Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING
2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 /877-276-5554
www.dob.texas.gov

INDUSTRY NOTICE 2015-8
Date: September 15, 2015

Cybersecurity Assessments & the FFIEC Cybersecurity Assessment Tool

As you are all aware, I regard cyber infringements as one of the major threats to the banking industry. Cyber intrusions have become societal in nature and continue to advance and accelerate and are challenging even the most technology savvy bankers. While cyber risks threaten all aspects of our society, the banking industry is a principal target. Therefore, it is important that banks continue to improve management of cyber risks to keep pace with the advancement of cyber threats. This industry notice outlines the Department's expectations regarding cybersecurity assessments.

The Department participated with federal agencies in the development of the Cybersecurity Assessment Tool that was released by the FFIEC on June 30, 2015, as a voluntary method to assist banks in measuring their inherent risks to cyber threats and measuring their cybersecurity maturity (preparedness). There are two parts to the Assessment: (i) an inherent risk profile and (ii) cybersecurity maturity.

- **Inherent Risk Profile -** Identifies the amount of risk posed to a bank by its usage of technology without taking into consideration any mitigating controls. The inherent risk helps identify risks that particularly need enhanced oversight. For example, for an activity that has a high inherent risk, it is important that adequate training be provided to staff and that controls are audited regularly to ensure they are continuing to function. While controls may result in low "residual" risk, should the control fail, the institution will be exposed to high risk.

- **Cybersecurity Maturity -** A five-level path of increasingly organized and more developed processes for controlling risk. "Maturity" refers to the degree of formality of processes. The five levels of maturity are 1) baseline, 2) evolving, 3) intermediate, 4) advanced, and 5) innovative.

Please note the "Baseline Maturity" level consists of statements taken only from existing regulatory guidance. Therefore, there is a regulatory expectation that all banks will achieve at least this "base" level of cybersecurity maturity. The Baseline Maturity statements can be found in Appendix A of the FFIEC Cybersecurity Assessment Tool webpage. The appropriate level of cybersecurity maturity for a bank, which may be higher than "baseline", depends on its inherent risk. Starting with a review at the baseline level is a good first introductory step for most community banks.

Although the Cybersecurity Assessment Tool is a voluntary method for banks to use, measuring risk and preparedness have never been optional elements of banking. Therefore, due to the

advanced and increasing trend of cyber threats to the banking system, the Department is requiring that all banks measure their inherent cyber risks and cybersecurity maturity (preparedness) by December 31, 2015.

Although there are a number of methods for achieving this mission, the Department encourages banks to use the FFIEC Cybersecurity Assessment Tool, as it is the only methodology specifically designed for the banking industry, particularly community banks. Estimates are that it takes approximately 50 to 60 hours for a multi-billion dollar bank to complete. Less time will be needed by smaller banks. It is designed to be completed by community banks without the need to hire consultants. An additional reason for utilizing the Cybersecurity Assessment Tool is that the FFIEC also developed an Overview for CEOs and Directors document that is particularly helpful for community banks to implement a cybersecurity assessment program.

For banks that prefer using an automated method for documenting their answers, instead of manually recording them on a paper document, a free automated version is in development by the FS-ISAC in cooperation with industry trade associations. The electronic version of the Cybersecurity Assessment Tool is expected to be available in late September. Contact your trade association or FS-ISAC for more information. Additionally, private firms are also offering free automated versions. At this time the Department has not reviewed these products and makes no representation to their completeness.

If your bank has been using or prefers to use a different method that achieves the same goals as the FFIEC Cybersecurity Assessment Tool, such as the NIST Cybersecurity Framework, please contact our staff to discuss this or any other method as an option.

Our examination staff will begin reviewing completed cybersecurity assessments starting January 1, 2016. Also, because of the continued rapid advancements in cyber threats, the normal 18 month examination cycle is too long to wait. Therefore, we will be reviewing assessments during normal-on-site examinations and as part of our off-site review process. If your bank is selected for an off-site review, you will be contacted to submit your completed assessment to our examination staff on or after January 1, 2016.

These are challenging times and the Department seeks your cooperation in making the delivery of financial services as safe as possible to the consumers of our great state. If you have any questions, please contact our Chief IT Security Examiner Linda Pearson via email or at 210-271-3923.

Sincerely,
/s/
Charles Cooper