Introduction to Federal Financial Institutions Examination Council's

Cybersecurity Assessment

Background: In June 2013, the FFIEC established the Cybersecurity and Critical Infrastructure Working Group (CCWIG) to collaborate on this important issue. This group has been coordinating with intelligence, law enforcement, Homeland Security, and industry officials to make sure the member agencies have accurate and timely threat information to assist institutions in protecting themselves and their customers from the growing risk posed by cyber-attacks. These activities are part of a broad FFIEC cybersecurity awareness initiative that covers institutions of all sizes and complexity. The FFIEC is currently focusing on providing resources to support community institutions that may not have access to the resources available to larger institutions. In light of the increasing volume and sophistication of cyber threats, the FFIEC members are piloting an exam work program (Cybersecurity Assessment) designed for federal and state banking regulators to assess the vulnerability of community institutions to cyber threats and their preparedness to mitigate cyber risks.

What is the Cybersecurity Assessment?

The Cybersecurity Assessment builds upon key aspects of existing supervisory expectations addressed in the *FFIEC IT Handbook* (http://ithandbook.ffiec.gov/it-booklets.aspx) and other regulatory guidance and also:

1. Assesses the complexity of an institution's operating environment, including the types of communication connections and payments initiated, as well as how the institution manages its information technology products and services.
2. Assesses an institution's current practices and overall cybersecurity preparedness, with a focus on the following key areas:
    - Risk Management and Oversight
    - Threat Intelligence and Collaboration
    - Cybersecurity Controls
    - External Dependency Management
    - Cyber Incident Management and Resilience

The Cybersecurity Assessment supplements existing examination work planned for each institution participating in the pilot. Therefore, if examiners find issues or have concerns that require attention (e.g., practices that do not meet existing legal requirements or supervisory expectations) while conducting their normal examination work; they will inform the institution and communicate necessary corrective action. It is important to note that the pilot Cybersecurity Assessment does not impose new expectations for institutions, nor will it result in any new examination rating.

The Cybersecurity Assessment will help the FFIEC member agencies make risk-informed decisions to identify and prioritize actions to enhance the effectiveness of cybersecurity-related supervisory programs, guidance and examiner training. It will also be beneficial in identifying actions that can strengthen their overall level of preparedness and ability to address the evolving and increasing cybersecurity threats.