the privacy provisions, section 501 of the G–L–B Act refers solely to customers' nonpublic personal information and customer records and information. Section 501(a) sets forth the ''policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information,'' while section 501(b), ''in furtherance of the policy in subsection (a)'', requires the Commission to establish standards: ''(1) To 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) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.'' Sections 501(a), 501(b)(1)–(3) (emphases added). The Commission requests comment on what constitutes ''customer records and information'' under subsection (b), particularly in light of the reference to ''customers' nonpublic personal information'' in subsection (a). Also, should the definition of ''customer records and information'' under the Safeguards Rule be similar to the definition of ''nonpublic personal information'' for customers under the Commission's Privacy Rule? Should the Safeguards Rule ever apply to ''consumer'' information maintained by a financial institution? Where, for example, a financial institution cannot accurately separate its customer records and information from its consumer records, should the Safeguards Rule require the financial institution to safeguard both types of records?

2. Range of Financial Institution Subject to the Safeguards Rule

The Commission also requests comment on the range of financial institutions to which the Safeguards Rule should apply. With certain exceptions, a financial institution is defined in the Act as any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). Under the Commission's Privacy Rule, any institution that is significantly engaged in such financial activities is a financial institution. 16 CFR 313.3(k)(1). However, only those financial institutions that have ''consumers'' or establish ''customer relationships'' have an obligation to disclose their privacy policies under the Act. §§ 502 & 503; 16 CFR 313.4 & 313.5. Financial institutions that have no customer relationships or consumers, but obtain nonpublic personal information from another financial institution (*see, e.g.,* 16 CFR 313.13) are subject to the Privacy Rule's limitations on redisclosure and reuse of nonpublic personal information. 16 CFR 313.11. How should the Safeguard Rule apply when a financial institution discloses customer records and information to a financial institution that has no customer relationships or consumers? Should the Safeguards Rule require the originating financial institution to disclose its ''customer records and information'' subject to the agreement of the party (*i.e.,* a different financial institution) receiving the information to comply with the Safeguards Rule in its handling of the information?

Section C. Questions as to Other Aspects of the Commission's Safeguards Rule

The Safeguards Rule must establish appropriate standards for financial institutions subject to its jurisdiction relating to the administrative, technical, and physical safeguards against the harms contemplated by the Act, in order to protect customer records and information from anticipated threats and hazards, and provide them with security and confidentiality, including protection against unauthorized access or use. At the same time, the Commission recognizes that financial institutions may deem different safeguards appropriate according to the size and complexity of the financial institution, the nature and scope of its activities, and the nature of its records. In what ways, if any, should the Safeguards Rule take into account the need for financial institutions to keep pace with changing technology and other changes to their operational environment? Should the Safeguards Rule set forth minimum procedures a financial institution must follow, a minimum level of effectiveness financial institutions must maintain through their safeguards, or a combination of both? Do any current private standards, association rules, or

guides provide useful guidance to the Commission in its formulation of safeguards standards for financial institutions subject to the Commission's jurisdiction? Should the Safeguards Rule delineate mechanisms for financial institutions to demonstrate compliance with the Rule? For example, should the Safeguards Rule require financial institutions to use a particular audit process to measure their own compliance?

1. Small Financial Institutions

The Commission seeks comment on how the Safeguards Rule will achieve the results contemplated by the Act without unduly burdening the ability of small financial institutions to serve consumers. Further, to the extent commenters recommend that the Safeguards Rule require specific administrative, technical and physical safeguards, the Commission requests comment on whether the requirements are appropriate for small financial institutions.

2. Specificity of the Safeguards Rule

What specific steps, if any, should the Safeguards Rule require financial institutions to take to provide administrative, technical, and physical safeguards for their customer records and information? Is a different level of specificity appropriate according to whether the Safeguards Rule is prescribing administrative, technical, or physical measures? For example, should the Safeguards Rule prescribe specific minimum measures, such as shedding of discarded paper records, that a financial institution must take to provide for the physical security of its customer records and information? Similarly, to provide for administrative security, should the Safeguards Rule require that financial institutions take particular minimum steps, such as designating an employee who is responsible for monitoring internal access to customer records and information? Alternatively, when dealing with technical safeguards, should the Safeguards Rule set forth a more general standard for adequate safeguards, such as ''effective controls or programs'' or ''reasonable policies and procedures''? If the Safeguards Rule provides a more general standard for administrative, technical, or physical safeguards, what examples or other clarification of adequate safeguards should be included? For example, should the Safeguards Rule set forth categories or areas of administrative, technical and physical safeguards (''safeguards categories'') for financial institutions to address in designing and implementing safeguards appropriate to their operations? Would safeguards categories that require a financial institution to focus on particular areas of operations, such as ''Personnel Training and Management,'' ''Information Storage and Transmission,'' and ''Records Disposal,'' assist financial institutions to develop and maintain safeguards in a thorough and consistent manner? Would a common standard, such as ''effective controls or programs'' or ''reasonable policies and procedures'' suggested above, apply to every safeguards category, or would some safeguards categories, such as ''Records Disposal,'' be subject to more objective requirements?

