Office of Thrift Supervision
Department of the Treasury *Managing Director, Examinations, Supervision, and Consumer Protection*
1700 G Street, N.W., Washington, DC 20552 • (202) 906-7984

December 14, 2005

MEMORANDUM FOR: CHIEF EXECUTIVE OFFICERS

FROM: Scott M. Albinson

SUBJECT: Compliance Guide
Interagency Guidelines Establishing Information Security Standards

The Office of Thrift Supervision, together with the other Federal Banking Agencies (Agencies), jointly issued the *Interagency Guidelines Establishing Information Security Standards* (Security Guidelines), formerly known as the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*. The Security Guidelines primarily implement two statutes, Section 501(b) of the Gramm-Leach-Bliley Act, and Section 216 of the Fair and Accurate Credit Transactions Act of 2003.

The Security Guidelines establish standards for administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information, and the proper disposal of customer and consumer information. Under the Security Guidelines, each financial institution must develop and maintain an effective written information security program tailored to the complexity of its operations.

The Agencies are jointly issuing the attached Compliance Guide (Guide) as a resource to assist financial institutions in their efforts to comply with the Security Guidelines. The Guide summarizes a financial institution's obligations to protect customer information and to dispose properly of customer and consumer information. The Guide also has an Appendix, which lists resources that may be helpful in designing an information security program.

If you have questions about the Guide, contact Kathleen M. McNulty, Technology Program Manager, Information Technology Risk Management, at 202-906-6322, or kathleen.mcnulty@ots.treas.gov.

Attachment

Interagency Guidelines Establishing Information Security Standards

Small-Entity Compliance Guide

I. INTRODUCTION

Purpose and Scope of the Guide

This Small-Entity Compliance Guide[1] is intended to help financial institutions[2] comply with the *Interagency Guidelines Establishing Information Security Standards* (Security Guidelines).[3] The guide summarizes the obligations of financial institutions to protect customer information and illustrates how certain provisions of the Security Guidelines apply to specific situations. The appendix lists resources that may be helpful in assessing risks and designing and implementing information security programs.

Although this guide was designed to help financial institutions identify and comply with the requirements of the Security Guidelines, it is not a substitute for the Security Guidelines. Moreover, this guide only addresses obligations of financial institutions under the Security Guidelines and does not address the applicability of any other federal or state laws or regulations that may pertain to policies or practices for protecting customer records and information.

Background and Overview of Security Guidelines

The Security Guidelines implement section 501(b) of the Gramm-Leach-Bliley Act (GLB Act)[4] and section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).[5] The Security Guidelines establish standards relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and the proper disposal of customer information.

---

[1] The guide is issued in accordance with the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, 110 Stat. 857, *reprinted in* 5 U.S.C.A. § 601, note (West Supp. 2004).

[2] This guide applies to the following types of financial institutions: National banks, Federal branches and Federal agencies of foreign banks and any subsidiaries of these entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OCC); member banks (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, Edge and Agreement Act Corporations, bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (Board); state non-member banks, insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (FDIC); and insured savings associations and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OTS).

[3] 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS). Citations to the Security Guidelines in this guide omit references to part numbers and give only the appropriate paragraph number.

[4] 15 U.S.C. § 6801.

[5] 15 U.S.C. § 1681w.

Each of the requirements in the Security Guidelines regarding the proper disposal of customer information also apply to personal information a financial institution obtains about individuals regardless of whether they are the institution's customers ("consumer information"). Consumer information includes, for example, a credit report about: (1) an individual who applies for but does not obtain a loan; (2) an individual who guarantees a loan; (3) an employee; or (4) a prospective employee. A financial institution must require, by contract, its service providers that have access to consumer information to develop appropriate measures for the proper disposal of the information.

Under the Security Guidelines, each financial institution must:

- Develop and maintain an effective information security program tailored to the complexity of its operations, and

- Require, by contract, service providers that have access to its customer information to take appropriate steps to protect the security and confidentiality of this information.

