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:

OMB provided a one-year clearance for revisions to the FFIEC Cybersecurity Assessment Tool (Assessment).[1] The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the OCC (Agencies) propose to extend OMB approval of the collection for the standard three years.

Cyber threats have evolved and increased exponentially with greater sophistication than ever before. Financial institutions[2] 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 Agencies, under the auspices of the FFIEC, have accelerated efforts 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 improving their abilities to provide 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 increased efforts, the Agencies developed the 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 financial institution's 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 will be able to 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 identify areas more rapidly that could improve the financial institution's cyber risk management and response programs, if needed. Use of the Assessment by financial institutions is voluntary.

[1] http://www.ffiec.gov/cyberassessmenttool.htm.
[2] 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 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 1320.5(d)(2):

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:

60-Day *Federal Register* Notice

On July 22, 2015, (80 FR 4355), the Agencies published a 60-day notice requesting comment on the collection of information titled "FFIEC Cybersecurity Assessment Tool (Assessment)." The Agencies also met with the Financial Services Sector Coordinating Council on November 5, 2015, in response to a request for a meeting. The Agencies received eighteen comments: twelve comments from individuals, five from industry trade associations, and one from the Financial Services Sector Coordinating Council (FSSCC). The comments described below address concerns related to the collection of information.

Request for more Information on the Information Being Collected

Eight of the commenters requested that the Agencies provide additional clarity and interpretative information regarding the Assessment. Several of these commenters requested that the Agencies clarify some of the statements in the Inherent Risk Profile.[3] Commenters also stated that many of the declarative statements in the Cybersecurity Maturity[4] were subjective and susceptible to different interpretation. Other commenters requested the Agencies provide additional information regarding the relationship between the Inherent Risk Profile and the Cybersecurity Maturity parts of the Assessment.

Five commenters requested that the Agencies publish information clarifying the Assessment, such as an appendix to the Assessment or a separate frequently asked questions (FAQ) document. One commenter requested that the Agencies issue a separate document describing the assumptions the Agencies used in developing the Assessment. Another commenter requested that the Agencies provide examples of how community financial institutions might satisfy certain declarative statements. Additionally, one commenter requested that the Agencies develop a 12-18 month collaborative process with the commenter to improve the Assessment prior to finalizing the Assessment or using the Assessment on examinations.

The Agencies appreciate the feedback and comments received from the commenters. The Agencies recognize that there may be a need to clarify certain aspects of the Assessment and will consider developing an FAQ document to address questions and requests for clarification that they have received since the publication of the Assessment, including from commenters. Additionally, the Agencies are developing a process to update the Assessment on a periodic basis. The update process will consider comments from interested parties.

Usability and Format of the Assessment

Four commenters suggested changes to the format of the Assessment to increase usability. The commenters requested that the Agencies develop an automated or editable form of the Assessment. Commenters stated that the ability to save and edit responses contained in the Assessment would improve a financial institution's ability to use the Assessment on an ongoing basis.

---

[3] Part One of the Assessment, the Inherent Risk Profile, assists a financial institution in identifying its inherent risk before implementing controls.

[4] Part Two of the Assessment, the Cybersecurity Maturity, assists a financial institution in determining its current state of cybersecurity preparedness represented by maturity levels across five domains.

One commenter also recommended that the Agencies revise the Assessment to include hyperlinks to the Assessment Glossary and User Guide instructions. Another commenter suggested that the Agencies revise the Assessment to assign a maturity level[5] automatically to the financial institution once it completes the Inherent Risk Profile portion of the Assessment. In addition, this commenter suggests that once a financial institution answers "no" to a declarative statement in a particular domain of the Cybersecurity Maturity, the Assessment should automatically prevent the financial institution from responding to the remainder of the declarative statements within that domain. The commenter also stated the Assessment should automatically populate answers to similar questions across domains and maturity levels.

The Agencies acknowledge the potential value of an automated or editable form of the Assessment for financial institutions that choose to use the Assessment and are exploring the possibility of developing an automated form in the future, including the possibility of hyperlinking to definitions and instructions. Any automation of the form, however, would not include the automatic assignment of a maturity level as the Agencies do not have expectations for any financial institution to reach a specific maturity level within the Assessment, and a financial institution may find value in identifying activities it is already performing at a higher maturity level.

