


MEMORANDUM

TO: Chief Executive Officers of All Alabama, State-Chartered Banks

FROM: John D. Harrison
Superintendent of Banks 

SUBJECT: Cybersecurity Risk Management & the FFIEC Cybersecurity Assessment Tool

DATE: January 4, 2016

Over the last year, the Alabama State Banking Department (Department) has participated with other State and Federal agencies to heighten awareness among bank directors and CEOs of the risks associated with cyberattacks and threats. The frequency and sophistication of cyberattacks against financial institutions continue to grow, and a successful attack can cause considerable financial, legal, and reputational risk to banks and their customers. Consequently, the Department reminds all Alabama, State-Chartered banks that cybersecurity is an issue that should be addressed at the Board, senior executive, and CEO level. Executive leadership is critical to ensure sufficient resources are available to address emerging threats. This memorandum outlines the Department's minimum expectations regarding cybersecurity and cyber risk management programs.

On all safety and soundness examinations conducted by the Department, examiners will be discussing and reviewing cyber-related issues with management. Specifically, examiners will be reviewing:

- Whether the bank actively participates in an information and threat sharing organization such as the Financial Services – Information Sharing and Analysis Center (FS-ISAC);
- Third-party service provider/vendor management policies and practices;
- Cyber Resilience/Disaster Recovery plans;
- The overall level of Director involvement, as indicated by a review of the Board minutes;
- Training and awareness programs for Directors, employees, and bank customers; and
- Policies and practices related to software updates/patches.

In addition, Department examiners will make inquiries, at each examination, regarding banks' efforts in conducting cybersecurity risk assessments. The Cybersecurity Assessment Tool that was released by the FFIEC on June 30, 2015, is a helpful, 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 for an activity with high inherent risk, 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:

<https://www.ffiec.gov/cyberassessmenttool.htm>. 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) effective immediately.

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. The FFIEC Cybersecurity Assessment Tool also includes 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. 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 as to their completeness.

Our examination staff will begin reviewing completed cybersecurity assessments starting with examinations beginning on or after July 5, 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 also review cybersecurity assessments 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 July 5, 2016.

The Department encourages each Alabama State-Chartered Bank to review its current policies and practices for appropriateness. Cybersecurity should be a regular item on Board agendas, and discussions should be documented in minutes. In addition, the Department strongly recommends that each bank actively participate in a threat and information sharing organization such as the FS-ISAC. Cybersecurity remains a major challenge for banks and regulatory agencies, and we must all work together to better protect the industry against attacks. If you have any questions or need further information, please contact Supervising Review Examiner Jesse Hudson at (334) 242-3553, jesse.hudson@banking.alabama.gov; Division Manager Nelson Cook at (334) 242-3547, nelson.cook@banking.alabama.gov; or Deputy Superintendent Trabo Reed in our office at 334-242-3507, trabo.reed@banking.alabama.gov.