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 exponentially with greater 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. 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 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 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 (together, 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 that can strengthen the oversight of financial industry cybersecurity readiness. The Agencies also have focused on providing financial institutions with resources that can assist in protecting financial institutions and their customers from the growing risks posed by cyber attacks.

As part of these efforts, the Agencies 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 the technologies and connection types, delivery channels, online/mobile products and technology services that it offers to its customers, its organizational characteristics, and the 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 the financial institution's cyber risk management and oversight, threat intelligence capabilities, 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 the financial institution's 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 risk management and response programs, as appropriate. Use of the Assessment by financial institutions is voluntary.

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

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

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 financial institutions 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 expectations outlined in the FFIEC IT Examination Handbook. Finally, the Agencies issued 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 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 April 5, 2019, the OCC, on behalf of the Agencies published a 60-day notice requesting comment on this collection of information.[2]

The OCC received two comments from industry trade associations and one comment from the Financial Services Sector Coordinating Council (FSSCC). The comments, described below, address concerns related to the collection of information.

Usability and Format of the Assessment

One industry group suggested changes to the format of the Assessment to increase usability. This industry group suggested that the FFIEC provide banks an automated or interactive document that banks can use to input information for the Assessment, as opposed to a static PDF document of questions and responses. The industry group added that many community banks are using the Financial Services Sector Coordinating Council's automated Assessment spreadsheet to complete the Assessment in advance of their examinations.

While this industry group asked the Agencies to provide the Assessment in a format that can be easily completed and provided to the examiner, if requested, the commenter also stated that none of the banks it represents reacted favorably to the questions in the notice inviting comment on the FFIEC agencies' potential use of automated collection techniques or other forms of information technology to collect Assessment information. This industry group stated that several banks were concerned that automated collection would lead to a greater need to provide defensible answers during the examination review of the Assessment. The industry group also stated, however, that many banks find it useful to discuss the Assessment with the examiner on-site.

The Agencies acknowledge the potential value of an automated or editable form of the Assessment for financial institutions that choose to use the Assessment. However, as the commenters noted, there are currently available a number of automated versions of the Assessment developed by financial institutions and industry groups. Automated versions are available publicly through trade associations, the Financial Services Information Sharing and Analysis Center, and the FSSCC. Accordingly, the Agencies do not intend to release an additional automated or editable version of the Assessment at this time.

Utility of the Assessment

One industry group commenter stated that the inherent risk review is very linear and could be better rooted in bank operations and market conditions. As an example, this commenter stated that many community banks engage cloud providers for data management, and while cloud computing is a standard term, not all cloud computing companies are equal. They do not all have the same risks or mitigating controls. The commenter stated that when a community bank checks the "most" risk level due to the sheer number of cloud providers, the Assessment should allow for an additional level of risk mitigation, such as vendor management and vendor type, which could significantly reduce the risk.

[2] 84 FR 13786.

The Agencies appreciate the feedback and are continually seeking ways to update and improve the tools they use to assess cybersecurity. For example, in response to requests from financial institutions, the Agencies recently updated the Assessment to expand the response options for each declarative statement. With the additional response options, financial institutions' management may include supplementary or complementary behaviors, practices, and processes that represent current practices of the institution in assessing declarative statements.

Voluntary Nature of the Assessment

Both industry groups and the FSSCC stated that most financial institutions employ the Assessment as one of the tools they use to assess their cybersecurity risk and maturity. However, they do not use the Assessment exclusively. Most use the Assessment in conjunction with other recognized technology frameworks. As such, the commenters said that examiners should not require the use of the Assessment nor require a financial institution to translate any other risk framework they use into the Assessment format. The commenters stated that if a regulator requires an examiner to complete the Assessment, then the examiner should translate the framework used by the institution into the Assessment format.