The standards set forth in the Security Guidelines are consistent with the principles the Agencies follow when examining the security programs of financial institutions.[6] Each financial institution must identify and evaluate risks to its customer information, develop a plan to mitigate the risks, implement the plan, test the plan, and update the plan when necessary. If an Agency finds that a financial institution's performance is deficient under the Security Guidelines, the Agency may take action, such as requiring that the institution file a compliance plan.[7]

Distinction between the Security Guidelines and the Privacy Rule

The requirements of the Security Guidelines and the interagency regulations regarding financial privacy (Privacy Rule)[8] both relate to the confidentiality of customer information. However, they differ in the following key respects:

- The Security Guidelines address safeguarding the confidentiality and security of customer information and ensuring the proper disposal of customer information. They are directed toward preventing or responding to foreseeable threats to, or unauthorized access or use of,

---

[6] *See* Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook's Information Security Booklet (the "IS Booklet") *available at* http://www.ffiec.gov/guides.htm.

[7] 12 U.S.C. § 1831p-1. There are a number of other enforcement actions an agency may take. For example, the OTS may initiate an enforcement action for violating 12 C.F.R. § 568.5 based on noncompliance with the Security Guidelines.

[8] Each of the Agencies, as well as the National Credit Union Administration (NCUA), has issued privacy regulations that implement sections 502-509 of the GLB Act; the regulations are comparable to and consistent with one another. *See* 65 Fed. Reg. 35,162 (June 1, 2000) (Board, FDIC, OCC, OTS) and 65 Fed. Reg. 31740 (May 18, 2000) (NCUA) promulgating 12 C.F.R. Parts 40 (OCC), 216 (Board), 332 (FDIC), 573 (OTS), and 716 (NCUA). Citations to the Privacy Rule in this guide omit references to part numbers and give only the appropriate section number.

that information. The Security Guidelines provide that financial institutions must contractually require their affiliated and non-affiliated third party service providers that have access to the financial institution's customer information to protect that information.

– The Privacy Rule limits a financial institution's disclosure of nonpublic personal information to unaffiliated third parties, such as by selling the information to unaffiliated third parties. Subject to certain exceptions, the Privacy Rule prohibits disclosure of a consumer's nonpublic personal information to a nonaffiliated third party unless certain notice requirements are met and the consumer does not elect to prevent, or "opt out of," the disclosure.[9] The Privacy Rule requires that privacy notices provided to customers and consumers describe the financial institution's policies and practices to protect the confidentiality and security of that information. It does not impose any other obligations with respect to safeguarding customers' or consumers' information.

II. IMPORTANT TERMS USED IN THE SECURITY GUIDELINES

Customer Information

The Security Guidelines require financial institutions to safeguard and properly dispose of customer information. Customer information is any record containing nonpublic personal information about an individual who has obtained a financial product or service from the institution that is to be used primarily for personal, family, or household purposes and who has an ongoing relationship with the institution.

Customer Information Systems

Customer information systems means any method used to access, collect, store, use, transmit, protect, or dispose of customer information. ¶ I.C.2 of the Security Guidelines. Customer information systems encompass all the physical facilities and electronic facilities a financial institution uses to access, collect, store, use, transmit, protect, or dispose of customer information. The Security Guidelines apply specifically to customer information systems because customer information will be at risk if one or more of the components of these systems are compromised.

Information Security Program

An *information security program* is the written plan created and implemented by a financial institution to identify and control risks to customer information and customer information systems and to properly dispose of customer information. The plan includes policies and procedures regarding the institution's risk assessment, controls, testing, service-provider oversight, periodic review and updating, and reporting to its board of directors.

---

[9] The Privacy Rule defines a "consumer" to mean an individual who obtains or has obtained a financial product or service that is to be used primarily for personal, family, or household purposes. For example, an individual who applies to a financial institution for credit for personal purposes is a consumer of a financial service, regardless of whether the credit is extended. Privacy Rule § __.3(e).

Service Providers

Service provider means any party, whether affiliated or not, that is permitted access to a financial institution's customer information through the provision of services directly to the institution. ¶ I.C.2 of the Security Guidelines.

