OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches
Supporting Statement
OMB Control No. 1557-0321

A. Justification

1. Circumstances that make the collection necessary:

The OCC's guidelines codified in 12 CFR part 30, appendix D establish minimum standards for the design and implementation of a risk governance framework for insured national banks, insured Federal savings associations, and insured Federal branches of a foreign bank (bank). The guidelines apply to a bank with average total consolidated assets: (i) equal to or greater than $50 billion; (ii) less than $50 billion if that bank's parent company controls at least one insured national bank or insured Federal savings association that has average total consolidated assets of $50 billion or greater; or (iii) less than $50 billion, if the OCC determines such bank's operations are highly complex or otherwise present a heightened risk as to warrant the application of the guidelines (covered banks). The guidelines also establish minimum standards for a board of directors in overseeing the framework's design and implementation.

The standards contained in the guidelines are enforceable under section 39 of the Federal Deposit Insurance Act (FDIA)[1], which authorizes the OCC to prescribe operational and managerial standards for insured national banks, insured Federal savings associations, and insured Federal branches of a foreign bank.

2. Use of the information:

Following the financial crisis, the OCC developed a set of *heightened expectations* to enhance supervision and strengthen the governance and risk management practices of large national banks.

The guidelines formalize the OCC's heightened expectations program. They also further the goal of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010[2] to strengthen the financial system by focusing management and boards of directors on improving and strengthening risk management practices and governance, thereby minimizing the probability and impact of future financial crises.

The standards for the design and implementation of the risk governance framework, which contain collections of information, are set forth below.

Standards for Risk Governance Framework

[1] 12 U.S.C. 1831p-1. Section 39 was enacted as part of the Federal Deposit Insurance Corporation Improvement Act of 1991, P.L. 102-242, section 132(a), 105 Stat. 2236, 2267-70 (Dec. 19, 1991).
[2] Public Law 111-203, 124 Stat. 1376 (2010).

Covered banks should establish and adhere to a formal, written risk governance framework designed by independent risk management. It should include delegations of authority from the board of directors to management committees and executive officers as well as risk limits established for material activities. It should be approved by the board of directors or the board's risk committee and reviewed and updated at least annually by independent risk management.

Front Line Units

Front line units should take responsibility and be held accountable by the Chief Executive Officer (CEO) and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. In fulfilling this responsibility, each front line unit should, either alone or in conjunction with another organizational unit that has the purpose of assisting a front line unit: (i) assess, on an ongoing basis, the material risks associated with its activities and use such risk assessments as the basis for fulfilling its responsibilities and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the unit's risk profile or other conditions; (ii) establish and adhere to a set of written policies that include front line unit risk limits (such policies should ensure risks associated with the front line unit's activities are effectively identified, measured, monitored, and controlled, consistent with the covered bank's risk appetite statement, concentration risk limits, and all policies established within the risk governance framework); (iii) establish and adhere to procedures and processes, as necessary to maintain compliance with the policies described in (ii); (iv) adhere to all applicable policies, procedures, and processes established by independent risk management; (v) develop, attract, and retain talent and maintain staffing levels required to carry out the unit's role and responsibilities effectively; (vi) establish and adhere to talent management processes; and (vii) establish and adhere to compensation and performance management programs.

Independent Risk Management

Independent risk management should oversee the covered bank's risk-taking activities and assess risks and issues independent of the front line units by: (i) designing a comprehensive written risk governance framework commensurate with the size, complexity, and risk profile of the covered bank; (ii) identifying and assessing, on an ongoing basis, the covered bank's material aggregate risks and using such risk assessments as the basis for fulfilling its responsibilities and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the covered bank's risk profile or other conditions; (iii) establishing and adhering to enterprise policies that include concentration risk limits; (iv) establishing and adhering to procedures and processes to ensure compliance with policies in (iii); (v) identifying and communicating to the CEO and board of directors or board's risk committee material risks and significant instances where independent risk management's assessment of risk differs from that of a front line unit, and significant instances where a front line unit is not adhering to the risk governance framework; (vi) identifying and communicating to the board of directors or the board's risk committee material risks and significant instances where independent risk management's assessment of risk differs from the CEO, and significant instances where the CEO is not adhering to, or holding front line units accountable for adhering to, the risk governance

framework; and (vii) developing, attracting, and retaining talent and maintaining staffing levels required to carry out the unit's role and responsibilities effectively while establishing and adhering to talent management processes and compensation and performance management programs.