The FSSCC and one industry group commenter stated that most of the financial institutions under the Agencies' respective jurisdictions do not perceive the Assessment to be voluntary. To clarify this misperception, these commenters asked the Agencies to make a clear statement that other methodologies, such as NIST Cybersecurity Framework and the FSSCC Cybersecurity Profile, are acceptable inputs into the examination process. The FSSCC also stated that the Agencies should more closely align the Assessment with the NIST Cybersecurity Framework or a NIST-based standard, like the FSSCC Cybersecurity Profile, because the NIST Cybersecurity Framework represents a leading approach to cybersecurity with an international community of users.

One industry group commenter stated that several of its members expressed concern that examiners sometimes provide only a cursory review of the Assessment, if at all, with financial institution staff. This industry group asked the Agencies to clarify that if an institution takes the time to complete the Assessment, examiners should spend time reviewing it with the institution, and that if examiners complete the Assessment as part of the examination process, then the examiner-completed Assessment should be reviewed with the institution during the exam.

The Agencies agree that the NIST Cybersecurity Framework is a valuable tool that provides a mechanism for cross-sector coordination. When developing the Assessment, the Agencies were informed by the NIST Cybersecurity Framework, the FFIEC Information Technology Examination Handbook, and industry accepted cybersecurity practices. In addition, Appendix B of the Assessment provides a mapping of the Assessment to the NIST Cybersecurity Framework. NIST reviewed and provided input on the mapping to ensure consistency with the NIST Cybersecurity Framework principles and to highlight the complementary nature of the two resources.

The NIST Cybersecurity Framework is intended to address cybersecurity across many different sectors. The Agencies determined that developing an assessment, informed by the NIST Cybersecurity Framework but tailored to the specific risks and risk management and controls expectations within the banking industry, could help financial institutions to effectively assess their cybersecurity preparedness. Additionally, we note that prior to the development of the Assessment, the Agencies received many requests from financial institutions, particularly smaller financial institutions, to provide them with a meaningful way to assess cyber risks themselves based on financial sector-specific risks and mitigation techniques. The Agencies developed the Assessment, in part, to address those requests and received several positive comments about how the Assessment met this need. Thus, the Agencies believe the Assessment supports financial institutions by giving them a systematic way to assess their cybersecurity preparedness and evaluate their progress.

Finally, as the Agencies stated when the Assessment was first published, use of the Assessment by financial institutions is voluntary. Therefore, financial institutions may choose to use the Assessment, the NIST Cybersecurity Framework, or any other risk assessment process or tool to assess cybersecurity risk. The Agencies' examiners will not require a financial institution to complete the Assessment, nor will they require financial institutions to translate other risk frameworks into the Assessment format. However, if a financial institution has completed the Assessment, examiners may ask the financial institution for a copy, as they would for any risk self-assessment performed by a financial institution.

Benchmarking

One industry group stated that an advantage to the broad collection of Assessment information across the entire financial services sector is the ability to compile information into useful benchmarking data for banks of comparable size and risk profiles so that peer institutions may become aware of their overall cybersecurity posture in the sector. The industry group stated that the information may be useful to an information security officer or board of directors, particularly when it comes time to discuss budget impacts of the financial institution's security posture. Additionally, benchmarking may allow the Agencies insight into broad categories of risk and exposure in the financial services sector.

Since use of the Assessment by financial institutions is voluntary and may vary across financial institutions, the Agencies do not to intend to publish or otherwise make publicly available the results of financial institutions' use of the Assessment.

Accuracy of Burden Estimate

The Agencies estimated that, annually, it would take a financial institution between 80 and 180 burden hours, depending on the institution's size, to complete the Assessment.