For example, a processor that directly obtains, processes, stores, or transmits customer information on an institution's behalf is its service provider. Similarly, an attorney, accountant, or consultant who performs services for a financial institution and has access to customer information is a service provider for the institution.

III. DEVELOPING AND IMPLEMENTING AN INFORMATION SECURITY PROGRAM

Paragraphs II.A-B of the Security Guidelines require financial institutions to implement an information security program that includes administrative, technical, and physical safeguards designed to achieve the following objectives:

- Ensure the security and confidentiality of their customer information;
- Protect against any anticipated threats or hazards to the security or integrity of their customer information;
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
- Ensure the proper disposal of customer information.

To achieve these objectives, an information security program must suit the size and complexity of a financial institution's operations and the nature and scope of its activities.

The various business units or divisions of the institution are not required to create and implement the same policies and procedures. If the business units have different security controls, the institution must include them in its written information security program and coordinate the implementation of the controls to safeguard and ensure the proper disposal of customer information throughout the institution.

Implementing an information security program begins with conducting an assessment of reasonably foreseeable risks. Like other elements of an information security program, risk assessment procedures, analysis, and results must be written.

Under the Security Guidelines, a risk assessment must include the following four steps:

- Identifying reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

– Assessing the likelihood and potential damage of identified threats, taking into consideration the sensitivity of the customer information;

– Assessing the sufficiency of the policies, procedures, customer information systems, and other arrangements in place to control the identified risks; and

– Applying each of the foregoing steps in connection with the disposal of customer information.

Identifying Reasonably Foreseeable Internal and External Threats

A risk assessment must be sufficient in scope to identify the reasonably foreseeable threats from within and outside a financial institution's operations that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems, as well as the reasonably foreseeable threats due to the disposal of customer information. The scale and complexity of its operations and the scope and nature of an institution's activities will affect the nature of the threats an institution will face.

For example, a financial institution should review the structure of its computer network to determine how its computers are accessible from outside the institution. If the computer systems are connected to the Internet or any outside party, an institution's assessment should address the reasonably foreseeable threats posed by that connectivity.

The risk assessment also should address the reasonably foreseeable risks to:

– Customer information stored on systems owned or managed by service providers, and

– Customer information disposed of by the institution's service providers.

Assessing the Likelihood and Potential Damage of Identified Threats

In addition to identifying reasonably foreseeable threats to customer information, customer information systems, and customer information that a financial institution disposes of, a risk assessment must evaluate the potential damage from these threats. The Security Guidelines allow latitude to determine the sensitivity of customer information in the course of assessing the likelihood of and potential damage from the identified threats.

For example, to determine the sensitivity of customer information, an institution could develop a framework that analyzes the relative value of this information to its customers based on whether improper access to or loss of the information would result in harm or inconvenience to them.

In the course of assessing the potential threats identified, an institution should consider its ability to identify unauthorized changes to customer records. In addition, it should take into consideration its ability to reconstruct the records from duplicate records or backup information systems.

Assessing the Sufficiency of Policies and Procedures

Evaluating the sufficiency of policies and procedures is a key element of a financial institution's risk assessment. The evaluation process includes identifying weaknesses or other deficiencies in existing security controls and assessing the extent to which customer information and customer information systems are at risk as a result of those weaknesses. It should also identify the extent to which customer information is at risk as a result of improper methods of disposal.

The risk assessment may include an automated analysis of the vulnerability of certain customer information systems. However, an automated analysis likely will not address manual processes and controls, detection of and response to intrusions into information systems, physical security, employee training, and other key controls. Accordingly, an automated analysis of vulnerabilities should be only one tool used in conducting a risk assessment.

When performing a risk assessment, an institution may want to consult the resources and standards listed in the appendix to this guide and consider incorporating the practices developed by the listed organizations when developing its information security program.[10]

Hiring an Outside Consultant to Conduct the Risk Assessment

A financial institution may decide to hire an outside consultant to conduct the risk assessment of its information security program, but it nevertheless remains responsible for the adequacy of the assessment. Therefore, the institution must ensure that the assessment specifically examines the risks that relate to *its* customer information, customer information systems, and systems for disposal of customer information.

