 The logo for Yosemite Farm Credit features the words "YOSEMITE", "FARM", and "CREDIT" stacked vertically in a serif font. A green four-leaf clover is positioned to the right of the word "FARM". A brown arc curves over the top of the text, and another brown arc curves under the word "CREDIT".	<p style="text-align: right;"><b>Helping Our Members Prosper!</b></p> <p style="text-align: center;">806 W. Monte Vista Avenue Turlock, CA 95382 P.O. Box 3278 Turlock, CA 95381 Office: (209) 667- 2366 Fax: (209) 634-9612</p> <p style="text-align: center;"><a href="http://www.yosemitefarmcredit.com">www.yosemitefarmcredit.com</a></p>
--	--

September 12, 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

To whom it may concern:

Yosemite Farm Credit appreciates the opportunity to comment on the Farm Credit Administration's Notice of Proposed Rulemaking regarding Cyber Risk Management that was published in the Federal Register on July 28, 2022.

Yosemite Farm Credit supports the comments of the Farm Credit Council and the System Cyber Security Workgroup regarding the ambiguity of terms and lack of definition regarding aspects of the proposed rules.

1. The Proposed Rules do not align with the "principles-based" approach suggested by FCA.
  - a. 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.
  - b. The Proposed Rule not only sets principles but also prescribes how to accomplish them leading us to believe it is more prescriptive.
  - c. We agree that leveraging standard frameworks based on industry standards (e.g., FFIEC, NIST) will allow the regulation to remain relevant for rapidly changing technologies.
  
2. The proposed Rule uses qualitative and subjective language without clear definitions.
  - a. Ambiguity leads to inconsistent implementation and enforcement of rules.
  - b. Words such as "Appropriate", "effective," and "comprehensive" are subjective and could be misinterpreted or applied unevenly.
  - c. We agree with the recommendation to remove these requirements and focus the scope on the association's cyber risk management program based on modern control frameworks and documented risk-based approaches.

- d. This is consistent with a principles-based approach and would allow the implementation of measures commensurate with our size and risk profile.
3. The Proposed Rule does not explain “consistent with the size and complexity of the institution.”
  - a. 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 defined thresholds or additional guidance of what is expected for the size and scope of operations. It also does not define the term “complexity.”
  - b. The lack of guidance or definition could lead to inconsistencies and misaligned expectations between examiners and institutions.
  - c. 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.
4. The Proposed Rule does not consider the varied role and responsibilities of institutions receiving information technology services from a service provider.
  - a. The Proposed Rule does not consider the different operating environments and associated expectations for institutions that receive substantial information technology services (and, by extension, cyber security services) from a third-party service provider within the Farm Credit System.
  - b. The Proposed Rule should address the unique service provider relationship and structure between some System entities to minimize examination inconsistencies.
5. The Proposed Rule does not reference specific industry standards or applicable laws or regulations.
  - a. Section 609.930(b) requires the cyber risk management program to “be consistent with industry standards to ensure the institution’s safety and soundness and compliance with law and regulation.”
  - b. The Proposed Rule does not refer to a particular industry standard, nor does it articulate which “laws and regulations” the regulator expects System institutions to follow.
  - c. We recommend adding this information to help minimize inconsistencies and misaligned expectations between institutions and examiners.
  - d. Additionally, using the word “ensure” sets an unreasonably high bar for System entities to meet, as examiners may deem a regulatory violation every time there is an incident or breach as it could, in theory, impact “safety and soundness.” We respectfully suggest “ensure” be replaced with the phrase “manage the risk” or similar nomenclature.
  - e. Similarly, Section 609.930(c) requires the cyber risk management program to include “an annual risk assessment.” However, there is no reference to any applicable risk framework. Similarly, Section 609.930(d) requires an institution to “consider privacy and other legal compliance issues” but does not provide expectations on the privacy framework or the other legal or compliance requirements.
  - f. We recommend the Proposed Rule specify that System institutions leverage modern frameworks based on industry standards and recognize modern frameworks must be

customized for that entity's risk environment and consider applicable state and federal law legal requirements in their risk management programs.

