FARM CREDIT COUNCIL

September 19, 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:

On behalf of Farm Credit System ("FCS") institutions, Farm Credit Council ("FCC") appreciates the opportunity to comment on the Farm Credit Administration's ("FCA") Noticed of Proposed Rulemaking regarding Cyber Risk Management ("Proposed Rule") that was published in the *Federal Register* on July 28, 2022.

In order to better analyze the complexities and wide impact of the Proposed Rule and prepare a comment on behalf of all FCS institutions, FCC coordinated with the multi-disciplinary FCS Cybersecurity Workgroup ("Workgroup") of experts from FCS institutions who met over the course of several months to analyze and discuss the Prepublication Copy of the Proposed Rule, the Proposed Rule, existing regulations and relevant FCA-published materials. In addition, FCC also regularly apprised FCS leadership of its efforts regarding the Proposed Rule, including multiple calls with Farm Credit System regulatory professionals to solicit and garner feedback. A draft comment letter was circulated to all FCS institutions for review prior to submitting this final version to FCA.

In summary, the comments in this letter reflect general perspectives on the Proposed Rule, as well as specific comments on specific provisions of the Proposed Rule, based on FCC's review of the Workgroup's feedback, inputs obtained from others in the FCS, and its review and consideration of relevant authorities. Overall, the FCC/System Workgroup supports FCA's objective to modernize the information technology regulations and replace the outdated E-Commerce Plan requirement with a Cybersecurity Risk Management framework. Accordingly, the comments that follow are targeted at improving the FCA's Proposed Rule and creating a "principles-based" approach that will hold up over time in a rapidly changing operating environment.

1. <u>The Proposed Rule does not align with the "principles based" approach suggested by the FCA.</u>

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.

As outlined throughout in this comment letter, 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 throughout this letter 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 Proposed Rule uses qualitative language without clear definitions.</u>

The Proposed Rules uses qualitative, subjective language throughout without providing definitions. The ambiguity could lead to inconsistent implementation of the rule and inconsistent enforcement of the rule. For example, the Proposed Rule uses but does not define or quantify, the following:

> **"appropriate"** – Section 609.905 requires System institutions to "engage in appropriate risk management practices to ensure safety and soundness of their operations," to establish "an appropriate vulnerability management program," and to "establish appropriate reporting mechanisms to the institution's board and FCA," but there is no definition of the word "appropriate".
>
> **"effective" -** Section 609.905 provides that "a System institution's board and management must maintain effective policies, procedures, and controls to mitigate cyber risks," but there is no definition of the word "effective."
>
> **"comprehensive" -** Section 609.930(a) provides that each institution "must implement a comprehensive, written cyber risk management program," but there is no definition of the word "comprehensive".

The words "appropriate," "effective," and "comprehensive," are subjective and would certainly lead to misunderstanding and uneven application. The terms do not give institutions sufficient guidance regarding expectations and could easily lead to inconsistencies among examiners in the field. We recommend the Proposed Rule remove these qualitative requirements and instead articulate that the scope and extent of various aspects of each institution's cyber risk management program be based on modern control frameworks and aligned with its documented risk-based approach. This is consistent with the principles-based approach discussed at the FCA board meeting and would allow entities to implement measures commensurate with their size and risk profile.

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."

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. 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 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 substantial information technology services (and by extension, cyber security services) from a third-party service provider within the Farm Credit System. The majority of institutions within the System receive significant end-to-end information technology services from service providers, including front-end applications, back-end processing, network configuration and management, and end user computing and mobile devices.

The Proposed Rules concerning System vulnerability management in Section 609.930 (c)(3) are especially concerning because they do not consider the specific expectations for these institutions that do not own or operate the underlying technology and infrastructure they use and instead rely on another System institution or third-party service provider. Additionally, Section 609.930 (c)(6)(ii) requires an independent party to perform testing but does not factor in the size and complexity of the institution's operations and whether that requirement is warranted, especially for institutions that receive end-to-end information technology services from third parties.

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.

5. The Proposed Rule does not reference any specific industry standards or applicable laws or regulations.

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." While the reference to industry standards is appropriate in establishing a principles-based rule, the Proposed Rule does not reference to particular industry standard, nor does it articulate which "laws and regulations" the regulator expects System institutions to follow. Adding this information would help to minimize inconsistencies and misaligned expectations between institutions and examiners.

Additionally, use of 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.

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.

We recommend the Proposed Rule specify that System institutions leverage modern frameworks based on industry standards, and that it 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. <u>The Proposed Rule's incident management requirements are unclear and impractical.</u>

a. The Proposed Rules uses, but does not define, the word "incident."

Section 609.930(c)(3)(i) charges an institution with "[a]ssessing 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.

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 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, 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.

We respectfully request that this timeline be extended to 72 hours after an incident is determined (in line with recent proposed reporting rules by both (a) the National Credit Union Administration; and (b) the Cyber Incident Reporting for Critical Infrastructure Act of 2022) and that 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 guidance on security incidents that may affect an institution's operations, reputation, or sensitive customer information.

c. The Proposed Rules does not define "known visitors" or "potential customers."

Section 609.930(c)(3)(vi) requires "[n]otifying 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.

We recommend the Proposed Rule remove the verbiage related to "[f]ormer, current, or potential customers and employees and known visitors to a website" and be simply replaced with notification "[i]n accordance with state and federal laws."

d. The Proposed Rule requires detailed procedures for Security Event identification, containment, and resumption.

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.

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. <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 particular terms and conditions of Microsoft, a large and critical vendor that provides the majority of 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 actually 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 particular 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. 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 tests results would add 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.

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.

8. <u>The Proposed Rule's vulnerability management requirements are not feasible.</u>

Section 609.905 requires an institution to "mitigate any known vulnerabilities." Requiring institutions to mitigate every know 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.

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 allow 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. <u>The Proposed Rule's business plan requirements do not align to established business processes.</u>

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. <u>Various provisions of the Proposed Rule are ambiguous and open to multiple interpretations.</u>

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, Section_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.

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.

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.

Therefore, 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.

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 as a result of the proposed technology changes only.

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.

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.

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.

Again, 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".

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

We appreciate the opportunity to comment on the Proposed Rule and to present FCS institutions' concerns to FCA for its consideration. In general, we support FCA's efforts to modernize the information technology regulations and replace the outdate E-Commerce

Plan requirement with a Cybersecurity Risk Management framework. We trust that our comments, as well as those comments submitted by individual 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,

Robert Paul Boone, III
Senior Vice President and General Counsel
Farm Credit Council