Utility of the Assessment

Two commenters stated that there are a number of cybersecurity assessment frameworks available to financial institutions to use in determining their inherent risk and cybersecurity preparedness. These commenters questioned the need for the development of an additional framework. One commenter focused on the potential duplication between the National Institute of Standards and Technology's Cybersecurity Framework (NIST Framework) and the Assessment. This commenter stated that use of the Assessment by financial institutions, instead of the NIST Framework, could dilute the value of the NIST Framework as a tool for cross-sector collaboration.

The Agencies, under the auspices of the FFIEC, developed the Assessment to assist financial institutions in addressing the cyber risks unique to the financial industry. The Assessment supports financial institutions by giving them a systematic way to assess their cybersecurity preparedness and evaluate their progress. Unlike other frameworks, the Assessment is specifically tailored to the products and services offered by financial institutions and the control and risk mitigation techniques used by the industry. In addition, the Agencies have 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. As discussed more fully below, a financial institution is not required to use the Assessment and may choose any method the financial institution determines is relevant and meaningful to assess its inherent risk and cybersecurity preparedness.

The Agencies agree that the NIST Framework is a valuable tool and the Agencies incorporated concepts from the NIST Framework into the Assessment. The Assessment contains an appendix that maps the NIST Framework to the Assessment. NIST reviewed and provided input on

[5] Within the five domains of the Cybersecurity Maturity, declarative statements describe the requirements for achieving five possible maturity levels for each domain.

the mapping to ensure consistency with the NIST Framework's principles and to highlight the complementary nature of the two resources. The Agencies also agree that the NIST Framework provides a mechanism for cross-sector coordination. However, because of the unique cyber risks facing the financial industry, the Agencies identified a need to develop a more granular framework that is more specific to the financial services industry to assist financial institutions in evaluating themselves.

Several commenters also raised questions regarding the Agencies' use of a maturity model as a part of the Assessment. Four commenters were concerned with the "all or nothing" approach to achieving a maturity level, particularly insofar as a financial institution might not be credited for activities taken at a higher level that might mitigate risks at a lower level. Some commenters stated that a maturity model is too prescriptive and does not adequately account for compensating controls or risk tolerance and others questioned why the Assessment does not discuss the concept of residual risk.

The Agencies designed the Cybersecurity Maturity contained in the Assessment to assist financial institutions in understanding the ranges of controls and practices needed to manage cyber risk. As previously stated, use of the tool is voluntary and a financial institution may use any method to assess inherent risk and cybersecurity preparedness that it considers relevant and meaningful.

The User's Guide does provide general parameters to assist financial institutions that choose to use the Assessment in considering how to align inherent risk with the financial institution's processes and control maturity.

Accuracy of Burden Estimate

The Agencies estimated that, annually, it would take a financial institution 80 burden hours, on average, to complete the Assessment. Five comment letters addressed the accuracy of the Agencies' burden estimate. These letters generally stated that the Agencies' burden estimate understated the burden involved. One commenter stated that credit unions that choose to use the Assessment could take 80-100 hours to complete it. However, other commenters stated that it may take a financial institution several hundred hours to complete the Assessment in the first year of use.

One commenter stated that the estimated burden will vary based on financial institution size, with smaller financial institutions requiring hundreds of hours to complete the Assessment, medium-sized financial institutions approaching 1,000-2,000 hours, and the large financial institutions investing 1,000-2,000 hours or more. This commenter stated that the burden estimate includes the amount of time needed to collect information and documentation sufficient to provide answers supportable in the examination context, report to internal steering committees, and prepare for examinations. Another commenter stated that the Agencies' evaluation of 80 hours "largely underestimates" the time required to complete the Assessment. This commenter stated that the initial completion of the Assessment would include collecting data, discussing and verifying responses, performing gap analysis, preparing and implementing action plans, where needed, and presenting results to executives.