Internal Audit

Internal audit should ensure that the covered bank's risk governance framework complies with the Guidelines and is appropriate for the size, complexity, and risk profile of the covered bank. It should maintain a complete and current inventory of all of the covered bank's material processes, product lines, services, and functions, and assess the risks, including emerging risks, associated with each, which collectively provide a basis for the audit plan. It should establish and adhere to an audit plan, which is periodically reviewed and updated, that takes into account the covered bank's risk profile, emerging risks, issues, and establishes the frequency with which activities should be audited. The audit plan should require internal audit to evaluate the adequacy of and compliance with policies, procedures, and processes established by front line units and independent risk management under the risk governance framework. Significant changes to the audit plan should be communicated to the board's audit committee. Internal audit should report in writing, conclusions and material issues and recommendations from audit work carried out under the audit plan to the board's audit committee. Reports should identify the root cause of any material issues and include: (i) a determination of whether the root cause creates an issue that has an impact on one organizational unit or multiple organizational units within the covered bank; and (ii) a determination of the effectiveness of front line units and independent risk management in identifying and resolving issues in a timely manner. Internal audit should establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis. The independent assessment should include a conclusion on the covered bank's compliance with the standards set forth in the Guidelines. Internal audit should identify and communicate to the board's audit committee significant instances where front line units or independent risk management are not adhering to the risk governance framework. Internal audit should establish a quality assurance program that ensures internal audit's policies, procedures, and processes comply with applicable regulatory and industry guidance, are appropriate for the size, complexity, and risk profile of the covered bank, are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry internal audit practices, and are consistently followed. Internal audit should develop, attract, and retain talent and maintain staffing levels required to effectively carry out its role and responsibilities. Internal audit should establish and adhere to talent management processes and compensation and performance management programs that comply with the guidelines.

Strategic Plan

The CEO, with input from front line units, independent risk management, and internal audit, should be responsible for the development of a written strategic plan that should cover, at a minimum, a three-year period. The board of directors should evaluate and approve the plan and monitor management's efforts to implement the strategic plan at least annually. The plan should include a comprehensive assessment of risks that impact the covered bank, an overall mission

statement and strategic objectives, an explanation of how the covered bank will update the risk governance framework to account for changes to its risk profile projected under the strategic plan, and be reviewed, updated, and approved due to changes in the covered bank's risk profile or operating environment that were not contemplated when the plan was developed.

Risk Appetite Statement

A covered bank should have a comprehensive written statement that articulates its risk appetite that serves as the basis for the risk governance framework. It should contain qualitative components that describe a safe and sound risk culture and how the covered bank will assess and accept risks and quantitative limits that include sound stress testing processes and address earnings, capital, and liquidity.

Risk Limit Breaches

A covered bank should establish and adhere to processes that require front line units and independent risk management to: (i) identify breaches of the risk appetite statement, concentration risk limits, and front line unit risk limits; (ii) distinguish breaches based on the severity of their impact; (iii) establish protocols for disseminating information regarding a breach; (iv) provide a written description of the breach resolution; and (v) establish accountability for reporting and resolving breaches.

Concentration Risk Management

The risk governance framework should include policies and supporting processes appropriate for the covered bank's size, complexity, and risk profile for effectively identifying, measuring, monitoring, and controlling the covered bank's concentrations of risk.

Risk Data Aggregation and Reporting

The risk governance framework should include a set of policies, supported by appropriate procedures and processes, designed to provide risk data aggregation and reporting capabilities appropriate for the covered bank's size, complexity, and risk profile and to support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for: (i) the design, implementation, and maintenance of a data architecture and information technology infrastructure that support the covered bank's risk aggregation and reporting needs during normal times and during times of stress; (ii) the capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board of directors and the OCC; and (iii) the distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.

Talent and Compensation Management

A covered bank should establish and adhere to processes for talent development, recruitment, and succession planning. The board of directors or appropriate committee should review and approve a written talent management program. A covered bank should also establish

and adhere to compensation and performance management programs that comply with any applicable statute or regulation.

