September 23, 2022

Autumn R. Agans
Deputy Director, Office of Regulatory Policy
Farm Credit Administration
1501 Farm Credit Drive
McLean, VA 22102-5090

Re: Notice of Proposed Rulemaking - 12 CFR Part 609 –- RIN 3052-AD53; *Cyber Risk Management;* 87 Federal Register 45281-45284

Dear Ms. Agans:

The Farm Credit Bank of Texas ("FCBT" or the "Bank") appreciates the opportunity to comment on the Farm Credit Administration's Notice of Proposed Rulemaking regarding Cyber Risk Management ("Proposed Rule") that was published in the *Federal Register* on July 28, 2022.

FCBT welcomes the modernization of the information technology regulations and the replacement of the outdated E-Commerce Plan requirement with a Cybersecurity Risk Management framework. FCBT has particular interest in this area because it provides information technology services, including cybersecurity risk management to its 14 associations.

FCBT participated in the development of the comments submitted by the Farm Credit Council ("FCC") in response to the Proposed Rule and fully supports those comments, which are targeted at improving the Proposed Rule and creating a "principles-based" approach that will hold up over time in a rapidly changing operating environment. In addition to supporting the position of the FCC regarding the Proposed Rule, FCBT would like to highlight the following points of particular significance to it.

The Proposed Rule does not contemplate the varied roles and responsibilities for institutions that receive cyber security services from another System institution.

As noted in the FCC comments, many System institutions receive significant end-to-end information technology services from third-party service providers within the Farm Credit System. This is the case within the Texas District. FCBT provides an array of information technology services to its associations, including front-end applications, back-end processing, network configuration and management, and end user computing and mobile devices. As a result, FCBT is responsible for many aspects of associations' cyber security risk management. For example, FCBT handles vulnerability management for the infrastructure and approved hardware and software it provides to its associations. Similarly, in the context of incident response, in the event of an incident, FCBT would be responsible for any required infrastructure

recovery, restoration, or forensics. There are aspects of cybersecurity that associations cannot be expected to manage given that in some cases, they do not own or manage the underlying information technology infrastructure.

Moreover, some of the Proposed Rule's requirements may not be warranted for an association that receives significant information technology services from a third-party service provider within the System. For example, section 609.930 (c)(6)(ii) requires an independent party to perform testing. For the associations that receive significant information technology services from FCBT, independent testing may not add value.

FCBT respectfully requests that the Proposed Rule address the unique service provider relationship and structure between System entities to minimize examination inconsistencies and omit duplicative or inapplicable requirements.

The Proposed Rule does not sufficiently address differences in size/complexity of institutions.

As the funding bank for associations of varying size, FCBT is keenly aware of the distinctions between the operations of larger and more complex associations and smaller associations. As a result, FCBT fully supports the view that each institution's cyber risk management program will inherently look different depending on the size and complexity of the institution's operations.

However, Section 609.930, which requires each institution to "implement a comprehensive, written cyber risk management program consistent with the size and complexity of the institution's operations" does not include thresholds or offer any additional guidance as to what is expected depending on an institution's size and scope of operations, nor does the rule define the term "complexity."

This lack of guidance or definition of the term "complexity" could lead to inconsistencies and misaligned expectations between examiners and institutions. Without a framework or other guidance quantifying what is expected based on the size and complexity of an institution, an institution that has defined its scope and designed a cyber risk management program to align with its view of the size and complexity of its operations is at risk of having its program interpreted as insufficient or inappropriate by examiners in the field with a differing view. To remedy this, we recommend that the Proposed Rule articulate that the scope and extent of each cyber risk management program be based on a modern risk management framework and aligned with each institution's documented risk-based approach.

Conclusion

FCBT appreciates the opportunity to comment on the Proposed Rule and to present our concerns to FCA for its consideration. We trust that our comments, as well as those comments submitted by the FCC and other System institutions, will assist FCA in its consideration of the Proposed Rule. If you have any questions, please do not hesitate to contact me.

Sincerely,

Nanci Tucker
SVP Corporate Affairs & General Counsel