COMPEER FINANCIAL

2600 Jenny Wren Trail
PO Box 810
Sun Prairie, WI 53590

P: (844) 426-6733
F: (507) 344-5144

compeer.com

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:

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

Compeer fully supports and agrees with the comments submitted on this matter by the Farm Credit Council and urges FCA to adopt the Farm Credit Council's position.

In addition, Compeer would like to express its appreciation to FCA for its work on the Proposed Rule, and in particular for its proposed adoption of a principles-based approach to the fast moving and challenging problems of cybersecurity risk management. We appreciate FCA's proposed adoption of a modern, flexible, framework-based regulation.

The advantage of a principles-based approach to cyber risk management (as compared with a more prescriptive rules-based approach) is, of course, that there may be more than one valid way of satisfying the principles expressed in the regulation. While this flexibility is appropriate and appreciated in the highly technical, fast-moving world of cyber risk management, we would ask FCA to minimize examination inconsistency by recognizing (and clarifying in the final rule) the appropriate role of the institution and its board of directors in selecting the appropriate approach from among the many which might satisfy the principles found in the rule. We would also ask that FCA to clarify in the final rule that, when there are multiple practices which satisfy the principles-based approach of the regulation, FCA examination staff will not second-guess an institution's choice of one approach over another.

For example, § 609.930 of the Proposed Rule currently requires institutions to adopt a "comprehensive" cyber risk management program which "ensure[s]" the security and confidentiality of protected information. Unfortunately, perfect security is neither possible nor desirable: there is often a fundamental tradeoff between security and convenience (or user experience). While clients appropriately value the security of their information, they are often willing to accept *some* security risk in exchange for a *better* user experience.

As a cooperative, our member-owners influence these decisions by electing their board of directors each year. After balancing competing desires (such as the trade-offs between cybersecurity and client experience) our board of directors establishes (and we believe should establish) our cybersecurity risk appetite. Compeer's management team is then accountable for developing a cybersecurity risk management program which is consistent with the risk appetite expressed by the board of directors.

We believe that, in a cooperative, this is an appropriate allocation of responsibility as between the board of directors and the management of an FCS institution. We would therefore ask FCA to clarify in the final rule, including in § 609.930, that (1) the role of the board of directors is to *oversee* (as opposed to adopt) the FCS institution's written cybersecurity risk management program and (2) the cybersecurity risk management program may be tailored to the size and complexity of the risks faced by the FCS institution and to the risk appetite expressed by the board of directors (as opposed to adopting a blanket obligation to "ensure" impossibly perfect security and confidentiality).

We also encourage FCA to recognize explicitly in the final rule that, as a matter of administrative law, informal guidance (such as bookletters or "Frequently Asked Questions") may provide FCA's interpretation of an ambiguity in an existing regulation but are not themselves enforceable and may not be used to de facto create or amend specific requirements which are not present in the regulation itself.

In addition, and for similar reasons, we encourage FCA in the final rule to more precisely phrase its expectations for a sound cyber risk management program. For example, the requirement in § 609.930 of the Proposed Rule that an association's cyber risk management must "ensure" the security and confidentiality of protected information is unrealistically absolute and might inadvertently expand an association's liability to third parties in the event of a lawsuit resulting from a data breach or cybersecurity incident. We believe that FCA may not have considered or intended this result. This section, and others like it, should be revised to require only that System institutions make reasonable efforts, consistent with industry standards, to ensure security and confidentiality.

Again, thank you for the opportunity to comment on the Proposed Rule. Overall, we greatly appreciate FCA's work in proposing a modern, flexible, and principles-based approach to cyber risk management.

Sincerely,

Bill Moore
Chief Risk Officer