First National of Nebraska

1620 Dodge Street
Omaha NE 68197
402.341.0500

September 21, 2015

To whom it may concern,

The purpose of this letter is to respond to the request for comment from the OCC on behalf of the Agencies concerning the recently published "FFIEC Cybersecurity Assessment Tool" (Assessment). While the Assessment is a valuable exercise for financial institutions, certain improvements should be considered in order to enhance its benefits.

The Agencies took an important step in assisting financial institutions with understanding and evaluating cybersecurity risks and controls. Appendix A is extremely helpful in clarifying Baseline Cybersecurity Maturity statements, as it maps each statement to precise sections of Agency Guidance. However, the remainder of the Assessment leaves much open to interpretation, which will likely differ from institution to institution. If the Agencies plan to utilize the Assessment going forward, consideration should be given to creating an additional Appendix or publishing an FAQ document when institutions request interpretation on specific items. Distribution of the information would ensure consistent use of the Assessment.

Where the individual Assessment statements are flexible, the Assessment framework is rigid. The Assessment is designed as though the Agencies possess a singular view of cybersecurity programs. For example, the Agencies seem to make the assumption that a central risk group will exist and includes Disaster Recovery, Business Continuity, and Information Security functions. The Assessment needs to allow more variance to account for different organizational structures within financial institutions. What is crucial for purposes of the Assessment is whether or not a financial institution performs a particular function, not necessarily which group carries out the responsibility.

Throughout the Assessment, the "Innovative" category is the most problematic. A large number of statements in this category refer to development of processes or tools for use by the entire financial sector, as well as other critical infrastructures. These statements go beyond what should be expected of financial institutions, and appear to be largely the role of the Agencies and other government entities. While holistic views of cybersecurity risks can prove enlightening, this may not be practical. In addition, groups such as the FS-ISAC already do an excellent job of fostering collaboration on cybersecurity threats sector-wide and across other critical infrastructures.

Certain statements within the Assessment pose specific issues. For instance, the Inherent Risk Profile includes several questions regarding use of applications. Risk levels for these items are defined in terms of fixed numbers, and are not analyzed in perspective of a financial institution's overall application portfolio. A large institution may have a substantial number of cloud providers, but cloud providers may be insignificant in comparison to the total number of applications. On the other hand, a community bank could have few cloud providers, but that small number could comprise the entirety of applications in use. Perhaps it would be prudent to use a percentage evaluation when determining application risk, just as the Agencies have done with money movement activities.

In Domain 3, an institution is asked about its contribution to development of open source. Since open source code presents inherent risk, an institution's maturity level should not be downgraded for failure to undertake this activity. Several statements within Domain 5 should be re-assessed for applicability and value. As an example, most financial institutions would avoid DDoS testing of their own systems, primarily due to the fact that testing in this manner could very likely cause impact to the customer (i.e. system downtime). With regard to incident management, our institution is not aware of any tool that exists which would take automated incident response action. Furthermore, any security system will produce too many false positives for real time direct incident response team involvement.

Upon completion of the Assessment, financial institutions have the ability to determine their cybersecurity maturity. The Agencies should examine whether the information gathered through the Assessment could be anonymized and shared among financial institutions in order to benchmark themselves against similarly sized institutions. Benchmarking would provide institutions the opportunity to further assess areas for improvement.

Overall, the Agencies have largely underestimated the burden of the collection of information necessary to complete the Assessment. The initial Assessment requires an effort much larger than that of 80 hours. Institutions must start by converting the Assessment to a format that can be edited, request feedback from appropriate personnel within the institution, allow time for discussion and follow-up questions, perform gap analysis and vetting, create action plans where needed, and present results to executives. In addition, the ongoing maintenance of ensuring the Assessment is updated on a regular basis, as well as whenever risks change, will require a significant amount of effort. This all contributes to an increasing cost of compliance for financial institutions.

While the Cybersecurity Assessment can be a beneficial tool for financial institutions, the Agencies also recognize the possibility of associated costs. Since the Assessment is relatively new, the compliance and related personnel expenses are difficult to ascertain but are undoubtedly considerable in nature. The largest cost is the time personnel will have to spend completing all aspects of the Assessment, including time commitments to perform ongoing maintenance. Time is quantified in both the cost of hours spent, and also the hours lost executing other duties such as serving customers either directly or indirectly. Finally, financial institutions' costs of compliance will increase at varied rates based on identified gaps unique to each institution. Action plans may require additional personnel, purchase of tools, etc. for remediation. Thus, costs continue to accumulate even after the Assessment is finalized.

It is encouraging that the Agencies are seeking ways to reduce the additional burden the Assessment places on financial institutions. Strong emphasis must be placed on the Agencies' development of an automated tool that would be made available to financial institutions to use and update responses as necessary. In its current published state, the Assessment is not an editable document. This significantly adds to the effort needed for completion. A tool could be structured to require completion of the Inherent Risk Profile, after which an accompanying Cybersecurity Maturity level is automatically assigned based on the answers provided. Then, an institution would only be required to fill out the Cybersecurity Maturity document up to the assigned level. Once a "No" response is provided, the institution would not be allowed to proceed further in that category. If this approach is taken, a gap analysis version should still be made available for institutions to review areas for advancement.

Going forward, the Agencies should conduct a comparison analysis against previously published risk assessments and note where there is overlap. Any duplication should be heavily scrutinized and eliminated wherever possible. If assessments are not combined, a well-designed automated tool could ask a question once and then populate the institution's response in the appropriate places where the question is repeated. This would help reduce the burden of collection on respondent financial institutions.

We appreciate the Agencies' focus on continued improvement and analysis of the effectiveness of the FFIEC Cybersecurity Assessment Tool.

Sincerely,

Jeffrey C. Weeks
VP & CISO, Information Security