3. Statutory Objectives

The Commission seeks comment on how the Safeguards Rule should reflect the three objectives for information safeguards that are set forth in section 501(b)(1)–(3) of the Act.

a. Anticipation of Threats or Hazards to Security or Integrity

Section 501(b) requires the Commission to establish standards for administrative, technical and physical safeguards to ''protect against anticipated threats or hazards to the security or integrity'' of customer records and information obtained by financial institutions. Section 501(b)(2). Should ''anticipated threats and hazards'' be defined, and if so, how? Should the Safeguards Rule require financial institutions to anticipate threats and hazards according to particular procedures? If so, what threats and hazards should be assessed, and by what procedures? Should the Safeguards Rule require financial institutions to assess threats and hazards according to particular categories (''risk categories''), such as ''Risks to Physical Security,'' ''Risks to Integrity,'' or ''Risks in Records Disposal''? When assessing threats and hazards, should a financial institution be required to classify the value and sensitivity of the records to be protected and/or the gravity of any threats? Under what circumstances, if any, should financial institutions be required to conduct these assessments in writing?

Should the Safeguards Rule require that financial institutions reassess the threats or hazards to their information security systems, and, if so, at what intervals? Should the Safeguards Rule define technical or other changes to an institution's information security environment that warrant reevaluation of existing safeguards? Among other times, should a financial institution be required to assess threats and hazards within a reasonable time after it knows or should know of a new or emerging threat or hazard to the security or integrity of its records? Similarly, should the Safeguards Rule require that the effectiveness of existing safeguards be evaluated through appropriate tests? If so, how specifically should the standards define these tests?

Finally, how should the Safeguards Rule protect against anticipated threats and hazards to the integrity of customer records and information? Should protecting integrity of customer records and information include requiring a financial institution to notify a customer when his or her records and information are subject to loss, damage, or unauthorized access? Does insuring integrity of customer records and information require that customers be granted periodic access to their records, in order to monitor the accuracy of this information?

b. Preventing Unwarranted Access and Use

In addition to requiring protection against anticipated threats and hazards, section 501(b) requires that the safeguards standards ''protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.'' Section 501(b)(3). Should ''unauthorized access'' and ''unauthorized use'' be defined, and if so, how? Should the Safeguards Rule require financial institutions to follow certain minimum procedures to ''protect against unauthorized access to'' customer records and information? Are there any circumstances under which financial institutions should be required to maintain written records of their procedures for preventing unauthorized access and use?

If the Safeguards Rule should require financial institutions to follow certain minimum steps to prevent unauthorized access and use, what procedures are most appropriate for the diverse range of financial institutions subject to the Commission's jurisdiction? For example, should the Safeguards Rule require that financial institutions designate a person within the institution who is responsible for preventing and detecting unauthorized access to and use of customer records and information? Similarly, should the Safeguards Rule require that financial institutions enter into confidentiality agreements with their employees or train their employees in procedures for preventing unauthorized access to and

use of customer records and information?

c. Insuring Security and Confidentiality

In addition to requiring protection against anticipated threats and hazards and against unauthorized access and use, section 501(b) requires that the safeguards standards ''insure the security and confidentiality of customer records and information'' Section 501(b)(1). Does this requirement mean something more than protecting against anticipated threats and hazards and unauthorized access and use? In particular, what should insuring ''confidentiality'' of information mean? What measures should the Safeguards Rule require a financial institution to take to maintain the confidentiality and security of customer records and information that it discloses? Where applicable, should the Safeguards Rule require a financial institution that discloses customer records and information to notify the recipients of the limitations on reuse and redisclosure of the information imposed by the Privacy Rule?

