LONE STAR
AG CREDIT

September 26, 2022

Ms. 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:

Lone Star, ACA appreciates the opportunity to comment on the Farm Credit Administration's ("FCA") Notice of Proposed Rulemaking regarding Cyber Risk Management ("Proposed Rule") that was published in the *Federal Register* on July 28, 2022.

We fully support the comments made by the Farm Credit Council ("FCC") on behalf of Farm Credit System institutions ("System") in response to the Proposed Rule. While we agree with the goal of modernizing the information technology regulations, for the reasons more fully explained in the FCC's comment letter [and herein], we do not believe that the Proposed Rule meets the objective of creating a "principles-based" approach.

In addition to the FCC comment letter, Lone Star submits the following four comments for your consideration:

1. **The Proposed Rule does not align with the "principles based" approach suggested by the FCA.**

The Proposed Rule was introduced as principles-based at the FCA Board meeting in June. However, a true principles-based approach should be designed to outline a set of principles that specify the intention of regulation, rather than a prescriptive set of rules detailing administrative requirements for a System institution's approach.

The Proposed Rule not only sets principles, but also prescribes how to accomplish them (i.e. every identified vulnerability to be remediated, a detailed vendor management process, and specifying the exact content (i.e. metrics) and frequency of board reporting). A narrow focus on prescriptive rules and compliance reporting often leads to the letter of the law being followed while the spirit of the law is missed. To establish a more principles-based approach, we recommend that the Proposed Rule instead refer System institutions to leverage modern

frameworks based on industry standards (e.g. NIST), which each institution may customize for its particular risk environment. We believe this is important in a principles-based regulation and will also allow the regulation to remain relevant in the rapidly changing technology environment. A true principles-based approach will provide guidance and set standards but will also allow for the adoption of necessary advancements in cyber risk management as technology evolves over time.

2. <u>The vendor management requirements are not feasible.</u>

Section 609.930(c)(5)(i) requires an institution to "require its vendors, by contract, to implement appropriate measures designed to meet the objectives of the institution's cyber risk program." Requiring System institutions to require vendors, by contract, to implement appropriate measures per Section 609.930 (c)(5)(ii) is not feasible. Whenever an institution negotiates a vendor contract, it is a matter of risk assessment and business judgment. Some large vendors, because of their size and bargaining position, refuse to negotiate their standard terms and conditions. For example, System institutions are keenly aware they cannot "require" any terms and conditions of Microsoft, a large and critical vendor that provides most operating systems and software for many institutions. For larger vendors like Microsoft, the institution may need to review documentation on the vendor's cyber risk measures for adequacy but may not be able to negotiate them into the contract. Not allowing this flexibility would hamstring institutions' ability to use their business judgment to balance risk while negotiating contracts for critical services. Likewise, some smaller vendors providing low risk services may not be able to implement cyber risk measures — and determining which measures are "appropriate" varies depending on the vendor and service provided. A more workable approach would be to require institutions to "evaluate" cyber risk as part of their vendor management programs.

The monitoring requirements in Section 609.930(c)(5) are also troublesome. It is not consistently feasible to review vendor audits or summaries of test results, per Section 609.930(c)(5)(iii). Some vendors simply will not provide these materials. Requiring institutions to negotiate the right to an audit with every vendor will greatly hinder institutions' choice of vendors. For many vendors, this simply isn't necessary or practical. There is a limited universe of vendors for which reviewing audits or summaries of test results adds value. Finally, requiring a review of audits or summaries of vendor tests results would add significant administrative burden and cost.

3. <u>The Proposed Rule does not explain what it means for programs to be "consistent with the size and complexity of the institution."</u>

We support 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."

The 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. We recommend 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.

We appreciate the FCA's efforts to update the existing information technology regulations and replace the outdated E-Commerce Plan requirement. However, as outlined above, we believe some revisions would make the Proposed Rule clearer and easier to implement and more effective in the rapidly changing technological environment.

Thank you again for the opportunity to comment on the Proposed Rule. We hope that our comments herein, as well as those submitted by the FCC and other System institutions, will assist the FCA in its consideration of the Proposed Rule.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Joe Hayman
Chief Executive Officer