For example, a generic assessment that describes vulnerabilities commonly associated with the various systems and applications used by the institution is inadequate. The assessment should take into account the particular configuration of the institution's systems and the nature of its business.

If an outside consultant only examines a subset of the institution's risks, such as risks to computer systems, that is insufficient to meet the requirement of the Security Guidelines. The institution will need to supplement the outside consultant's assessment by examining other risks, such as risks to customer records maintained in paper form.

For example, a financial institution should also evaluate the physical controls put into place, such as the security of customer information in cabinets and vaults.

Management must review the risk assessment and use that assessment as an integral component of its information security program to guide the development of, or adjustments to, the institution's information security program.

Engaging in an Ongoing Risk Assessment Process

[10] Financial institutions also may want to consult the Agencies' guidance regarding risk assessments described in the IS Booklet.

Risk assessment is an ongoing process. Financial institutions should continually review their current policies and procedures to make certain they are adequate to safeguard customer information and customer information systems. The review of policies and procedures should also ensure the proper disposal of customer information. Financial institutions should also include their review and findings in their written information security program. The institution must also update the risk assessment, as necessary, to account for system changes before they are implemented, or new products or services before they are offered.

IV. DESIGNING SECURITY CONTROLS

The Security Guidelines require a financial institution to design an information security program to control the risks identified through its assessment, commensurate with the sensitivity of the information and the complexity and scope of its activities. Thus, an institution must consider a variety of policies, procedures, and technical controls and adopt those measures that it determines appropriately address the identified risks.

The Security Guidelines provide a list of measures that an institution must consider and, if appropriate, adopt. These are:

- 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;

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

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

- Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program;

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

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

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

– 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. ¶ III.C.1.a-h of the Security Guidelines.

For example, the Security Guidelines require a financial institution to consider whether it should adopt controls to authenticate and permit only authorized individuals access to certain forms of customer information. ¶ III.C.1.a of the Security Guidelines. Under this security control, a financial institution also should consider the need for a firewall for electronic records. If an institution maintains any sort of Internet or other external connectivity, its systems may require multiple firewalls with adequate capacity, proper placement, and appropriate configurations.

Similarly, an institution must consider whether the risk assessment warrants encryption of electronic customer information. If it does, the institution must adopt appropriate encryption measures that protect information in transit, in storage, or both. ¶ III.C.1.c of the Security Guidelines. However, the Security Guidelines do not impose any specific authentication[11] or encryption standards.[12]

A financial institution must consider the use of an intrusion detection system to alert it to attacks on computer systems that store customer information. ¶ III.C.1.f. of the Security Guidelines. In assessing the need for such a system, an institution should evaluate the ability of its staff to rapidly and accurately identify an intrusion. It should also assess the damage that could occur between the time an intrusion occurs and the time the intrusion is recognized and action is taken.

Financial institutions must develop, implement, and maintain appropriate measures to properly dispose of customer information in accordance with each of the requirements of paragraph III. ¶ III.C.4. of the Security Guidelines. Although the Security Guidelines do not prescribe a specific method of disposal, the Agencies expect institutions to have appropriate risk-based disposal procedures for their records.

An institution should:

– Ensure that paper records containing customer information are rendered unreadable as indicated by its risk assessment, such as by shredding or any other means; and

– Recognize that computer-based records present unique disposal problems. Residual data frequently remains on media after erasure. Since that data can be recovered, additional disposal techniques should be applied to sensitive electronic data.

---

[11] On December 14, 2004, the FDIC published a study, *Putting an End to Account-Hijacking Identity Theft*, which discusses the use of authentication technologies to mitigate the risk of identity theft and account takeover. FDIC Financial Institution Letter (FIL) 132-2004. Additional discussion of authentication technologies is included in the FDIC's June 17, 2005, Study Supplement. FIL 59-2005.

