National Credit Union Administration
SUPPORTING STATEMENT

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

Summary of Action:
A notice of proposed rulemaking was published July 27, 2022, on 87 FR 45029, to address the increased frequency and severity of cyberattacks on the financial services sector. The NCUA Board is proposing to require a federally insured credit union (FICU's) that experiences a reportable cyber incident to report the incident to the NCUA as soon as possible and no later than 72 hours after the federally insured credit union reasonably believes that it has experienced a reportable cyber incident. The cyber incident reporting requirement will help promote early awareness of emerging threats to FICUs and the broader financial system. This early awareness will help the NCUA react to these threats before they become systemic. This reporting requirement is intended to serve as an early alert to the agency and is not intended to include a lengthy assessment of the incident. The agency will require only certain basic information, to the extent it is known to the FICU at the time of reporting.

The proposed rule adds a cyber incident reporting under 748.1(c) where FICUs would be required to report these incidents, as defined. The burden associated with the reporting requirements identified under Appendix B will be removed because most reporting will now fall under the new cyber incident requirement.

A. JUSTIFICATION

1. Circumstances that make the collection of information 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. Purpose and use of the information collection.

The information collection helps federally insured credit unions (FICUs) 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. Use of 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. **Duplication of information.**

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

5. Efforts to reduce burden on 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 of not conducting the collection.

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. Inconsistent with guidelines in 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 Paperwork Reduction Act (PRA) notice was published in the preamble of the proposed rulemaking on July 27, 2022, at 87 FR 45029, providing an opportunity for the public to comment on the information collection requirements prescribed by this rule. Comments will be summarized and addressed in the PRA submission associated with the final rulemaking.

9. Payment or gifts to respondents.

There are no payments or gift provided to respondents.

10. 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. Questions of a sensitive nature.

No personally identifiable information (PII) is collected.

12. Burden of information collection.

The proposed rule would require FICUs to notify the appropriate NCUA-designated point of contact of the occurrence of a reportable cyber incident via email, telephone, or other similar methods that the NCUA may prescribe. The information collection requirements associated with 12 CFR part 748 are cleared under OMB control number 3133-0033 and provide for catastrophic act reporting and GLBA incident reporting guidance under Appendix B to part 748. The proposed rule adds a cyber incident reporting under § 748.1(c) where FICUs would be required to report these incidents, as defined. The burden associated with the reporting requirements identified under Appendix B will be removed because most reporting will now fall under the new cyber incident requirement. The NCUA estimates a one-hour annual reporting burden on each FICU, for a total of 4,903 hours.

Adjustment will also be made to the information collection requirements under part 748 to reflect a reduction in the current number of FICUs and to provide for a more accurate response rate per respondent.

	12 CFR	TASK	Information Collection Activity	Type of Burden	# Respondents	# Responses per Respondent	# Annual Response	Hours per Response	Total Annual Burden	Previous Burden	Adjustment	Program	Total Change
1	748.0(a) and Appx. B., Para II.i	Information Security Program	Each FICU will develop a written security program within 90 days of the effective date of insurance.	Record keeping	4,903	12	58,836	1	58,836	63,696	-4,860	0	-4,860
		Risk-based response program	Every CU should also develop and implement a risk-based response program to address incidents of unauthorized access to member information in member information systems that occur, nonetheless.	Record keeping	4,903	1	4,903	4	19,612	21,232	-1,620	0	-1,620
2	Appx. B. Para. III.F	Status Report to the Board	Each CU should report to its board at least annually on its overall status of the information security program and the CU's compliance with these guidelines.	Record keeping	4,903	4	19,612	2	39,224	42,464	-3,240	0	-3,240
3	748.1(a)	Certify Compliance	The president or managing official of each FICU must certify compliance with the requirements of this part in its CU Profile annually through NCUA's online information management system.	**Covered in OMB Nos. 3133-0004**									
4	748.1(b)	Catastrophic act report	Each FICU will notify the regional director within 5 business days of any catastrophic act that occurs at its office(s).	Reporting	150	1	150	1	150	63,696	-63,546	0	-63,546
5	748.1(c)	Cyber Incident Report	Each FICU must notify NCUA of the occurrence of a reportable cyber incident via email, telephone, or other similar methods that NCUA may prescribe. NCUA must receive this notification as soon as possible and no later than 72 hours after a FICU determines or reasonably should determine that it has experienced a reportable cyber incident.	Reporting	4,903	1	4,903	1	4,903	0	0	4,903	4,903
6	748.1(b)	Suspicious Activity Report	A CU must report any unknown or suspected crime or any suspicious transaction related to money laundering or other illegal activity by sending a completed suspicious activity report (SAR) to the Financial Crimes Enforcement Network (FinCEN).	**Covered in OMB No. 1506-0065 - FinCEN reporting**									
7	~~Appx B. II. A. 1. b.~~	~~Notice to NCUA~~	~~Notifying the appropriate NCUA Regional Director as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information.~~	~~Reporting~~	0	0	0	0	0	63,696	-63,696	0	-63,696
8	Appx B. III. A.	Member Notice	CU should notify its members when it becomes aware of an incident of unauthorized access to sensitive member information.	Third-party Disclosure	4,903	1	4,903	24	117,672	127,392	-9,720	0	-9,720
TOTALS					4,903	19.03	93,307	2.576409	240,397	382,176	-146,682	4,903	-141,779
											240,397		

The total cost to respondent is based on a $35 hourly wage rate for a total of $8,413,895.

13. Capital start-up or on-going operation and maintenance costs.

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

14. Annualized costs to Federal government.

There is no cost to the federal government.

15. Changes in burden.

The proposed rule would require FICUs to notify the appropriate NCUA-designated point of contact of the occurrence of a reportable cyber incident via email, telephone, or other similar methods that the NCUA may prescribe. The information collection requirements associated with 12 CFR part 748 are cleared under OMB control number 3133-0033 and provide for catastrophic act reporting and GLBA incident reporting guidance under Appendix B to part 748. The proposed rule adds a cyber incident reporting under § 748.1(c) where FICUs would be required to report these incidents, as defined. The burden associated with the reporting requirements identified under Appendix B will be removed because most reporting will now fall under the new cyber incident requirement. The NCUA estimates a one-hour annual reporting burden on each FICU, for a total of 4,903 hours.

An adjustment is being made to reflect the current number of FICUs and to provide for a more accurate response rate per respondent. A total reduction of 146,682 burden hours is due to this adjustment.

16. Information collection planned for statistical purposes.

The information is not planned for publication.

17. Request non-display the expiration date of the OMB control number.
The OMB control number and expiration date associated with the PRA submission will be displayed on the Federal government's electronic PRA docket website at www.reginfo.gov.

18. Exceptions to Certification for Paperwork Reduction Act Submissions.
There are no exceptions to the certification statement.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

This collection does not employ statistical methods.