From: Baechle, Lisa A on behalf of Burch, Robert C
To: PRAINFO; oira_submission@omb.eop.gov
Subject: Comments submission for the FFIEC Cybersecurity Assessment Tool
Date: Friday, January 15, 2016 4:14:02 PM

Ladies and Gentlemen:

KeyBank National Association ("KeyBank") appreciates the opportunity to comment on the notice and request for comment ("Notice") concerning the renewal of the information collection titled "FFIEC Cybersecurity Assessment Tool," which was issued by the Office of the Comptroller of the Currency ("OCC") on behalf of the federal banking agencies (the "Agencies") and published in the December 16, 2015 issue of the Federal Register. KeyBank is a wholly-owned subsidiary of KeyCorp, one of the nation's largest bank-based financial services companies with assets of approximately $94 billion.

Domain Maturity Level Assessment Comments

Currently, the tool is a series of yes/no questions. This is not a flexible format and understates a financial institution's true cybersecurity preparedness for the following reasons:

- For any given maturity level, all questions must have a "yes" answer prior to moving to the next maturity level. Elevation to the next level is not possible if only one question has a "no" answer, even when controls from a higher maturity level are implemented and can offset or mitigate items not being done at a lower maturity level.
- Some questions do not provide for a risk based answer. Instead, the question implies that the control must be implemented 100% of the time, for all situations, even if the risk does not merit this level of protection. Implementing a control without first considering risk may not be realistic and/or financially feasible.
- A yes/no answer does not provide an accurate representation of a financial institution's maturity level. Instead, an answer should be provided in terms of "percentage of readiness". For example, to say that a control is 80% implemented is more accurate than having to answer no (implying 0%) to a question because the control is not fully implemented.
- Because comments are not required when answering a question, it is not possible to justify the answer.
- There is no consideration given for substituting an equivalent compensating control when answering "no" to a question.

Inherent Risk Profile Assessment Comments

The answers to questions in the Inherent Risk Profile assessment range from 1 – 5. This format limits the ability to calculate an accurate representation of risk for the following reasons:

- The FFIEC Guidance does not provide a clear process for determining the overall inherent risk rating when the totals for each category can be spread across the five risk levels.
- Some judgment is required for a final decision.
- The External Threat category contains only one question. This category should be further developed and divided into more questions, e.g., a question on phishing, a

question on DDoS.

General Comments

Due to the large amount of questions, performing this assessment requires a significant amount of time and resources to analyze and complete. This is further compounded by the vagueness of many of the questions. More definition and clarification of specific terms used in the questions are needed.

Though this assessment is voluntary, it appears that it will be used by the OCC examiners as part of the exam process. As a result, the expectations on how this tool will be used and how "completed and acceptable" are defined are unclear.

KeyBank thanks the OCC and the Agencies for the opportunity to comment on the Notice and respectfully asks for consideration of our recommendations and suggestions. If you have any questions, please do not hesitate to contact me.

Sincerely,

Robert C. Burch
Chief Information Security Officer
Key Bank – Enterprise Security Services
robert_c_burch@keybank.com
(216) 813-3258