Farm Credit Administration

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

INFORMATIONAL MEMORANDUM

October 23, 2019

To: Chair, Board of Directors
Chief Executive Officer
Each Farm Credit System Institution

From: Roger Paulsen, Director and Chief Examiner
Office of Examination

Subject: National Oversight Plan for Fiscal Year 2020

The Farm Credit Administration's Office of Examination establishes a National Oversight Plan (NOP) as part of our annual planning processes. The plan identifies the risk topics FCA examiners will emphasize in their examination and oversight activities for the fiscal year.

We issue this informational memorandum each year to notify Farm Credit System (System) institutions about our concerns, priorities, and resulting NOP risk topics so you can consider them in your risk assessment and business planning processes. Based on our assessment of current conditions, we identified three risk topics for 2020:

- Lending controls
- Governing the third line of defense (internal audit)
- Cybersecurity and emerging threats

We are aware that many boards of directors and management teams carefully assess the impact of these issues on their institutions' financial and portfolio condition, resource needs, and strategic plans. We encourage you to continue to have challenging conversations around these topics. We also encourage you to discuss this memorandum with your examiner-in-charge and other examination staff.

## Lending controls

Economic and credit conditions remain difficult for many System borrowers. Net farm income has been declining for several years and is now projected to be $69 billion in 2020 — nearly 40% lower than the record high in 2013. While payments from the USDA Market Facilitation Program (MFP) have helped many borrowers, a combination of low commodity prices, U.S. trade issues, and weather are all negatively impacting net farm income, borrower financial conditions, and the credit risk profile of some System institutions. The dairy sector, in particular, has experienced significant losses, causing consolidation and liquidations within the industry.

Overall System credit quality remains sound despite these conditions. This is a testament to the System's portfolio diversity and efforts to proactively manage credit risk. It also reflects generally stable land values and the financial resilience of many System borrowers.

As we head into 2020, our examination program will emphasize risk identification in stressed industries and institutions' lending controls. We will particularly emphasize topics such as collecting and analyzing accurate and timely financial information, evaluating carry-over operating debt and repayment capacity projections, and servicing loans to correct weaknesses in borrower credit factors. We will also continue our focus on collateral-related controls including the frequency and depth of evaluations and inspections for loans with increasing risk. Finally, we will take further steps to assess the effectiveness and reliability of automated lending systems used to underwrite loans.

We expect institutions' internal credit review or audit programs to assess and review these areas as needed. We are currently updating our FCA Examination Manual and examination program to better assess and identify an institution's effectiveness in these areas.

### Governing the third line of defense (internal audit)

Our examination program will emphasize board governance over internal controls, with a specific focus on the internal audit program. A few System institutions have encountered credit losses or fraudulent activities that stemmed from, or were made worse by, internal control weaknesses. We often have tied these weaknesses to the lack of effective board governance over controls, the "tone at the top," and the internal audit function. Much of this begins with each board's audit committee functions. As such, we will focus on ensuring your institution has the following:

- A fully functioning and well-trained audit committee empowered to act
- A qualified and independent internal audit provider, which reports directly to the audit committee
- A comprehensive audit universe, risk assessment, and a risk-based audit scope whose depth and breadth are well documented and approved by the audit committee
- A properly documented audit (including audit reports and workpapers)
- A corrective action tracking system for all audit and examination findings
- An ongoing discussion with the internal auditor, contracted auditors, and FCA examiners
- A third-party evaluation or peer evaluation of your audit processes every 3 to 5 years

In 2019, we completed an assessment of our examination program surrounding internal controls. Based on results of that assessment, we are updating our examination guidance and training programs. We also plan to enhance our evaluations of your internal control environment in 2020 and beyond.

### Cybersecurity and emerging threats

Information technology-related security threats are growing exponentially. Your institution must understand its inherent cybersecurity threats and vulnerabilities, and the risk these present to your institution's lending and operating activities. In the past, we have shared

information with you to heighten your security awareness. We continue to encourage you to follow these sound business practices:

- Ensure your board and management understand your institution's cybersecurity risks.
- Discuss cybersecurity issues during meetings.
- Promote cybersecurity threat and vulnerability awareness throughout your institution.
- Establish and maintain a strong cybersecurity control environment.
- Manage secure connections with and to third parties.
- Develop and test business continuity and disaster recovery plans that incorporate cybersecurity-incident response scenarios.
- Recruit or appoint directors with information technology expertise.

System institutions reported numerous security incidents in recent years. These incidents reflect a wide range of security risks, including the following:

- Lost and stolen devices (such as laptops and other mobile devices)
- Wire fraud
- Phishing attempts
- Compromised email accounts and credentials
- Release of personally identifiable information (PII)

These incidents are becoming more frequent for businesses and individuals. The trend requires System boards to better understand cyber risks and to ensure that controls protect customer information and ensure safe and sound operations. We will continue evaluating various aspects of your institution's security program and provide guidance as needed.

The first step toward creating a strong cybersecurity control environment is for the board of directors to set the appropriate security culture. That's why every institution director must establish and maintain a secure institution-sponsored email account (or similarly secured communication process) for institution business purposes.

Your institution's email system and its platforms for sharing data and documents should be subject to security and disaster recovery protections that are not available for public email accounts. This will help every board member transact official business with his or her institution, FCA, and others in a secure and confidential manner.

This concludes the summary of our National Oversight Plan for FY 2020. Please distribute it to, and discuss it with, your board members, the audit committee chair, other board committees, and your executive management team. If you have any questions, please contact your designated examiner-in-charge or me at 703-883-4265 (PaulsenR@fca.gov).