Board of Directors Training and Evaluation

The board of directors of a covered bank should establish and adhere to a formal, ongoing training program for all directors. The board of directors should also conduct an annual self-assessment.

3. Consideration of the use of improved information technology:

Respondents may use any method of improved technology that meets the requirements of the guidelines.

4. Efforts to identify duplication:

The required 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.

The information collection does not have a significant impact on a substantial number of small businesses or other small entities.

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

If the information were collected less frequently, the OCC would encounter significant difficulties in supervising covered banks and determining whether their governance and risk management practices are appropriate.

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

The information collection would be conducted in a manner consistent with 5 CFR part 1320.

8. Comments in response to the federal register notice and efforts to consult with persons outside the agency:

On July 5, 2017, the OCC issued a notice for 60 days of comment regarding this collection, 82 FR 31151. One comment was received. The commenter suggested that the OCC rescind and not renew the information collection associated with appendix D of 12 CFR part 30 for a number of reasons.

The commenter suggested that almost one half of the banks subject to appendix D have total assets that are significantly less than $50 billion but the narrative surrounding “heightened

standards" leads the public to believe that the guidelines are only applicable to the largest banks or banks that are highly complex or present a heightened risk. Appendix D applies to 34 OCC-supervised banks.[3] Ten of these 34 banks have less than $50 billion in average total consolidated assets. Appendix D applies to banks with less than $50 billion in average total consolidated assets if a bank's parent company controls at least one other bank with average total consolidated assets equal to or greater than $50 billion or if the OCC determines such bank's operations are highly complex or otherwise present a heightened risk as to warrant the application of appendix D. Of the 10 banks covered by appendix D that have less than $50 billion in average total consolidated assets, eight are covered because their parent companies control another bank with average total consolidated assets equal to or greater than $50 billion.[4] One of the two remaining banks is a covered bank because the OCC exercised its reservation of authority to apply appendix D to the bank.[5] The other remaining bank is covered because that bank previously had average total consolidated assets equal to or greater than $50 billion. Appendix D applies to a bank with less than $50 billion in average total consolidated assets when that bank's parent company controls at least one other bank with average total consolidated assets equal to or greater than $50 billion because, in some instances, the OCC has observed that a covered bank's parent company does not pay sufficient attention to the operations of these smaller entities in a holding company structure. Appendix D covers these entities because the OCC believes that a covered bank's parent company should devote adequate attention to assessing and managing the risk associated with these entities' activities. These smaller covered banks are affiliates of large banking organizations, which should have the compliance resources to cover all of their bank charters.

The commenter also indicated that the OCC's annual burden estimate for appendix D was excessive, particularly for institutions that have less than $10 billion in total assets and that appendix D should be rescinded and revised to reduce the excessive costs. As discussed above, appendix D applies primarily to larger banks. The only covered banks that have less than $10 billion in average total consolidated assets are covered banks because their parent companies control another bank with average total consolidated assets equal to or greater than $50 billion. The OCC believes that the burden estimate is reasonable and that it is appropriate for these banks to devote sufficient resources to risk governance and the standards necessary to manage and control risk-taking activities. The burden on these smaller covered banks is not excessive because they have the resources of a larger affiliate bank to rely on. Also, while the commenter recommended that the OCC rescind appendix D, the OCC cannot rescind regulations or guidelines through the PRA renewal process.

The commenter also stated that the collection of information for appendix D is unnecessary and of little utility because appendix D has been ineffectual in fostering enterprise risk governance over large complex financial institutions since almost seven years after the

[3] In the July 5, 2017, Federal Register notice proposing a renewal of the information collection associated with appendix D to 12 CFR part 30, the OCC calculated that 41 OCC-supervised entities were subject to appendix D. The calculation has been updated. This reduced number of respondents is due in part to the fact that certain large banking organizations have consolidated the number of bank charters within their holding company structure.

[4] The commenter requested that the OCC disclose the number of banks with less than $10 billion in total assets that are subject to appendix D. There are five covered banks with average total consolidated assets less than $10 billion, all of which are covered banks because their parent companies control another bank with average total consolidated assets equal to or greater than $50 billion.

