SUPPORTING STATEMENT
Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
(OMB Control No. 1550-0110)

A. JUSTIFICATION

1. Circumstances and Need

On March 29, 2005, the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), and Office of Thrift Supervision (OTS) (collectively, the Agencies) published the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (70 FR 15736) (Guidance). The Guidance interprets the requirements of section 501(b) of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801, and the Interagency Guidelines Establishing Information Security Standards (Security Guidelines)[1] to include the development and implementation of a response program to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The Guidance states that every financial institution should develop and implement a response program designed to address incidents of unauthorized access to customer information maintained by the institution or its service provider, and describes the appropriate elements of a financial institution's response program, including customer notification procedures. OTS is now seeking OMB's approval to renew this collection of information.

2. Use of the Information Collected

The collection helps to establish standards for financial institutions 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 that could result in substantial harm or inconvenience to any customer.

A response program, of which this collection is a critical part, contains policies and procedures that enable the financial institution to: (a) assess the situation to determine the nature and scope of the incident, and identify the information systems and types of customer information affected; (b) notify the institution's primary Federal regulator and, in accordance with applicable regulations and guidance, file a Suspicious Activity Report and notify appropriate law enforcement agencies; (c) take measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls; and (d) address and mitigate harm to individual customers.

[1] 12 CFR part 570, app. B (OTS).

3. Use of Technology to Reduce Burden

OTS permits and encourages savings associations to use advanced technology in the preparation of the required information.

4. Effort to Identify Duplication

The information collection is not duplicative within the meaning of the PRA and OMB regulations. The collection is unique and covers each institution's particular circumstances.

5. Minimizing the Burden on Small Entities

The collection applies to all institutions, regardless of size.

6. Consequences of Less Frequent Collections

OTS believes that less frequent collection (a less stringent disclosure standard) would result in unacceptable harm to customers of financial institutions.

7. Special Circumstances

These information collections are conducted in a manner consistent with the requirements of 5 CFR 1320.

8. Consultation with Persons Outside the Agency

Notice of intent to renew this information collection was published in the *Federal Register* on December 18, 2006 (71 FR 75812). OTS received no comments.

9. Payment or Gift to Respondents

No payments or gifts are made in connection with this information collection.

10. Confidentiality

Financial institutions would treat these disclosure requirements with the same degree of confidentiality as other disclosures of sensitive customer information.

11. Information of a Sensitive Nature

The disclosure of this information would be limited to account holders.

12. Estimate of Annual Burden

It is estimated that it will initially take institutions 24 hours (three business days) to develop and produce the notices described in the Guidance and 29 hours per incident to determine which customers should receive the notice and notify the customers. For the purposes of this analysis, 113 was used as the number of incidents of unauthorized access requiring customer notice under the Guidance. This is the actual number experienced by covered institutions in 2006.

Thus, the burden associated for this collection of information may be summarized as follows:

Developing Notices: 24 hours x 840 = 20,160 hours

Notifying Customers: 29 hours x 113 = 3,277 hours

Total Estimated Annual Burden = 23,437 hours

Estimate of annualized cost: 23,437 hours x $50/hour = $1,171,850.

13. Total Annual Cost Burden

Not applicable.

14. Annualized Cost to the Federal Government

Negligible.

15. Reason for Program Changes or Adjustments

There is an overall increase of 1,882 hours of total burden. This occurred because, although there is a decrease in the number of respondents (from 880 to 840), where OTS initially estimated the number of covered institutions that experienced an incident of unauthorized access to customer information resulting in customer notification by using two percent of the total number of covered institutions, OTS is now using the actual number of such institutions for 2006, thus reflecting a net increase in the burden for notifying customers.

16. Publication

Not applicable.

17. Display of Expiration Date

Not applicable.

18. Exceptions to Certification

None.

B. STATISTICAL METHODS

Not applicable.