



September 18, 2015

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
Attention: 1557-0328
400 7th Street SW, Suite 3E-218, Mail Stop9W-11
Washington, DC 20219

RE: FFIEC Cybersecurity Assessment Tool
OMB Number: 1557-0328

Ladies and Gentlemen:

We appreciate the opportunity to provide comments about the FFIEC Cybersecurity Assessment Tool.

First Tennessee Bank National Association is a regional bank with \$25 billion in total assets as of June 30, 2015. Our 4,300 employees provide financial services through more than 170 bank locations in and around Tennessee. In addition, our FTN Financial Capital Markets division is a capital markets industry leader in fixed income sales, trading and strategies for institutional customers in the U.S. and abroad. The company was founded during the Civil War in 1864 and has the 14th oldest national bank charter in the country.

The Office of the Comptroller of Currency along with other federal agencies and under the auspices of the FFIEC developed the cybersecurity assessment tool to assist financial institutions of all sizes in assessing their inherent cybersecurity risks and their risk management capabilities. We have carefully reviewed the tool and offer the following comments for your consideration.

We are concerned that the assessment tool creates prescriptive expectations for managing cybersecurity risks and will be used in exams to evaluate the effectiveness of cybersecurity programs. While we believe the use of assessment tools is important and support the use of capability and maturity models to determine our level of investment, we would like to understand the use of such a model in a regulatory context. Capability and maturity models are useful as additional sources of input for consideration as management considers risk posture, but should not be used as reference sources by regulators for regulatory examination guidelines.

In the inherent risk model, some of the risk level responses lack clarity in definition or they assume bundled services, both of which force rationalizing and judgment which may impact the accuracy of the calculated inherent risk. For example, the trust services and merchant acquirer activities descriptions lack clarity. As another example, the wire transfer risk levels bundle domestic wires, international wires and wire transfer channel. The statements should be better defined or supporting definitions should be provided.

The maturity model includes 494 declarative statements, categorized into five domains which are further categorized into components and assessment factors. The maturity levels range from baseline to innovative. To achieve a baseline maturity level for a particular domain, an institution has to answer "Yes" to all declarative statements for the various component baselines across all assessment factors for the entire domain. One "No" answer prevents an institution from achieving baseline maturity. In order to achieve a higher maturity level, an institution has to answer "Yes" to all the declarative statements that correspond with that maturity level in a given domain and "Yes" to all lower level declarative statements.

In the maturity model, the use of definitive terms like "All" contradicts the application of protection profiles as defined in the FFIEC Information Security Handbook. Also, some declarative statements that use definitive terms like "All" would appear to be difficult for any financial institution to respond to affirmatively. For example: "All passwords are encrypted in storage and transit." Some declarative statements, including the password example, may be too strong for the associated maturity level.

The prescriptive nature of the cybersecurity maturity level determination ignores compensating controls or activities which may effectively mitigate the cybersecurity risks. Declarative statements become prescriptive since the first "No" sets the maturity level. The methodology does not allow for partial credit for activities conducted above the current maturity level. We disagree with some declarative statements on principle (e.g. antivirus on mobile devices like mobile phones) where we use compensating controls to effectively mitigate the cybersecurity risk.

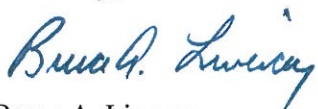
There is a significant amount of subjectivity in the determination of cybersecurity maturity level. As the sophistication of systems and levels of expertise increase, the more likely answers will be nuanced and potentially negative. For example: When a declarative statement begins "Management considers..." how should "considers" be assessed?

The declarative statements require a multi-echelon approach to answer. No single level within an organization will have all of the answers since topics range from the C-suite to the detailed application of technology solutions. This increases the expenditure of resources to complete the assessment.

This assessment represents a new methodology and is time consuming and costly to complete as we question clarity and interpretation of the contents and requirements. If the assessment tool creates prescriptive expectations for managing cybersecurity risks by reducing the level of inherent risks or increasing the maturity level, it could result in significant costs in areas such as business processes, operational controls, and reporting. It could also lead to inaccurate regulatory findings and benchmark comparisons and inappropriate benchmark comparisons.

Once again, we appreciate the opportunity to share our comments.

Sincerely,

A handwritten signature in blue ink that reads "Bruce A. Livesay". The signature is written in a cursive, flowing style.

Bruce A. Livesay
EVP, Chief Information Officer