September 15, 2015

Legislative and Regulatory Activities Division,
Office of the Comptroller of the Currency,
Attention: 1557-0328

prainfo@occ.treas.gov
Office of the Comptroller of the Currency

Re: FFIEC Cybersecurity Assessment Tool

Thank you for the opportunity to comment on the FFIEC Cybersecurity Assessment Tool that was released in July of 2015. After our evaluation of the tool, we have made a couple of observations that we would like share as part of this response period.

It appears the tool is designed to identify inherent risk at the enterprise level through the use of the profile questionnaire. While users are given the flexibility to weight specific portions of the questionnaire, this "enterprise approach" does not seems to match with the maturity levels evaluated at the process level or "component" as referred to within the tool. This unequal comparison seems inconsistent with traditional risk assessment methodologies. Typically, an organization would identify the inherent risk at the process/component level, determine the control effectiveness or maturity level, and then develop an action plan to move the process/component to an acceptable level of residual risk or target maturity level.

While the tool does have various categories of risk within the inherent risk profile, it does not seem that the inherent risk for a specific category is meant to be considered against the maturity level of a specific domain. For example, the inherent "organizational characteristics" risk is not evaluated directly against the "Cyber Risk Management and Oversight" domain. Adjusting the tool to help an organization assess its inherent risk at the component level could provide a more accurate picture rather than a prescriptive maturity level that must be achieved in all domains dependent upon the overall inherent risk.

In addition to the overall methodology, we have also made observations regarding the declarative statements used within the tool. Based on the guidance within the tool, all declarative statements have to be met in order for a maturity level to be considered achieved. This does not seem to allow for an organization to have flexibility when maturing its processes or reducing its residual risk. Allowing for compensating controls that may or may not be specifically listed within the tool could provide such flexibility.

Finally, we observed that the declarative statements were especially prescriptive in their descriptions and yet were open for interpretation. For example, in the area of Access and Data Management, an Intermediate level statement includes, "Controls are in place to prevent unauthorized escalation of user privileges". This statement could be interpreted in multiple ways. An organization could have controls in place that would only allow provisioning of access that

commensurate with a user's job responsibilities. This declarative statement could also be interpreted to mean a specific tool or function within the system will prevent escalation of privileges. The prescriptive nature of the statement also does not allow for a detective control to be implemented. While we agree preventive controls are preferable, there will be times when an organization will have to rely upon a detective control to mitigate its risk due to the cost of implementing a preventive control.

Overall we feel that the tool provides a good opportunity to initiate and/or continue the discussion of cyber security risk with our Board members, and we appreciate the opportunity to offer comments on its development.

Thank you,

David Poczynek
Chief Information Security Officer
BOK Financial and BOKF, NA