d. Consideration of Other Agencies' Safeguards Standards

The proposed Interagency Guidelines and the NCUA's proposed Guidelines (collectively, ''the proposed Guidelines'') both require regulated financial institutions to implement an ''Information Security Program'' that is developed by following certain procedures outlined by the respective proposed Guidelines. In their respective section III.A., the proposed Guidelines require each financial institution to involve its board of directors and management in various aspects of developing, implementing, and assessing an information security program. Under both proposals, a financial institution must take four basic steps to develop an information security program: (1) Identify and assess the risks that may threaten protected information; (2) develop a written plan containing policies and procedures to manage and control these risks; (3) implement and test the plan; and (4) adjust the plan on a continuing basis to account for changes in technology, the sensitivity of the protected information, and internal or external threats to information security. Similarly, in their respective sections III.C., both proposals provide a list of factors that a financial institution should consider in developing its information security program. The factors include specific potential elements of a security plan that should be considered, such as ''contract provisions and oversight mechanisms'' to protect the security of information handled by service providers (respective III.C.(g)), as well as broader issues that the security plan should address, such as ''[a]ccess rights to [covered] information,'' (respective III.C.(a)). Using the procedures provided by the proposed Guidelines, each covered financial institution is to develop a comprehensive information security program, the adequacy of which will be reviewed by the relevant agency through established oversight procedures, such as safety and soundness reviews. Finally, in their respective sections III.D., the proposed Guidelines require financial institutions to exercise due diligence in managing and monitoring outsourcing arrangements, in order to make sure that its service providers have implemented an effective information security program.

The proposed guidelines focus on the procedures that should be followed to develop a written information security program, and do not specify particular security measures that must be adopted. They do provide, however, that the Board of Directors must oversee efforts to develop, implement, and maintain an ''effective'' information security program. Should the Commission's Safeguards Rule be similar to the proposed Guidelines, and if so, how? Does the Act's requirement that the Commission issue a rule, rather than guidelines, warrant a different approach? Does the fact that the Commission does not conduct regular examination of financial institutions warrant more specific security measures? What, if any, features of the more general approach to safeguards taken by the SEC in its Privacy of Consumer Financial Information Final Rule (described in Section A, *supra*) are suitable for the Commission's Safeguards Rule?

By direction of the Commission.

C. Landis Plummer,

Acting Secretary.

[FR Doc. 00–22945 Filed 9–6–00; 8:45 am]

BILLING CODE 6750–01–M

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 210 and 240

[Release No. 33–7883, 34–43219; File No. S7–13–00]

Revision of the Commission's Auditor Independence Requirements

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule; extension of time period to submit materials for public hearing on September 20, 2000; location of hearings.

SUMMARY: The Securities and Exchange Commission is extending the time period by which participants must submit written materials for the public hearing on September 20, 2000, on the proposed rule Revision of the Commission's Auditor Independence Requirements (65 FR 43148 July 12, 2000). On August 10, 2000, the Commission issued a Notice announcing public hearings on September 13, 2000 in New York and September 20, 2000 in Washington, DC (65 FR 49954 8/16/2000). The original submission date for materials was September 5, 2000. The new submission date for those testifying on September 20, 2000 is September 12, 2000.

DATES: Written submissions for the September 20, 2000 hearing are due on September 12, 2000.

ADDRESSES: Oral statements or summaries of testimony, and other written testimony or comments, should be mailed to Jonathan G. Katz, Secretary, Securities and Exchange Commission, 450 Fifth Street, NW., Washington, DC 20459–0609 or filed electronically at the following e-mail address: rule-comments@sec.gov. All oral statements or summaries of testimony, and other written testimony or comments, should refer to Comment File No. S7–13–00. Electronic submissions should include ''Comment File No. S7–13–00'' and ''Testimony'' in the subject line. Copies of all requests and other submissions and transcripts of the hearings will be available for public inspection and copying in the Commission's Public Reference Room at 450 Fifth Street, NW., Washington, DC 20549. Electronically submitted requests and other materials will be posted on the Commission's internet web site (www.sec.gov) following the hearings.

The hearing on September 13 will be held at Pace Downtown Theatre at Pace University, Spruce Street between Park Row and Gold Street, New York, New York (across from City Hall Park). The hearing on September 20 will be held in the William O. Douglas Room at the Commission's headquarters at 450 Fifth Street, NW., Washington, DC 20549.

FOR FURTHER INFORMATION CONTACT: John M. Morrissey, Deputy Chief Accountant, Office of the Chief Accountant, at (202) 942–4400.

Dated: August 29, 2000.