[12] The Agencies have issued guidance about authentication, through the FFIEC, entitled "Authentication in an Internet Banking Environment" (Oct. 12, 2005) *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf. Additional information about encryption is in the IS Booklet.

In addition to considering the measures required by the Security Guidelines, each institution may need to implement additional procedures or controls specific to the nature of its operations. An institution may implement safeguards designed to provide the same level of protection to all customer information, provided that the level is appropriate for the most sensitive classes of information.

Insurance coverage is not a substitute for an information security program. Although insurance may protect an institution or its customers against certain losses associated with unauthorized disclosure, misuse, alteration, or destruction of customer information, the Security Guidelines require a financial institution to implement and maintain controls designed to prevent those acts from occurring.

Develop and Implement A Response Program

The Agencies have issued an interpretation of the Security Guidelines regarding programs to respond to unauthorized access to customer information, the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (Incident Response Guidance).[13] According to the Incident Response Guidance a financial institution should develop and implement a response program as part of its information security program. The response program should address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

The components of an effective response program include:

- Assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused;

- Prompt notification to its primary federal regulator once the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;

- Notification to appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report, in situations involving Federal criminal violations requiring immediate attention;

- Measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence; and

- Notification to customers when warranted.

[13] 70 Fed. Reg. 15736 (Mar. 29, 2005) promulgating 12 C.F.R. Part 30, app. B, Supplement A (OCC); 12 C.F.R. Part 208, app. D-2, Supplement A and Part 225, app. F, Supplement A (Board); 12 C.F.R. Part 364, app. B, Supplement A (FDIC); and 12 C.F.R. Part 570, app. B, Supplement A (OTS).

Circumstances for Customer Notice

The Incident Response Guidance describes when and how a financial institution should provide notice to customers affected by unauthorized access or misuse of sensitive customer information. In particular, it indicates that:

– Once the institution becomes aware of an incident of unauthorized access to sensitive customer information, it should conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused.

– If the institution determines that misuse of customer information has occurred or is reasonably possible, it should notify any affected customer as soon as possible.[14]

Sensitive customer information means:

– A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account; or

– Any combination of components of customer information that would allow an unauthorized third party to access the customer's account electronically, such as user name and password or password and account number.

V. TRAINING STAFF

The Security Guidelines require a financial institution to train staff to prepare and implement its information security program. ¶ III.C.2 of the Security Guidelines. The institution should consider providing specialized training to ensure that personnel sufficiently protect customer information in accordance with its information security program.

For example, an institution should:

– Train staff to recognize and respond to schemes to commit fraud or identity theft, such as guarding against pretext calling;[15]

[14] The Incident Response Guidance recognizes that customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

[15] *See* "Identity Theft and Pretext Calling," FRB Sup. Ltr. SR 01-11 (April 26,2001) (Board); OCC Advisory Ltr. 2001-4 (April 30, 2001) (OCC); CEO Ltr. 139 (May 4, 2001) (OTS); FIL 39-2001 (May 9, 2001) (FDIC).

- Provide staff members responsible for building or maintaining computer systems and local and wide-area networks with adequate training, including instruction about computer security; and

- Train staff to properly dispose of customer information.

VI. TESTING KEY CONTROLS

The Security Guidelines require a financial institution to test the key controls, systems, and procedures of its information security program. ¶ III.C.3 of the Security Guidelines. The institution's risk assessment should determine the scope, sequence, and frequency of testing.

The Agencies expect an institution or its consultant to regularly test key controls at a frequency that takes into account the rapid evolution of threats to computer security. Testing may vary over time depending, in part, on the adequacy of any improvements an institution implements to prevent access after detecting an intrusion. Independent third parties or staff members, other than those who develop or maintain the institution's security programs, must perform or review the testing.