[5] https://www.occ.gov/news-issuances/news-releases/2015/nr-occ-2015-105a.pdf.

introduction of the OCC's "heightened expectations" and three years after the issuance of appendix D, the OCC continues to identify enterprise risk governance as a key risk facing large banks in the OCC's spring 2017 Semiannual Risk Perspective.[6] However, while appendix D is intended to promote enterprise risk governance, the OCC recognizes that appendix D cannot eliminate the possibility of all enterprise risk governance weaknesses. The OCC believes that appendix D is a valuable mechanism for promoting sound enterprise risk governance and has observed significant improvement in risk governance since the adoption of appendix D. However, we also realize that risk governance weaknesses may remain and can be a risk to the safety and soundness of banks.

The commenter also indicated that there is a disconnect between the specific risks identified in the OCC's Semiannual Risk Perspectives and the "abstract generalized" standards in appendix D. According to the commenter, appendix D does not provide standards addressing the specific risks identified in the Semiannual Risk Perspectives, such as cyber security and Bank Secrecy Act (BSA) and Anti-Money Laundering risks (AML). The standards in appendix D are not intended to exhaustively address all of the risks facing OCC-regulated banks. Indeed, there is a separate appendix to 12 CFR part 30, appendix B that contains standards addressing information security. Banks are also subject to separate BSA and AML requirements.[7]

The commenter also expressed the opinion that the standards in appendix D are not actually heightened or more robust than the standards the OCC applies to many banks with $1 billion or more in total assets and that the reality is the OCC applies the standards in appendix D to many midsize and community banks. The commenter pointed specifically to the Comptroller's Handbook on Corporate and Risk Governance (handbook), suggesting that OCC examiners use this handbook for all OCC supervised banks.[8] Appendix D only applies to banks with average total consolidated assets equal to or greater than $50 billion, banks with average total consolidated assets less than $50 billion when a bank's parent company controls at least one other bank with average total consolidated assets equal to or greater than $50 billion, and banks with average total consolidated assets less than $50 billion if the OCC determines that a bank's operations are highly complex or otherwise present a heightened risk. The handbook referenced by the commenter specifically notes that only banks with average total consolidated assets of $50 billion or greater (or banks that are otherwise included as covered banks in appendix D) should adhere to the standards in appendix D. The handbook includes separate and specific criteria for the covered banks subject to appendix D. Appendix D contains various standards that are not applied to smaller banks. For example, appendix D specifically provides that at least two members of a covered bank's board of directors should qualify as independent and provides that boards should establish and adhere to a formal, ongoing training program. Appendix D also imposes specific requirements on covered banks' independent risk management that are not applied to all OCC-regulated banks, including requiring that banks covered by appendix D have written risk appetite statements that include quantitative limits. Additionally, the standards in appendix D are legally different than the standards contained in the handbook. The standards in

[6] https://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2017.pdf.
[7] See 12 CFR part 21.
[8] https://www.occ.treas.gov/publications/publications-by-type/comptrollers-handbook/corporate-risk-governance/pub-ch-corporate-risk.pdf.

Appendix D are legally enforceable standards adopted pursuant to section 39 of the FDIA while the handbook is a guidance document.

9. Payment or gift to respondents:

Not applicable.

10. Any assurance of confidentiality:

The information collection request will be kept private to the extent permissible by law.

11. Justification for questions of a sensitive nature:

Not applicable. No personally identifiable information is collected.

12. Burden estimate:

The OCC estimates the burden of this collection of information as follows:

Total number of respondents: 34
Total burden per respondent: 3,776
Total burden for collection: 128,384

Cost of Hour Burden
128,384 x $114 = $14,635,776

To estimate average hourly wages we reviewed data from May 2016 (released in March 2017) 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 $114 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 costs to respondents (excluding cost of hour burden in Item #12):

None.

14. Estimate of annualized costs to the Federal Government:

None.

15. Change in burden:

The estimated burden per respondent has not changed. The estimated number of respondents has changed in part because the number of charters subject to appendix D of 12 CFR part 30 has changed. The result is an overall increase in burden of 11,328 hours.

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

There are no publications.

17. Reasons for not displaying OMB approval expiration date:

The agency is not seeking to display the expiration date of OMB approval of the information collection.

18. Exceptions to certification statement:

There are no exceptions to the certification.

B. Collection of Information Employing Statistical Methods

The collection of this information does not employ statistical methods. Statistical methods are not appropriate for the type of information collected and would not reduce burden or improve accuracy of results.