BUREAU OF FINANCIAL INSTITUTIONS
Department of Professional and Financial Regulation
State of Maine
October 16, 2015

Bulletin #80 Cybersecurity Assessments & the FFIEC Cybersecurity Assessment Tool

To the Chief Executive Officer Addressed:

Cyber infringements are considered one of the major threats to the financial 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 financial industry is a principal target. Therefore, it is important that financial institutions continue to improve management of cyber risks to keep pace with the advancement of cyber threats. This Bulletin outlines the Bureau's expectations regarding cybersecurity assessments.

The FFIEC developed a Cybersecurity Assessment Tool that was released on June 30, 2015 as a voluntary method to assist financial institutions in measuring their inherent risks to cyber threats and measuring their cybersecurity maturity (preparedness). The Assessment Tool was designed to provide institutions a repeatable and measurable process for assessing their cybersecurity risks and preparedness over time. It is recommended that you begin with the **Overview for Chief Executive Officers and Boards of Directors** document, which is a high level summary. 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 financial institution by its usage of technology without taking into consideration any mitigating controls. The inherent risk profile 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 financial institutions 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 financial institution, which may be higher than "baseline," depends on its inherent risk. Generally, starting with a review at the baseline level is a good first introductory step for most community institutions.

While an institution's use of the Assessment Tool is voluntary, the Bureau encourages institutions to use the Tool, as it has been specifically designed for the banking industry. It is designed to be completed by community financial institutions without the need to hire consultants.

Bureau examination staff will begin reviewing and discussing with management completed cybersecurity assessments starting November 1, 2015 during normal on-site examinations. Examiners will not criticize an institution for not using the Assessment Tool, but do expect management to have adopted an equally robust method for assessing the institution's cyber risk and incorporating appropriate cybersecurity measures into its information security program.

The Assessment Tool, including an overview of the Tool's usage and benefits and a user's guide, is available on the Cybersecurity Awareness page of the FFIEC website at http://www.ffiec.gov/cybersecurity.htm. That website also contains several supporting cybersecurity related resources.

/s/ Lloyd P. LaFountain III
Superintendent