All three commenters addressed the accuracy of the Agencies' burden estimates. The FSSCC letter stated that the Agencies' burden estimate understated the burden involved in completing the Assessment, and one of the industry groups referenced and endorsed the FSSCC's conclusions in its letter. The FSSCC advised that to be more accurate, the Agencies'

burden hour estimates should include the time required to prepare for and complete the Assessment. The FSSCC stated that preparing to complete the Assessment includes the testing of controls and systems, gathering of materials as evidence, and the accompanying education of staff that are not familiar with the Assessment. The FSSCC stated that the time required to collect evidence and review systems before the Assessment can begin is significant, and the hours required to review the Assessment's more than 530 responses—usually by committee—is substantial. The FSSCC further stated that the hours required to complete responses to the Assessment, while concurrently completing assessments based on other industry-based standards (e.g., NIST Cybersecurity Framework) for other regulatory agencies (such as state or market regulators), is significant. The FSSCC added that the amount of time spent training cybersecurity professionals on the Assessment is underestimated.

The other industry group stated that the Agencies overestimated the burden hours necessary for community banks to complete and subsequently update the Assessment. This industry group stated that its members reported the burden of completing an initial Assessment as being 40 hours or less. Members of this industry group reported that the burden of completing annual updates to the Assessment for subsequent evaluations could take between 15 and 20 hours.

The Agencies do not believe that commenters provided any additional information that would result in the Agencies changing their burden estimates at this time. The PRA defines burden to include the "time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a federal agency." 44 U.S.C. § 3502(2). The Agencies note that the burden estimates assume that the Assessment is completed by knowledgeable individuals at the financial institution who have readily-available information to complete the Assessment. Additionally, while the Assessment's User's Guide provides that institutions may use the Assessment to prioritize improvement of their cybersecurity posture, completing the Assessment does not include development or implementation of action plans. The Agencies further note that completion of the Assessment does not include internal reporting. Any internal reporting that financial institutions may choose to undertake is therefore outside of the scope of the Assessment. Because reporting to committees, developing and implementing internal action plans, and preparing for examinations are not part of completing the Assessment, these activities do not constitute burden under the PRA. In addition, for financial institutions, reporting to boards and management generally constitutes a usual and customary business practice. Usual and customary business practices are excluded from the definition of burden under OMB regulations.[3]

The Agencies recognize that the size and complexity of a financial institution impacts the amount of time and resources necessary to complete the Assessment and, for that reason, the Agencies' burden estimates vary based on financial institution asset size. The Agencies also appreciate that the time necessary for a particular financial institution to complete the Assessment can vary, potentially widely, based on whether the institution has readily available information to complete the Assessment. The Agencies will review their burden estimates from time to time and will update them in the future, if warranted.

[3] 5 CFR 1320.3(b).

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:*

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:	823 x 80 = 65,840 hours	157 x 120 = 18,840 hours	123 x 160 = 19,680 hours	82 x 180 = 14,760 hours	1,185 respondents 119,120 hours
FDIC State Non-Member Banks and State Savings Associations:	2,689 x 80 = 215,120 hours	760 x 120 = 91,200 hours	34 x 160 = 5,440 hours	6 x 180 = 1,080 hours	3,489 respondents 312,840 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
NCUA Federally-Insured Credit Unions:	4,830 x 80 = 386,400 hours	536 x 120 = 64,320 hours	8 x 160 = 1,280 hours	1 x 180 = 180 hours	5,375 respondents 452,180 hours
Total:	11,110 x 80 = hours = 888,800	2,219 x 120 hours = 266,280 hours	246 hours x 160 = 39,360 hours	115 hours x 180 = 20,700 hours	13,690 Respondents 1,215,140 hours

1,215,140 x $114 = $138,525,960

To estimate wages we reviewed May 2018 data for wages (by industry and occupation) from the U.S. Bureau of Labor Statistics (BLS) for credit intermediation and related activities excluding nondepository credit intermediaries (NAICS 5220A1). To estimate compensation costs associated with the rule, we use $114 per hour, which is based on the average of the 90th percentile for nine occupations adjusted for inflation (2.8 percent as of Q1 2019 according to the BLS), plus an additional 33.2 percent for benefits (based on the percent of total compensation allocated to benefits as of Q4 2018 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: 1,474,660
Current Burden: 1,215,140
Difference: - 259,520

The reduction in burden is due to the reduction in the number of regulated entities.

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.