Farm Credit Administration

1501 Farm Credit Drive
McLean, Virginia 22102-5090
(703) 883-4000

INFORMATIONAL MEMORANDUM

December 16, 2014

To: Chairman, Board of Directors
Chief Executive Officer
All Farm Credit System Institutions

From: Samuel R. Coleman
Director and Chief Examiner
Office of Examination

Subject: Cybersecurity Framework and Other Recent Guidance

The purpose of this Informational Memorandum (memorandum) is to ensure Farm Credit System Institutions are aware of best practices and recent guidance for managing cybersecurity risk. All System institutions should be taking appropriate actions to monitor and maintain awareness of cybersecurity threats and vulnerabilities.

Underlying Federal Policy and Executive Order

On February 12, 2013, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The Order established that "it is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." The Order called for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

In February 2014, the National Institute of Standards and Technology issued the attached guidance describing the Framework and how an entity might use the Framework for understanding, managing, and expressing cybersecurity risk. The guidance includes the Framework Core, which is a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes.

Applicability to the Farm Credit System

Given the importance of the Farm Credit System to Rural America and the financial sector, FCA believes that all System institutions should review this Framework as a best practice for evaluating cybersecurity risks within their respective operating environments. Cyber-attacks continue to increase exponentially. These attacks have resulted in the loss of customer personally identifiable information (PII), as well as financial account information (banking, credit card, etc.). As a result, many financial institutions have experienced increased financial loss and reputation risks as a result of cyber-attacks and inadequate controls for handling customer PII.

FFIEC Assessment and Recommended Practices for FCS Institutions

On November 3, 2014, the Federal Financial Institutions Examination Council (FFIEC) released the attached Cybersecurity Assessment General Observations and recommended all regulated financial institutions participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FFIEC assessment found that the level of cybersecurity inherent risk varies significantly across financial institutions; and, it is important for institutions' boards and management to understand the inherent risk to cybersecurity threats and vulnerabilities when assessing cybersecurity preparedness. Cybersecurity inherent risk is defined as "the amount of risk posed by a financial institution's activities and connections, notwithstanding risk-mitigating controls in place."

The FFIEC made some general observations that the FCA believes are appropriate for all System institutions to implement within their organizations:

- Engage boards of directors and senior management to ensure they understand their institutions' cybersecurity risks;
- Routinely discuss cybersecurity issues in meetings;
- Monitor and maintain sufficient awareness of threats and vulnerabilities throughout the organization;
- Establish and maintain a dynamic control environment;
- Manage connections with and to third parties; and
- Develop and test business continuity and disaster recovery plans that incorporate cyber-incident scenarios.

In addition, the FFIEC's assessment contains sound and constructive questions that System boards and management should ask themselves relative to their own cybersecurity preparedness.

The previously discussed Framework and subsequent FFIEC assessment are best practices that System institutions should incorporate into their risk management processes. In addition, System institutions are encouraged to participate in FS-ISAC or similar organizations in order to

monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so that they may evaluate risk and respond accordingly.

If you have questions about this memorandum, please contact your Examiner-in-Charge or Operations Risk Program Manager Michael Anderson at (720) 213-0909 or by email at andersonm@fca.gov.

Attachments