Office of the Comptroller of the Currency (OCC)
Supporting Statement
Federal Financial Institutions Examination Council (FFIEC)
Cybersecurity Assessment Tool
OMB Control No. 1557-0328

A. Justification.

1. Circumstances that make the collection necessary:

Cyber threats continue to evolve and increase in frequency and sophistication. Financial institutions[1] are exposed to cyber risks because they are dependent on information technology to deliver services to consumers and businesses every day. Cyberattacks on financial institutions may result in access to, and the compromise of, confidential information, as well as the destruction of critical data and systems. Disruption, degradation, or unauthorized alteration of information and systems can affect a financial institution's operations and core processes and undermine confidence in the nation's financial services sector. Absent immediate attention to these rapidly increasing threats, individual financial institutions and the whole financial sector are at risk.

For this reason, the OCC, the Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation, and the National Credit Union Administration (collectively, the Agencies), under the auspices of the FFIEC, have worked diligently to assess and enhance the state of the financial industry's cyber preparedness and to improve the Agencies' examination procedures and training to strengthen the oversight of financial industry cybersecurity readiness. The Agencies also have focused on providing financial institutions with resources that can assist in protecting them and their customers from the growing risks posed by cyberattacks.

As part of these efforts, the Agencies, with the other FFIEC members, developed the Cybersecurity Assessment Tool (Assessment) to assist financial institutions of all sizes in assessing their inherent cyber risks and their risk management capabilities. The Assessment allows a financial institution to identify its inherent cyber risk profile based on technologies and connection types, delivery channels, online/mobile products and technology services, organizational characteristics, and cyber threats it is likely to face. Once a financial institution identifies its inherent cyber risk profile, it can use the Assessment's maturity matrix to evaluate its level of cybersecurity preparedness based on its cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resiliency planning. A financial institution may use the matrix's maturity levels to identify opportunities for improving its cyber risk management based on its inherent risk profile. The Assessment also enables a financial institution to rapidly identify areas that could improve the financial institution's cyber response programs, as appropriate. Use of the Assessment by financial institutions is voluntary.

---

[1] For purposes of this information collection, the term "financial institution" includes banks, savings associations, credit unions, and bank holding companies.

2. Use of the information:

The Assessment may be used by financial institutions to assist in evaluating and managing their inherent risk and cybersecurity preparedness. Financial institutions, particularly smaller institutions, have requested this assistance. The Assessment facilitates the ability of financial institutions to address their cybersecurity preparedness on an ongoing basis, as cyber threats evolve, and as they introduce new products and services and employ new technologies.

3. Consideration of the use of improved information technology:

The collection is available electronically. Any improved information technology may be used to complete the assessment.

4. Efforts to identify duplication:

The information is unique and is not duplicative of any other information already collected.

5. If the collection of information impacts small businesses or other small entities, describe any methods used to minimize burden:

Financial institutions of all sizes, including small institutions, may use the Assessment to evaluate and manage their inherent risk and cybersecurity preparedness. The Assessment takes into account an individual institution's risk and complexity. Further, use of the Assessment by financial institutions is voluntary.

To assist financial institutions in using the Assessment efficiently, the Agencies developed a User's Guide that explains how to complete the Assessment and a Glossary to provide easy access to the definitions of terms contained in the Assessment. The Agencies also have included an appendix to the Assessment that maps the baseline maturity level statements contained in the Assessment to the risk management and control standards outlined in the FFIEC Information Technology Examination Handbook. The Agencies also issued responses to frequently asked questions and an "Overview for Chief Executive Officers and Boards of Directors" that provides an executive summary of the Assessment and identifies questions financial institution boards and senior management may ask to facilitate the use of the Assessment by institutions.

The Agencies also updated the Assessment to provide additional response options for each declarative statement. With the additional response options, financial institution management may include supplementary or complementary behaviors, practices, and processes that represent the institution's current practices.

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

The collection is collected at the minimum level of frequency. If the collection were conducted less frequently, disruption, degradation, or unauthorized alteration of information and systems could affect a financial institution's operations and core processes and undermine confidence in the nation's financial services sector. Absent immediate attention to these rapidly increasing threats, financial institutions and the financial sector as a whole would be at risk.

7. Special circumstances that would cause an information collection to be conducted in a manner inconsistent with 5 CFR part 1320:

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

8. Efforts to consult with persons outside the agency:

On May 31, 2022, the OCC, on behalf of the Agencies, published a 60-day notice requesting comment on this collection of information, 87 FR 32497. No comments were received.

9. Payment or gift to respondents:

None.

10. Any assurance of confidentiality:

The information is kept private to the extent permitted by law.

11. Justification for questions of a sensitive nature:

Not applicable. No personally identifiable information is collected.

12. Burden estimate:[2]

Assessment Burden Estimate	*Estimated number of respondents less than $500 million @ 80 hours*	*Estimated number of respondents $500 million - $10 billion @ 120 hours*	*Estimated number of respondents $10 billion - $50 billion @ 160 hours*	*Estimated number of respondents over $50 billion @ 180 hours*	*Estimated total respondents and total annual burden hours*
OCC National Banks and Federal Savings Associations:	656 x 80 = 52,480 hours	376 x 120 = 45,120 hours	37 x 160 = 5,920 hours	29 x 180 = 5,220 hours	1,098 respondents 108,740 hours
FDIC State Non-Member Banks and State Savings Associations:	2,116 x 80 = 169,280 hours	953 x 120 = 114,360 hours	51 x 160 = 8,160 hours	8 x 180 = 1,440 hours	3,128 respondents 293,240 hours
Board State Member Banks and Bank Holding Companies:	2,768 x 80 = 221,440 hours	766 x 120 = 91,920 hours	81 x 160 = 12,960 hours	26 x 180 = 4,680 hours	3,641 respondents 331,000 hours

[2] Burden is estimated conservatively and assumes all institutions will complete the Assessment. Therefore, the estimated burden may exceed the actual burden because use of the Assessment by financial institutions is voluntary. The burden estimates for financial institutions include technology service providers who may assist financial institutions in completing their Assessments.

NCUA Federally-Insured Credit Unions:	4,223 x 80 = 337,840 hours	672 x 120 = 80,640 hours	17 x 160 = 2,720 hours	2 x 180 = 360 hours	4,914 respondents 421,560 hours
Total:					12,781 Respondents 1,154,540 hours

1,154,540 x $119.63 = $138,117,620.20

To estimate wages the OCC reviewed May 2021 data for wages (by industry and occupation) from the U.S. Bureau of Labor Statistics (BLS) for credit intermediation and related activities (NAICS 5220A1). To estimate compensation costs associated with the rule, the OCC uses $119.63 per hour, which is based on the average of the 90th percentile for six occupations adjusted for inflation (6.1 percent as of Q1 2022), plus an additional 32.8 percent for benefits (based on the percent of total compensation allocated to benefits as of Q4 2021 for NAICS 522: credit intermediation and related activities).

13. Estimate of total annual startup and annual capital costs to respondents (excluding cost of hour burden in Item #12):

Not applicable.

14. Estimate of annualized costs to the Federal government:

Not applicable.

15. Change in burden:

Previous Burden: 1,215,140
Current Burden: 1,154,540
Difference: - 60,600

The change in burden is due to changes in the number of regulated entities within each asset size category.

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

The Agencies have no plans to publish the information for statistical purposes.

17. Reasons for not displaying OMB approval expiration date:

Not applicable. The Agencies will display the OMB approval expiration date.

18. Exceptions to the certification statement:

None.

B. Collections of Information Employing Statistical Methods.

Not applicable.