In light of the comments received and recent supervisory experience performing information technology examinations, the Agencies are revising their burden estimates. In revisiting the burden estimates, the Agencies are taking a more conservative approach to estimating the potential burden involved in using the Assessment. The Agencies recognize that size and complexity of a financial institution, as noted by some of the commenters, impacts the amount of time and resources to complete the Assessment and therefore the Agencies have further refined their burden estimates based on financial institution asset size.

The Agencies note that the revised burden estimates assume that the Assessment is completed by knowledgeable individuals at the financial institution who have readily-available information to complete the Assessment. The Agencies' revised burden estimates do not include the amount of time associated with reporting to management and internal committees, developing and implementing action plans, and preparing for examination as such time and resources are outside the scope of the information collection.

Information Storage and Confidentiality

Two commenters requested information on how the Agencies will use and store the Assessment information that financial institutions provide to the Agencies. The Agencies are subject to compliance with the Federal Information Security Management Act (FISMA) and they operate cybersecurity programs to protect critical information resources, including sensitive financial institution information obtained or created during their supervision activities. The programs include policies, standards and controls, monitoring, technical controls, and other information assurance processes. If a financial institution provides the Assessment, or any other, confidential information to an examiner as part of the supervisory process, the storage and use of such information would be subject to the Agencies' cybersecurity programs.

Benchmarking

One commenter suggested that the Agencies collect, anonymize, and share Assessment information to allow financial institutions to benchmark themselves against comparably sized financial institutions. Since use of the Assessment by financial institutions is voluntary, the Agencies do not to intend to collect the Assessment from financial institutions or publish the results.

Voluntary Use of the Assessment

Several commenters expressed concern that since some of the Agencies will be using the Assessment as an aid in their examination processes, financial institutions may believe that their use of the Assessment is mandated by the Agencies. Another commenter requested that the Agencies ensure that examiners do not force financial institutions to use the Assessment or require financial institutions to justify their decisions to use an alternative cybersecurity assessment. Several commenters requested that the Agencies reiterate to examiners and to financial institutions that use of the Assessment by a financial institution is voluntary.

As the Agencies stated when the Assessment was first published, use of the Assessment by financial institutions is voluntary. Financial institutions may use the Assessment or any other framework or process to identify their inherent risk and cybersecurity preparedness. The Agencies' examiners will not require a financial institution to complete the Assessment. However, if a financial institution has completed an Assessment, examiners may ask the financial institution for a copy, as they would for any risk self-assessment performed by the financial institution. The Agencies are educating examiners on the voluntary nature of the Assessment and including statements about its voluntary nature in examiner training materials.

30-Day *Federal Register* Notice

On December 16, 2015, the Agencies published a 30-day notice requesting comment on the collection of information titled "FFIEC Cybersecurity Assessment Tool (Assessment)," (80 FR 78285). The Agencies received six comments: three comments from individuals, two from industry trade associations, and one from the FSSCC. The comments described below relate to the collection of information. Some commenters also discussed aspects of the Assessment unrelated to the collection of information; these comments are not relevant to this notice or the paperwork burden analysis and, accordingly, they are not addressed below. However, the comments unrelated to the paperwork burden analysis were provided to Agency personnel responsible for the Assessment for possible consideration in future Assessment updates.

Request for More Clarity on the Information Being Collected

Four of the commenters provided responses related to the clarity of the Assessment. Two commenters stated their appreciation of the Agencies' willingness to consider providing additional clarity regarding the Assessment. One of these commenters requested examples of how smaller community financial institutions could satisfy certain declarative statements.[6] Another commenter stated that providing additional definitions and clarifying terms would help with completing the Assessment. A commenter also supported the Agencies' decision to develop a process to update the Assessment periodically. Two commenters requested that the Agencies engage in a collaborative process with the industry to update the Assessment.

The Agencies appreciate the feedback and comments. As the Agencies stated previously, they recognize that there may be a need to clarify certain aspects of the Assessment and intend to publish FAQs to provide further clarification on aspects of the Assessment. The Agencies anticipate issuing this FAQ document in third quarter 2016.

