Supporting Statement
FFIEC Cybersecurity Assessment Tool
OMB Control No. 1557-NEW

A. Justification.

1. Circumstances that make the collection necessary:

Cyber threats have evolved and increased exponentially, with greater sophistication than ever before. Financial institutions[1] are exposed to cyber risks because they are dependent on information technology to deliver services to consumers and businesses every day. Cyber attacks on financial institutions may not only result in access to, and the compromise of, confidential information, but also the destruction of critical data and systems. Disruption, degradation, or unauthorized alteration of information and systems can affect an 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 are at risk.

For this reason, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve, and the National Credit Union Administration (together, the "agencies"), under the auspices of the Federal Financial Institutions Examination Council ("FFIEC"), have accelerated efforts to assess and enhance the state of the financial industry's cyber preparedness, and to close gaps in the agencies' examination procedures and training that can strengthen the oversight of financial industry cybersecurity readiness. The agencies also have focused on improving their abilities to provide financial institutions with resources that can assist in protecting institutions and their customers from the growing risk posed by cyber attacks.

As part of these increased efforts, the agencies have developed a Cybersecurity Assessment Tool ("Assessment") that will assist financial institutions of all sizes in assessing their inherent cybersecurity risk and their risk management capabilities. The Assessment allows a financial institution to identify its inherent cyber risk profile based on the financial institution's technologies and connection types, delivery channels, online/mobile products and technology services it offers, organizational characteristics, and threats it is likely to face. Once an institution identifies its inherent risk, it can evaluate its level of cybersecurity preparedness based on the institution's cyber risk management and oversight, threat intelligence capabilities, cybersecurity controls, external dependency management, and cyber incident management and resiliency planning using the Assessment's maturity matrix. A financial institution can use the maturity levels to identify opportunities for improving the institution's cybersecurity, based on its inherent risk profile. The Assessment also will enable financial institutions to identify areas more rapidly that could improve their cybersecurity risk management and response programs, if needed.

---

[1] For purposes of this supporting statement and information collection, the term "financial institution" includes banks, savings associations, credit unions, bank and saving and loan holding companies and critical third-party service providers to financial institutions.

2. Use of the information:

The Assessment can be used by financial institutions to assist in evaluating and managing their inherent risk and cyber preparedness. Financial institutions, particularly smaller institutions, have requested this assistance. The Assessment will facilitate the ability of financial institutions to address their cybersecurity preparedness on an ongoing basis, as cyber threats evolve, and as financial institutions introduce new products and services, and employ new technologies. Concepts contained in the Assessment will also be incorporated into agency examination processes.

3. Consideration of the use of improved information technology:

The collection will be 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 cyber preparedness. The Assessment also takes into account an individual institution's risk and complexity. Further, use of the Assessment is not mandatory.

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 expectations outlined in the FFIEC IT Examination Handbook. Finally, the agencies are issuing 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.

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

The collection will be 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 1320.5(d)(2):

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

8. Efforts to consult with persons outside the agency:

The Assessment incorporates the publicly available cybersecurity framework developed by the National Institute of Standards and Technology. The Assessment tailors this framework to the financial industry. We have requested a waiver from the *Federal Register* publication requirement for our emergency request, therefore we have not published a notice for comment.

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:*

OCC:

Estimated Number of Respondents: 1,511 (19 large; 48 mid-size (including credit card banks); and 1,444 community national banks and Federal savings associations)

Estimated Burden per Response: 80 hours

Total Estimated Burden: 120,880 hours

Board:

Estimated Number of Respondents: 5,282 (858 state member banks; 522 large bank holding companies; 3902 small bank holding companies)

Estimated Burden per Response: 80 hours

Total Estimated Burden: 422,560

FDIC:

Estimated Number of Respondents: 4,084 (includes 3,882 community banks)

Estimated Burden per Response: 80 hours

Total Estimated Burden: 326,720

NCUA:

Estimated Number of Respondents: 6,206

Estimated Burden per Response: 80 hours

Total Estimated Burden: 496,480

All Agencies:

Estimated Number of Respondents: 176 technology service providers

Estimated Burden per Response: 80 hours

Total Estimated Burden: 14,080 hours

Grand Total Estimated Burden: 1,380,720 hours

1,380,720 **x $95.50 = $131,858,760**

To estimate compensation costs associated with the collection, we used $95.50 per hour, which is based on May 2012 Bureau of Labor Statistics wage data for the average of the 90th percentile for seven occupations (i.e., accountants and auditors, compliance officers, financial analysts, lawyers, management occupations, software developers, and statisticians) plus an additional 33 percent to cover inflation adjustments and private sector benefits. According to Bureau of Labor Statistics employer costs of employee benefits data, thirty percent represents the average private sector costs of employee benefits. We use an inflation estimate of 3 percent.

* Burden is estimated conservatively and assumes all institutions will complete the Assessment. Therefore, the estimated burden will likely exceed the actual burden because of the Assessment by financial institutions is not mandatory.

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:

The increase in burden is because this is a new collection.

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.