

Supporting Statement
National Credit Union Administration

Security Program, 12 CFR 748
OMB No. 3133-0033

A. Justification

1. Circumstances that make the collection necessary:

This collection is a notice requirement derived from a rule requiring federally insured credit unions to design their security programs to:

- protect each credit union from robberies, burglaries, larcenies, and embezzlement,
- safeguard member information,
- respond to incidents of unauthorized access to member information,
- assist in the identification of commit or attempt to commit such actions and crimes, and;
- prevent destruction of vital records as defined in 12 CFR part 749.

The rule sets forth the minimum requirements of a security program. It further addresses member notification, filing with the Financial Crimes Enforcement Network (FinCEN), and monitoring Bank Secrecy Act (BSA) compliance.

The rule is accompanied by guidance, in the form of appendices A and B. Appendix A describes NCUA's expectations for credit unions to safeguard member information. Appendix B describes NCUA's expectations for credit union response programs to incidents of unauthorized access to member information. Both Appendix A & B closely follows similar guidance published by the other federal banking agencies (Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency).

In accordance with Title V of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§6801 et seq., federally-insured credit unions are required to implement information security programs designed to protect member information as described in Appendix A. Appendix B describes the components of a response program and establishes a standard for providing notice to members affected by unauthorized access to or use of member information that could result in substantial harm or inconvenience to those members, thereby reducing the risk of losses due to fraud or identity theft.

The Appendix B guidance describes NCUA's expectation that "a credit union should notify affected members when it becomes aware of unauthorized access to sensitive member information unless the credit union, after an appropriate investigation, reasonably concludes that misuse is unlikely to occur and takes appropriate steps to safeguard the interests of affected members, including monitoring affected members' accounts for unusual or suspicious activity." This third party disclosure is considered a collection of information under the Paperwork Reduction Act.

2. Use of the information:

The collection helps federally insured credit unions to develop and implement administrative, technical, and physical safeguards to: (1) insure the security and confidentiality of member 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 member.

A response program, which this collection is a critical part, contains policies and procedures that enable the credit unions to: (A) assess the situation to determine the nature and scope of the incident, and identify the information systems and types of member information affected; (B) notify the credit union'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 member 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 members.

3. Consideration of the use of improved information technology:

Annual certification conducted through NCUA's online information management system (OMB No. 3133-0004) and suspicious activity reporting through FinCEN's web-based BSA E-Filing website (OMB No. 1506-0065) are cleared under separate OMB numbers.

4. Efforts to identify duplication:

The information collection is unique to federally-insured credit unions and is not duplicated elsewhere.

5. Methods used to minimize burden if the collection has a significant impact on substantial number of small entities:

The guidelines implementing the provisions of the GLBA applies to all financial institutions. The response program guidance provides each credit union with flexibility to design a risk-based response program tailored to the size, complexity, and nature of its operations.

6. Consequences to the Federal program if the collections were conducted less frequently:

NCUA believes that less frequent collection (i.e., a less comprehensive security program with diminished expectations as to the member response elements) would result in harm to credit union members.

7. Special circumstances necessitating collection inconsistent with 5 CFR §1320.5(d)(2):

The collection of information is conducted in a manner consistent with the requirements of 5 CFR 1320.5(d)(2)

8. Efforts to consult with persons outside the agency:

A 60-day notice was published in the *Federal Register* on August 16, 2016, at 81 FR 54608, soliciting comments from the public and no comments were received.

9. Payment to respondents:

There are no payments or gift provided to respondents.

10. Any assurance of confidentiality:

Federally-insured credit unions, like all other regulated financial institutions, are required to preserve and maintain the confidentiality of member financial information. All collected information associated with this rule would be treated with the same degree of confidentiality as other disclosures of sensitive member information.

11. Justification for questions of a sensitive nature:

No personally identifiable information (PII) is collected.

12. Burden estimate:

As of December 31, 2015, there were 6,021 FICUs. NCUA estimates 4 new FICUs will be chartered in 2016 based upon 2015 new charters. For the renewal of this collection, NCUA estimates it will take a newly chartered federally-insured credit union 20 hours (2.5 business days) to produce their initial policies and incident notices described in the rule and 24 hours per incident (three business days) to determine which members should receive the notice and to notify the members. For this analysis, it is estimated that two percent of federally-insured credit unions will experience an incident of unauthorized access to member information on an annual basis, resulting in member notification.

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

12 CFR Part 748	Information Collection	# Respondents	# Responses Per Respondent	Annual Responses	Hours Per Response	Total Annual Burden
§748.0 (Apx. A.II.A and Apx. II.i)	Developing Programs: (1) Information Security and (2) risk-based response program (recordkeeping)	4	1	4	20	80
A.III.F	On-going Program Maintenance (recordkeeping)	6,201	1	6,021	2	12,042
§748.1(a)	Certify Compliance (reporting)	OMB No. 3133-0004				
§748.1(b)	Report Catastrophic Act (reporting)	30	1	30	1	30
§748.1(c)	Suspicious Activity Report (reporting)	OMB Nos. 3133-0098, 1506-0065				
§748.1(2)	Monitoring BSA Compliance (recordkeeping)	OMB No. 3133-0108				
	Notifying NCUA of incident (reporting)	121	1	121	2	242
Apx.B.III.	Notifying Members of incident (disclosure)	121	1	121	24	2,904
TOTALS		6,201	1.02	6,297	2.43	15,298

The total cost to respondent is based on a \$35 hourly wage rate for a total of \$535,430.

13. Estimates of capital start-up and maintenance costs

There are no capital start-up costs and maintenance costs are included in Question 12.

14. Estimates of annualized cost to the Federal Government:

There are no cost to the federal government.

15. Changes in burden:

Adjustments reflect a reduction in burden due to (1) a decrease in the number of respondents due to the decline in the number of federally-insured credit unions since the previous submission (2) and an effort to identify the information collection requirements of this part in greater detail.

16. Information regarding collections whose results are planned to be published for statistical use:

There are no plans to publish results.

17. Display of expiration date:

The OMB control number and expiration date associated with the PRA submission will be displayed on the Federal government's electronic PRA docket at www.reginfo.gov.

18. Exceptions to certification statement:

There are no exceptions to the certification statement.

B. Collections of Information Employing Statistical Methods.

This collection does not employ statistical methods.