Additionally, the Agencies intend to consider comments from interested parties in any updates to the Assessment. The Agencies also have received feedback from interested parties through industry meetings related to cybersecurity since issuing the Assessment. The Agencies met with the FSSCC during the PRA comment process to obtain feedback on the Assessment. Finally, the Agencies held a working session during the National Institute of Standards and Technology (NIST) Cybersecurity Framework Workshop on April 7, 2016. The purpose of that meeting was to obtain additional industry feedback on possible improvements to the Assessment and on what additional FAQs could be helpful to institutions that choose to use the Assessment.

Utility of the Assessment

One commenter stated that the Assessment is not "harmonized" with the NIST Cybersecurity Framework in that an institution cannot also determine its risk posture under the NIST Cybersecurity Framework by completing the Assessment. The commenter stated that using the NIST Cybersecurity

[6] Within each of the five domains of the Cybersecurity Maturity section, declarative statements describe the capabilities an institution should implement and sustain to achieve the five possible maturity levels in each domain. The Cybersecurity Maturity section assists a financial institution in determining its current state of cybersecurity preparedness.

Framework as the foundation for the Assessment would facilitate a common cybersecurity lexicon and taxonomy, improve coordination with other sectors, and further facilitate vendor and third-party management.

In developing the Assessment, the Agencies were informed by the NIST Cybersecurity Framework, the FFIEC Information Technology Examination Handbook, and industry accepted cybersecurity practices. 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. Therefore, 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. Further, use of the Assessment by financial institutions is voluntary, and, therefore, institutions may choose to use the Assessment, the NIST Cybersecurity Framework, or any other risk assessment process or tool to assess cybersecurity risk.

Two commenters expressed concern with the certain elements of the Cybersecurity Maturity section of the Assessment.[7] These commenters suggested that the Assessment may not fully account for an institution's risk tolerance, compensating controls, and other risk mitigating activities. Rather than the Yes-No approach to meeting declarative statements contained in the Assessment, one commenter suggested allowing more possible responses, such as "Yes, No, Partial, Compensating Controls Used, or Not Applicable." The second commenter suggested that institutions using the Assessment should be able to provide a percentage of readiness based on the degree of implementation of a given control in response to a declarative statement.

As noted above, completion of the Assessment is voluntary. Therefore, while compensating controls are not specifically described in the Assessment, financial institutions may customize the Assessment. This may include identifying methods to account for compensating controls and an institution's individual risk tolerance.

One commenter also expressed concern with the Inherent Risk Profile,[8] stating that there is a lack of clear guidance on how to determine an overall risk level. To clarify how to determine an overall Inherent Risk Profile, an institution can determine its overall Inherent Risk Profile based on the number of applicable statements in each risk level for all activities, products, and services. Each category may, however, pose a different level of inherent risk. Therefore, in addition to evaluating the number of instances that an institution selects a specific risk level, management may also consider evaluating whether a specific category poses additional risk. The Assessment's User's Guide provides additional information on how financial institutions may choose to use the Assessment to identify their risks and determine their cybersecurity maturity.

Accuracy of Burden Estimate

[7] As noted above, part two of the Assessment, the Cybersecurity Maturity, assists a financial institution in determining its current state of cybersecurity preparedness represented by maturity levels across five domains.
[8] Part One of the Assessment, the Inherent Risk Profile, assists a financial institution in identifying its inherent risk before implementing controls.

Based on the comments received in response to the 60-day notice requesting comment on this information collection, published July 22, 2015, (80 FR 4355) (60-day notice), the Agencies increased their burden estimates and tiered the estimates based on asset size. One commenter appreciated that the Agencies had refined their burden estimates based on asset size. However, two commenters believed that the estimates remain understated. One of these commenters discussed the commenter's experience completing the Assessment, stating that the commenter had spent 200-300 hours working on the Assessment but had not yet completed it. The commenter included the time required to gather the data, because some questions require information that is not readily available at the commenter's institution. A second commenter disagreed with the Agencies' conclusion that the relevant burden estimate should not include the time associated with reporting to management and internal committees, developing and implementing action plans, and preparing for examinations. This commenter suggested that, because some of the Agencies will use the Assessment as part of the examination process, responses to the Assessment will take more time to prepare and review for accuracy and completeness.