6. The Proposed Rule's incident management requirements are unclear and impractical.
  - a. The term "incident" is not defined.
    - i. Section 609.930(c)(3)(i) charges an institution with "assessing the nature and scope of an incident and identifying what information systems and types of information have been accessed or misused," but does not define the word "incident." The Federal Financial Institutions Examination Council's (FFIEC) – IT Handbook – Information Security, which is routinely followed by FCA examiners, does not provide any additional clarity, as it does not define the term "incident" and defines only the terms "Security Event" and "Security Breach." Without a clear definition of what constitutes an "incident," there is likely to be inconsistent reporting among System institutions.
    - ii. We recommend the Proposed Rule incorporate concepts from FCA's June 27, 2017 Informational Memorandum on "[Reporting Security Incidents and Business Continuity Events to FCA](#)," which already includes a definition of security incidents that may affect an institution's operations, reputation, or sensitive customer information.
  - b. The timeline provided to report an incident is insufficient.
    - i. Section 609.930(c)(3)(v) requires "notifying 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, incidents can occur in an environment without discovery and determination for longer than 36 hours and 36 hours in many cases will not allow an institution sufficient time to review evidence and determine whether a reportable incident has occurred.
    - ii. We respectfully request that this timeline be extended to 72 hours after an incident is determined (in line with recent proposed reporting rules by the National Credit Union Administration) and that the Proposed Rule incorporates concepts from FCA's June 27, 2017 Informational Memorandum on "[Reporting Security Incidents and Business Continuity Events to FCA](#)," which already includes guidance on security incidents that may affect an institution's operations, reputation, or sensitive customer information.
  - c. "Known visitors" and potential customers" is not defined.
    - i. Section 609.930(c)(3)(vi) requires "notifying former, current, or potential customers and employees and known visitors to your website of an incident, when warranted, and in accordance with state and federal laws" – but does not provide definitions of "known visitor" or "potential customer." These terms are subject to varied interpretations and leave System institutions unclear as to when notification is required.

- ii. We recommend the Proposed Rule remove the verbiage related to “former, current, or potential customers and employees and known visitors to a website” and be simply replaced with notification “in accordance with state and federal laws.”
  - d. The Proposed Rule requires detailed procedures for Security Event identification, containment, and resumption.
    - i. Section 609.930(c)(3)(i-iii) requires each institution to document specific procedures on forensics, containment, and business resumption. This requirement is not feasible because the myriad ways Security Events are identified, contained, and then business is resumed are too large to outline in detail in a single document
    - ii. We recommend the Proposed Rule be reworded to focus less on specific procedures, and more on an adaptable and scalable framework to assess the nature/scope of an incident, contain the incident, and safely resume business activities.
- 7. Vendor management procedures are not feasible.
  - a. 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 that they cannot “require” any terms and conditions of Microsoft. This large and critical vendor provides the majority of operating systems and software for many institutions. For more significant vendors like Microsoft, the institution may need to review the documentation on the vendor’s cyber risk measures for adequacy. Still, it 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 require institutions to “evaluate” cyber risk as part of their vendor management programs.
  - b. 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. Moreover, for many vendors, this simply isn’t necessary or practical. For example, it is not necessary for an institution to review audits or summaries of test results for a vendor contracted to provide catering or lawn maintenance services. 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 test results would add a significant administrative burden and cost. Most institutions have hundreds of vendors, making it unfeasible for institutions to review audit results and tests for each of these vendors.

- c. 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 provided to that organization.
8. Vulnerability management requirements are not feasible.
    - a. Section 609.905 requires an institution to “mitigate any known vulnerabilities.” Requiring institutions to mitigate every known vulnerability is not feasible. The term “vulnerability” has not been defined and could lead to inconsistencies and misaligned expectations between examiners and institutions. A vulnerability could be surfaced through a network scanning tool, a qualitative risk assessment, or through general discussion at an institution, and may have varying levels of severity associated with it. Additionally, Section 609.930(c)(2) of the Proposed Rule allows an institution to adopt security measure based on its “nature and scope” of activities, but that language is not consistent with Section 609.905.
    - b. 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.
  9. Business Plan requirements do not align with established business processes.
    - a. Section 609.935(2) requires an institution to “detail the technology budget in the technology plan.” Some institutions present their technology budgets to their boards in conjunction with the overall operating expense budget, while other institutions present a business plan (with a technology plan component) but may not separate and display technology budget details. Requiring the budget to be separated would add unnecessary duplication and potential confusion in many System institutions.
  10. Various provisions of the Proposed Rule are ambiguous and open to multiple interpretations.
    - a. Section 609.930(c)(6)(i) on internal controls requires an institution to “determine the frequency and nature of the tests.” However, it provides no substantive guidance regarding how the institution’s risk assessment should guide the frequency and nature of testing. Similarly, § 609.930(c)(6)(iii) indicates that “Internal systems and controls must provide reasonable assurances that System institutions will prevent, detect, and remediate material deficiencies on a timely basis,”; however, there is no indication of how this will be measured, and there is no definition of the term “material.” In addition, “reasonable assurance” seems to refer to an auditor's degree of satisfaction the evidence obtained during the performance of the audit supports the assertions embodied in the financial statements. “Reasonable assurance” does not include

"remediation" in the definition, as a situation with material deficiencies (situations requiring remediation) would not allow an auditor to arrive at a level of reasonable assurance. We recommend separating this section into a testing element and a remediation element; a testing element related to "reasonable assurance" would assess the cyber capabilities of the organization to detect and prevent cyber-incidences of a material nature, while a remediation element related to incident response would assess the effectiveness of timely remediation of cyber-incidents that have a material impact on the entity.

