Farm Credit Administration

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

INFORMATIONAL MEMORANDUM

August 5, 2015

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

From: Samuel R. Coleman
Director and Chief Examiner

Subject: Cybersecurity Assessment and Expectations for System Institutions

The purpose of this Informational Memorandum is to ensure Farm Credit System institutions are aware of recent guidance concerning cybersecurity risks, as well as the Farm Credit Administration's (FCA) expectations related to cybersecurity. Cybersecurity attacks have exponentially increased over the past two years which emphasizes the importance of maintaining sound internal controls. On December 16, 2014, the FCA provided institutions with guidance for establishing a cybersecurity framework utilizing industry standards and best practices. This guidance also communicated general observations from the Federal Financial Institutions Examination Council (FFIEC) members' examination activities related to cybersecurity.

Recent FFIEC Cybersecurity Guidance

On March 30, 2015, the FFIEC released two statements about ways financial institutions can identify and mitigate cyber attacks that compromise user credentials or use destructive software, known as malware. More recently, on June 30, 2015, the FFIEC released guidance on a Cybersecurity Assessment Tool to help institutions identify their risks and assess their cybersecurity preparedness. This assessment tool provides institutions with a repeatable and measurable process to inform boards and management of their institution's risks and cybersecurity preparedness.

Applicability to the Farm Credit System

Institutions should view this guidance as best practices for evaluating cybersecurity risks within their operating environment. Boards and management should be aware of this information and should ensure appropriate actions are taken to maintain sufficient internal controls. This includes appropriate policies, procedures, and operating practices that mitigate financial, operational, legal, and reputational risks associated with cybersecurity threats and

vulnerabilities. Layered security controls are necessary to mitigate potential risks that include: loss of the confidentiality and integrity of sensitive data, the potential for operational disruptions, and the increased risk of fraudulent financial transactions. Moreover, standard operating practices that were considered acceptable in the past may no longer be a viable solution and could increase operational risks today. This includes maintaining operating systems and applications that have known vulnerabilities and are either losing support or are no longer supported by their vendor.

Consistent with regulatory and FFIEC guidance, institutions should take the following actions to ensure cyber threats are appropriately managed:

- Conduct ongoing information security risk assessments;
- Perform security monitoring, prevention, and risk mitigation;
- Protect against unauthorized access;
- Implement and test controls around critical systems regularly;
- Enhance information security awareness and training programs; and,
- Participate in industry information-sharing forums.

Compliance with the FFIEC guidance is not required; however, the absence of sound internal controls within an institution's operating environment will be identified as a safety and soundness concern. Our examination program incorporates these best practices discussed in the guidance in our evaluation of institutions' cybersecurity preparedness.

Links to FFIEC Guidance

The following links contain information on the FFIEC's Risk Assessment Tool and other regulatory guidance that can assist institutions in evaluating their cybersecurity preparedness:

- Cybersecurity Assessment Tool - June 30, 2015
- FFIEC Statements on Compromised Credentials and Destructive Malware - March 30, 2015
- FFIEC Observations From Recent Cybersecurity Assessment - November 3, 2014

If you have questions about this Informational 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.