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). There is no expectation that financial institutions develop supporting documentation when completing the Assessment. Because reporting to committees, developing and implementing internal action plans, and preparing for examinations are not part of completing the Assessment, the activities described do not constitute burden under the PRA. 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. Furthermore, 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. 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.[9]

The Agencies 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.

Voluntary Use of the Assessment

Several commenters addressed the voluntary nature of the Assessment. One commenter thanked the Agencies for clarifying that the Assessment is a voluntary self-assessment. A commenter appreciated that the Agencies' stated that they would continue to educate examiners on the voluntary nature of the Assessment. Since some of the Agencies will be using the Assessment as an aid in their examination processes, some commenters continue to be concerned that financial institutions may believe that their use of the Assessment is mandated by the Agencies. One commenter expressed concern that examiners may pressure financial institutions to reach a particular maturity or inherent risk level when reviewing the financial institution's completed self-assessment.

[9] 5 CFR 1320.3(b).

Use of the Assessment by financial institutions is voluntary. Financial institutions may use the Assessment or any other framework or process to identify their inherent risk and cybersecurity preparedness. The Agencies' examiners will not require a financial institution to complete the Assessment. Examiner training materials state that completion of the Assessment by financial institutions is voluntary. Further, the Agencies do not expect institutions to obtain a particular inherent risk level or maturity level under the Assessment. The Agencies will continue to emphasize the voluntary nature of the Assessment in the FAQs they intend to issue.

Usability and Format of the Assessment

Several comments on the 60-day notice requested that the Agencies develop an automated or editable version of the Assessment. In response to these comments, the Agencies previously indicated that they would explore the possibility of developing an automated version in the future. However, the Agencies have become aware of 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.[10] Accordingly, the Agencies do not intend to release an additional automated or editable version of the Assessment at this time.

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:*

Estimated Burdens:[11]

[10] See, e.g., https://www.fsisac.com/article/fsscc-automated-cybersecurity-assessment-tool.
[11] Burden is estimated conservatively and assumes all financial institutions will complete the Assessment. Therefore, the estimated burden may exceed the actual burden because use of the Assessment by financial institutions is not mandatory. The Agencies intend to address their review of the cybersecurity readiness and preparedness of financial institutions' technology service providers (TSPs) separately and therefore are no longer including a separate estimated burden for TSPs. However, the burden estimates for financial institutions does include that of TSPs who may assist financial institutions in completing their Assessment.

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:	1,102 x 80 = 88,160 hours	149 x 120 = 17,880 hours	132 x 160 = 21,120 hours	87 x 180 = 15,660 hours	1,470 respondents 142,820 hours
FDIC State Non-Member Banks and State Savings Associations:	3,224 x 80 = 257,920 hours	728 x 120 = 87,360 hours	22 x 160 = 3,520 hours	5 x 180 = 900 hours	3,979 respondents 349,700 hours
Board State Member Banks and Bank Holding Companies:	4,083 x 80 = 326,640 hours	1,083 x 120 = 129,960 hours	74 x 160 = 11,840 hours	42 x 180 = 7,560 hours	5,282 respondents 476,000 hours
NCUA Federally-Insured Credit Unions:	5,622 x 80 = 449,760 hours	463 x 120 = 55,560 hours	4 x 160 = 640 hours	1 x 180 = 180 hours	6,090 respondents 506,140 hours
Total:	14,031 x 80 = 1,122,480 hours	2,423 x 120 = 290,760 hours	232 x 160 = 37,120 hours	135 x 180 = 24,300 hours	16,821 respondents 1,474,660 hours

1,474,660 x $101 = $148,940,660

To estimate average hourly wages we reviewed data from May 2014 for wages (by industry and occupation) from the U.S. Bureau of Labor Statistics (BLS) for depository credit intermediation (NAICS 522100). To estimate compensation costs associated with the rule, we use $101 per hour, which is based on the average of the 90th percentile for seven occupations adjusted for inflation (2 percent), plus an additional 30 percent to cover private sector benefits. Thirty percent represents the average private sector costs of employee benefits.

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:

There is no change in burden.

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.