- b. Section 609.930(e) requires an institution to "report quarterly to its board or an appropriate committee" but does not provide the reasoning or understanding of what is driving this frequency. This may or may not be the correct frequency to inform a particular institution's Board.
- c. Section 609.930(e) requires the report to "contain material matters and metrics related to the institution's cyber risk management program, including specific risks and threats" but does not provide a framework or expectation for the metrics that are being presented to the Board, or consider institutions providing cyber metrics through another avenue, such as an entity-wide Risk Management Report. This could lead to inconsistencies and misaligned expectations between examiners and institutions; where the institution has defined their scope, but this could be interpreted as insufficient or inappropriate by examiners in the field as the proposed rule does not reference a framework or other guidance to quantify the sufficiency of the program.
  - i. We recommend the Proposed Rule instead refer System institutions to leverage modern frameworks based on industry standards, customized for its institution's risk environment, and aligned with its documented risk-based approach when defining the manner, scope, and formatting of board reporting.
- d. Section 609.935(3) requires institutions to identify and assess the "business risk of proposed technology changes and assesses the adequacy of the institution's cyber risk program." However, it is unclear if this requirement is to assess the adequacy of the program as a whole or because of the proposed technology changes only.
- e. Section 609.945 requires "records stored electronically must be accurate, accessible, and reproducible for later reference," but is silent on the scope and extent of the records, or any considerations to the institution's Data Retention policies. For instance, is this specific to loan documentation, or for 100% of logs from every single machine connected to the network? This could lead to inconsistencies and misaligned expectations between examiners and institutions. For example, an institution's defined scope could be interpreted as insufficient or inappropriate by examiners in the field because the Proposed Rule does not provide any guidance as to which electronic records this section applies to.
  - i. We recommend the Proposed Rule instead refer System institutions to leverage modern frameworks based on industry standards, customized for its institution's risk environment when defining the scope and extent of its electronic records retention program.

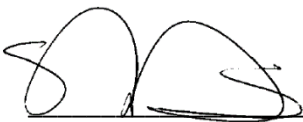
- f. Section 609.930(c)(2) requires institutions to “perform timely remediation” but does not define the term “timely,” which could lead to inconsistencies and misaligned expectations between examiners and institutions.
  - i. We recommend the Proposed Rule instead refer system institutions to leverage modern frameworks based on industry standards, customized for its institution’s risk environment, and aligned with its documented risk-based approach when defining “timely.”
- g. Section 609.930(c)(4) requires institutions to “Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution’s cyber risk program.” The requirement to train contractors and vendors is impractical. Many contractors and vendors will simply refuse to submit to institution-specific training based on their own business requirements. In these instances, System institutions should be able to confirm, either contractually or otherwise, that vendors have some acceptable level of training. It is simply unrealistic for an institution to train all contractors and vendors. We recommend the Proposed Rule be changed to reflect this. Additionally, this section improperly places the burden of implementing the institutions’ cyber risk program on vendors and contractors. While vendors and contractors can be expected to meet basic cyber risk requirements, they are not responsible for implementing an institution’s cyber risk program.

## Conclusion

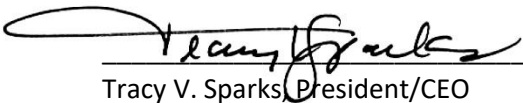
Yosemite Farm Credit has participated in dialog across the System and has provided input and comments to the letter which will be submitted by the Farm Credit Council on behalf of the entire Farm Credit System. We fully endorse and support this letter.

As part of the Farm Credit System, we are committed to providing safe and sound services to our members. We appreciate the opportunity to comment on the Proposed Rule. We continue to support FCA’s efforts to modernize and update the technical regulations and replace the E-Commerce plan with a Cyber Risk Management framework. We hope our comments will assist you in your consideration of the rule.

Respectfully submitted,



Nancy Sill, Board Chair



Tracy V. Sparks, President/CEO