VII. OVERSEEING SERVICE PROVIDERS

The Security Guidelines set forth specific requirements that apply to a financial institution's arrangements with service providers. An institution must:

- Exercise appropriate due diligence in selecting its service providers;

- Require its service providers by contract to implement appropriate measures designed to meet the objectives of the Security Guidelines; and

- Where indicated by its risk assessment, monitor its service providers to confirm that they have satisfied their obligations under the contract described above.

As stated in section II of this guide, a service provider is *any* party that is permitted access to a financial institution's customer information through the provision of services directly to the institution. Examples of service providers include a person or corporation that tests computer systems or processes customers' transactions on the institution's behalf, document-shredding firms, transactional Internet banking service providers, and computer network management firms.

Contracts With Service Providers

The contract provisions in the Security Guidelines apply to *all* of a financial institution's service providers. After exercising due diligence in selecting a company, the institution must enter into and enforce a contract with the company that requires it to implement appropriate measures designed to implement the *objectives* of the Security Guidelines.[16]

In particular, financial institutions must require their service providers by contract to

– Implement appropriate measures designed to protect against unauthorized access to or use of customer information maintained by the service provider that could result in substantial harm or inconvenience to any customer; and

– Properly dispose of customer information.

In addition, the Incident Response Guidance states that an institution's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution's customer information, including notification to the institution as soon as possible following any such incident.

Monitoring Service Providers

A financial institution must monitor each of its service providers in accordance with its risk assessment. However, the Security Guidelines do not impose any specific requirements regarding the methods or frequency of monitoring service providers to ensure that they are fulfilling their contractual obligations. Some service providers are financial institutions that are subject to the Security Guidelines, or to other standards for safeguarding information promulgated by their primary regulator, and therefore may have implemented their own information security programs.

To the extent that monitoring is warranted, a financial institution must confirm that the service provider is fulfilling its obligations under its contract. Institutions may review audits, summaries of test results, or equivalent evaluations of a service provider's work. These audits, tests, or evaluations should be conducted by a qualified party independent of management and personnel responsible for the development or maintenance of the service provider's security program.

The reports of test results may contain proprietary information about the service provider's systems or they may include non-public personal information about customers of another financial institution. Under certain circumstances it may be appropriate for service providers to redact confidential and sensitive information from audit reports or test results before giving the

[16] The third-party-contract requirements in the Privacy Rule are more limited than those in the Security Guidelines. When a financial institution relies on the "opt out" exception for service providers and joint marketing described in § __.13 of the Privacy Rule (as opposed to other exceptions), in order to disclose nonpublic personal information about a consumer to a nonaffiliated third party without first providing the consumer with an opportunity to opt out of that disclosure, it must enter into a contract with that third party. The contract must generally prohibit the nonaffiliated third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed.

institution a copy. Where this is the case, an institution should make sure that the information is sufficient for it to conduct an accurate review, that all material deficiencies have been or are being corrected, and that the reports or test results are timely and relevant.

The institution should include reviews of its service providers in its written information security program.

VIII. ADJUSTING THE PROGRAM

A financial institution should adjust its information security program to reflect the results of its ongoing risk assessment and the key controls necessary to safeguard customer information and ensure the proper disposal of customer information. It should adjust the program to take into account changes in technology, the sensitivity of its customer information, internal or external threats to information, and the institution's own changing business arrangement such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in customer information systems.

For example, the institution should ensure that its policies and procedures regarding the disposal of customer information are adequate if it decides to close or relocate offices. A change in business arrangements may involve disposal of a larger volume of records than in the normal course of business.

IX. RESPONSIBILITIES OF AND REPORTS TO THE BOARD OF DIRECTORS

Under the Security Guidelines, a financial institution's board of directors, or an appropriate committee of the board, must satisfy specific requirements designed to ensure that the institution's information security program is developed, implemented, and maintained under the supervision of those who are ultimately responsible. At the outset, the board, or appropriate committee, must approve the written information security program. Thereafter, the board or appropriate committee must oversee the implementation and maintenance of the program. These duties include assigning specific responsibility for implementing the program and reviewing management reports. ¶ III.A of the Security Guidelines.

