FARM CREDIT WEST

ADMINISTRATIVE OFFICE
3755 Atherton Road
Rocklin, California 95765
916-780-1166

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:

Farm Credit West, ACA ("FCW") 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.

FCW coordinated with a Farm Credit System (System) workgroup assembled by the Farm Credit Council ("FCC") to evaluate the Proposed Rule. FCW fully endorses the conclusions, recommendations, and requests addressed in the FCC's comment letter. This letter reflects FCW's specific responses to provisions of the Proposed Rule.

General Comments

FCW has long recognized the importance of having appropriate and effective cyber risk programs in place to protect the information assets of our company, our employees, and our customers. FCW conducts its cybersecurity program in conjunction with Financial Partners Inc. ("FPI"), our managed service provider.

In the preamble to this proposed rule, the FCA states that "implementing appropriate risk management strategies means System institutions will demonstrate effective cyber risk governance and continuously monitor and manage their cyber risk within the risk appetite and tolerance approved by their boards of directors." We fully agree with this objective, as it is important for institutions to be able to establish cyber risk programs that are in alignment with the risk tolerance and risk appetite of the board.

Overall, FCW supports FCA's objective to modernize the information technology regulations and replace the outdated E-Commerce Plan requirement with a Cybersecurity Risk Management framework, while maintaining maximum flexibility for System institutions. There are a few sections where the Proposed Rule veers away from principles-based guidance and becomes more

prescriptive than is needed—potentially creating unreasonable expectations, or unintentionally reducing flexibility. FCW's specific observations are listed in the next section.

Specific Concerns

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

The Proposed Rule not only sets out principles, but also prescribes how to accomplish them (e.g. every identified vulnerability to be remediated), and specifying the exact content (i.e. metrics) and frequency of board reporting. This removes our ability to address items in a risk-based fashion. To establish a more principles-based approach, we recommend that the Proposed Rule instead refer system institutions to 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.

The Proposed Rule does not consider the varied role and responsibilities for institutions receiving information technology services from a service provider.

The Proposed Rule does not consider the different operating environment and associated expectations for institutions that receive information technology services from a third-party service provider. FCW receives significant end-to-end information technology services from FPI, including front-end applications, back-end processing, network configuration and management, and end user computing and mobile devices. FCW recognizes that while you can outsource the function, institutions cannot outsource the responsibility to understand and manage the risk. This demands different roles and responsibilities between an association and its service provider. The Proposed Rule should address the unique service provider relationship and structure between some System entities to minimize examination inconsistencies as we have seen in the past.

The Proposed Rule requires an insufficient timeline to report an incident.

Section 609.930(c)(3)(v) requires "[n]otifying FCA as soon as possible or no later than 36 hours" after an incident occurs. The Proposed Rule does not indicate the basis for this specific, prescriptive timeline, which to our knowledge does not align with any other industry or regulatory guidance. Moreover, 36 hours in many cases will not allow an institution sufficient time to review evidence and determine whether a reportable incident has occurred.

FARM CREDIT WEST

ADMINISTRATIVE OFFICE
3755 Atherton Road
Rocklin, California 95765
916-780-1166

The vendor management requirements are not feasible.

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 always 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. Likewise, some smaller vendors providing low risk services may not be able to implement particular cyber risk measures. A more workable approach would be to require institutions to "evaluate" cyber risk as part of their risk-based vendor management programs.

The monitoring requirements in Section 609.930(c)(5) are also troublesome. There is a limited universe of vendors for which reviewing audits or summaries of test results adds value.

Accordingly, we recommend the Proposed Rule allow each institution to define its specific requirements related to vendors, based on its own risk-based vendor management profile and in line with industry practice where vendor contract requirements are tiered based on the services that are provided to that organization.

The Proposed Rule's vulnerability management requirements are not feasible.

Section 609.905 requires an institution to "mitigate any known vulnerabilities." Requiring institutions to mitigate every known vulnerability is not practical nor is it feasible. Also, the term "vulnerability" has not been defined and could lead to inconsistencies and misaligned expectations between examiners and institutions.

Accordingly, we recommend the FCA allows each System institution to define the term "vulnerability" based on a modern framework, removes the requirement that "any" vulnerability is remediated, and allows institutions to rank and prioritize vulnerabilities based on their defined risk-based program, including allowing known unmitigated vulnerabilities to be assessed and addressed based on that risk assessment.

Conclusion

In summary, FCW is deeply committed to ensuring its data assets are well protected. We appreciate FCA's attention to this important matter and the opportunity to provide comments on the Proposed Rule for FCA's consideration. In general, we support FCA's efforts to modernize the information technology regulations and replace the outdated E-Commerce Plan requirement with a Cybersecurity Risk Management framework.

FARM CREDIT WEST

ADMINISTRATIVE OFFICE
3755 Atherton Road
Rocklin, California 95765
916-780-1166

We trust that our comments, as well as those comments submitted by 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.

Respectfully,

John A. Barcelos
Executive Vice President / Chief Risk Officer