



THE COMMONWEALTH OF MASSACHUSETTS
DIVISION OF BANKS
1000 Washington Street, 10th Floor, Boston, Massachusetts 02118

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

JOHN C. CHAPMAN
UNDERSECRETARY

DAVID J. COTNEY
COMMISSIONER OF BANKS

November 30, 2015

Cybersecurity Assessments & the FFIEC Cybersecurity Assessment Tool

To the Chief Executive Officer of the Institution Addressed:

As you are all aware, cyber attacks are one of the major threats to the financial services industry. Cyber intrusions have become societal in nature and continue to advance and accelerate, challenging even the most technology savvy business leaders. While cyber risks threaten all aspects of our society, the financial services industry is a principal target. Therefore, it is critical that entities continue to improve management of cyber risks to keep pace with the advancement of cyber threats. This message outlines the Division of Banks' (Division) expectations regarding cybersecurity assessments.

The Division participated closely with federal agencies in the development of the Cybersecurity Assessment Tool that was released by the Federal Financial Institutions Examination Council (FFIEC) on June 30, 2015, as a voluntary method to assist institutions 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 an entity by its usage of technology without taking into consideration any mitigating controls. The inherent risk profile helps identify particular risks that 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 entities 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 found at <https://www.ffiec.gov/cyberassessmenttool.htm>. The appropriate level of cybersecurity maturity for an

November 30, 2015

Page 2

entity, 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 institutions.

Although the Cybersecurity Assessment Tool is a voluntary method for entities to use, measuring risk and preparedness have never been optional elements for banks or financial service providers. Therefore, due to the advanced and increasing trend of cyber threats to the financial system, the Division is strongly encouraging all non-depository institutions to measure their inherent cyber risks and cybersecurity maturity (preparedness) preferably by March 31, 2016, and by June 30, 2016 at the latest.

While there are a number of methods for achieving this mission, the Division encourages institutions to use the FFIEC Cybersecurity Assessment Tool, as it is the only methodology specifically designed for the financial services industry. Estimates are that it takes approximately 50 to 60 hours for a multi-billion dollar institution to complete. Less time will be needed by smaller entities. **It is designed to be completed without the need to hire consultants.** The FFIEC also developed an *Overview for CEOs and Directors* document that is particularly helpful for institutions to implement a cybersecurity assessment program.

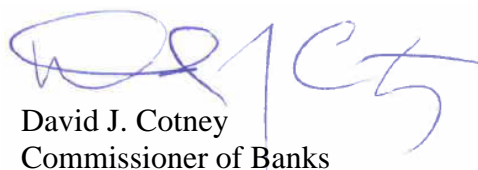
For those that prefer using an automated method for documenting their answers instead of manually recording them on a paper document, a free automated version was recently released by the Financial Services Sector Coordinating Council (FSSCC) which was developed in cooperation with industry trade associations. The electronic version of the Cybersecurity Assessment Tool can be found at <https://www.fsscc.org/eweb/startpage.aspx>. Additionally, private firms are also offering free automated versions. Please note that the Division has not reviewed these products and makes no representation relative to their completeness.

If your institution 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 feel free to contact our staff to discuss this or any other method as an option.

Our examination staff will begin reviewing completed cybersecurity assessments starting July 1, 2016.

These are challenging times and the Division seeks your cooperation in making the delivery of financial services as safe as possible to Massachusetts consumers. At the same time, we recognize the added efforts required of you and your staff and our goal is to serve as a resource as you assess your preparedness. If you have any questions, please contact Deputy Commissioner Kevin Cuff at kevin.cuff@state.ma.us.

Sincerely,



David J. Cotney
Commissioner of Banks