Correspondingly, management must provide a report to the board, or an appropriate committee, at least annually that describes the overall status of the information security program and compliance with the Security Guidelines. The report should describe material matters relating to the program.

For example, whether an institution conducts its own risk assessment or hires another person to conduct it, management should report the results of that assessment to the board or an appropriate committee.

The Security Guidelines provide an illustrative list of other material matters that may be appropriate to include in the report, such as decisions about risk management and control, arrangements with service providers, results of testing, security breaches or violations and

management's responses, and recommendations for changes in an information security program. ¶ III.F of the Security Guidelines.

APPENDIX

Note: This list of resources is intended to further assist financial institutions in complying with the *Interagency Guidelines Establishing Information Security Standards*. The listed organizations provide information on computer security, with a focus on risk-assessment methodologies and the design and implementation of computer security programs. Any mention of a commercial product is for information purposes only and does not imply a recommendation or endorsement by the Agencies.

Center for Internet Security (CIS) – A nonprofit cooperative enterprise that helps organizations reduce the risk of business and e-commerce disruptions resulting from inadequate security configurations. CIS develops security benchmarks through a global consensus process. Its members include the American Institute of Certified Public Accountants (AICPA), Financial Management Service of the U.S. Department of the Treasury, and Institute for Security Technology Studies (Dartmouth College). www.cisecurity.org

CERT Coordination Center – A center for Internet security expertise operated by Carnegie Mellon University. CERT provides security-incident reports, vulnerability reports, security-evaluation tools, security modules, and information on business continuity planning, intrusion detection, and network security. It also offers training programs at Carnegie Mellon. CERT has developed an approach for self-directed evaluations of information security risk called Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). www.cert.org/octave/

Information Systems Audit and Control Association (ISACA) – An association that develops IT auditing and control standards and administers the Certified Information Systems Auditor (CISA) designation. ISACA developed Control Objectives for Information and Related Technology (COBIT) as a standard for IT security and control practices that provides a reference framework for management, users, and IT audit, control, and security practitioners. www.isaca.org/cobit.htm

International Organization for Standardization (ISO) – A network of national standards institutes from 140 countries. Published *ISO/IEC 17799:2000, Code of Practice for Information Security Management*. www.iso.org. Interested parties should also review the *Common Criteria for Information Technology Security Evaluation*. http://niap.nist.gov/cc-scheme/index.html

Internet Security Alliance (ISA) – A collaborative effort between Carnegie Mellon University's Software Engineering Institute, the university's CERT Coordination Center, and the Electronic Industries Alliance (a federation of trade associations). ISA provides access to information on threats and vulnerability, industry best practices, and developments in Internet security policy. www.isalliance.org

Institute for Security Technology Studies (Dartmouth College) – An institute that studies and develops technologies to be used in counter-terrorism efforts, especially in the areas of threat characterization and intelligence gathering, threat detection and interdiction, preparedness and protection, response, and recovery. The institute publishes a daily news summary titled *Security in the News*, offers on-line training courses, and publishes papers on such topics as firewalls and virus scanning. The web site includes worm-detection tools and analyses of system vulnerabilities. www.ists.dartmouth.edu

National Institute of Standards and Technology (NIST) – An agency within the U.S. Commerce Department's Technology Administration that develops and promotes measurements, standards, and technology to enhance productivity. NIST operates the Computer Security Resource Center, which is dedicated to improving information systems security by raising awareness of IT risks, researching vulnerabilities, and developing standards and tests to validate IT security. Four particularly helpful documents are: *Special Publication 800-14,Generally Accepted Principles and Practices for Securing Information Technology Systems; Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems; Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems; Special Publication 800-30, Risk Management Guide for Information Technology Systems;* and *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems*. http://csrc.nist.gov. The web site provides links to a large number of academic, professional, and government sponsored web sites that provide additional information on computer or system security.

National Security Agency (NSA) – The National Security Agency/Central Security Service is America's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. A high technology organization, NSA is on the frontiers of communications and data processing. The web site includes links to NSA research on various information security topics. www.nsa.gov