TEXAS FARM CREDIT

September 15, 2022

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

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

Dear Ms. Agans:

Texas Farm Credit Services 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.

Cybersecurity is a risk that all industries face, from which no one is immune, and Texas Farm Credit has dedicated substantial resources to technology and in training to prepare for cybersecurity threats. Texas Farm Credit Services fully supports those comments made by the Farm Credit Council and would like to make the following additional comments regarding the Proposed Rule.

Mitigating "all known vulnerabilities" is not feasible

Without a full understanding of what FCA means when using the term "vulnerability," Texas Farm Credit Services can only apply the prevailing definition: the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally. If Texas Farm Credit were to mitigate "any known vulnerabilities," it would be forced to shut down all operations and methods of communication including email, telephone, and text. Furthermore, human capital is where we are most vulnerable. Without an employee clicking on a link, or opening a file, bad actors are much less likely to infiltrate technology platforms. Knowing where the vulnerabilities lie is not the same as knowing how to mitigate the next mechanism for doing so. It would take a team of industry experts to try and stay ahead of all cybersecurity risks, and once identified, mitigating those risks would essentially render associations unable to perform basic business operations.

Measuring whether an association is doing enough to mitigate those known vulnerabilities is purely subjective. Texas Farm Credit Services has taken, and will continue to take, steps in identifying and mitigating cybersecurity risks and vulnerabilities; however, mitigating "all" vulnerabilities would be cost prohibitive. As such, it is requested that section 609.930(c)(2) of the Proposed Rule be given careful consideration as to the practical implications of the existing wording.

Compliance with industry standards

In addition to the comments in the letter by the Farm Credit Council, Texas Farm Credit has concerns relating to the vagueness of the use of the term "industry standards." Providing guidance as set forth in the Farm Credit Council's letter would ensure that System Associations are making every effort to meet the expectations of the FCA. TFC takes every reasonable measure to reach a gold standard in regard to all areas, but cyber security is a focused effort. Each association has different resources, and industry standards may vary across the System depending on the size of each association, who the technology partners are, and multiple other factors.

Conclusion

Texas Farm Credit Services appreciates the opportunity to comment on the Proposed Rule and asks that the comments stated in the Farm Credit Council's letter, along with the comments presented here, be considered in preparing a final rule relating to cybersecurity.

Respectfully submitted,

Mark A. Miller,
Chief Executive Officer