[6705-01-P]

**FARM CREDIT ADMINISTRATION**

**12 CFR Part 609**

**RIN 3052-AD53**

**Cyber Risk Management**

**AGENCY:** Farm Credit Administration.

**ACTION:** Proposed rule.

**SUMMARY:** The Farm Credit Administration (FCA, we, our, or Agency) proposes to rescind and revise regulations at 12 C.F.R. Part 609 to reflect developments in cyber risk and continuously evolving business practices concerning electronic business (E-business) and to rename Section 609 to Cyber Risk Management.

**DATES:** Comments on this proposed rule must be submitted on or before [INSERT DATE THAT IS 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

**ADDRESSES:** We offer a variety of methods for you to submit comments. For accuracy and efficiency, commenters are encouraged to submit comments by email or through the FCA's Web site. As facsimiles (fax) are difficult for us to process and achieve compliance with section 508 of the Rehabilitation Act, we do not accept comments submitted by fax. Regardless of the method you use, please do not submit your comment multiple times via different methods. You may submit comments by any of the following methods:

- E-mail: Send us an email at reg-comm@fca.gov.
- FCA Web site: http://www.fca.gov. Click inside the "I want to…" field near the top of the page; select "comment on a pending regulation" from the dropdown menu; and click "Go." This takes you to an electronic public comment form.
- Mail: Autumn R. Agans, Deputy Director, Office of Regulatory Policy, Farm Credit Administration, 1501 Farm Credit Drive, McLean, VA 22102-5090.

You may review copies of all comments we receive at our office in McLean, Virginia, or on our Web site at http://www.fca.gov. Once you are in the Web site, click inside the "I want to…" field near the top of the page; select "find comments on a pending regulation" from the dropdown menu; and click "Go." This will take you to the Comment Letters page where you can select the regulation for which you would like to read the public comments. We will show your comments as submitted, but for technical reasons we may omit some items such as logos and special characters. Identifying information that you provide, such as phone numbers and addresses, will be publicly available. However, we will attempt to remove e-mail addresses to help reduce Internet spam.

**FOR FURTHER INFORMATION CONTACT:**

Technical information: Dr. Ira D. Marshall, Senior Policy Analyst, Office of Regulatory Policy, Farm Credit Administration, McLean, VA 22102-5090, (703) 883-4414, TTY (703) 883-4056.

Legal information: Jane Virga, Assistant General Counsel, Office of General Counsel, Farm Credit Administration, McLean, VA 22102-5090, (703) 883-4020, TTY (703) 883-4056.

**SUPPLEMENTARY INFORMATION:**

## I. Objectives:

Our objectives in this proposed rule are to:

- Delete references to the requirements of "Electronic Signatures in Global and National Commerce Act" (E-SIGN) (Pub. L. 106-229), which became effective October 1, 2000. E-SIGN governs transactions relating to the conduct of business, consumer, or commercial affairs between two or more persons. We also propose to delete references to the Federal Reserve Board (FRB) Regulations B, Z, and M. These laws apply to the Farm Credit System (System) regardless of citation in Part 609. Thus, we believe that these references are no longer necessary.
- Revise Part 609 to codify existing expectations and ensure the relevance and adequacy of risk management

practices, corporate governance, and internal control systems for conducting business in an electronic environment.

## II. Background

The regulations at 12 C.F.R. Part 609 were enacted in 2002. The FCA's information technology-related regulations primarily focus on E-commerce terminology and the concept of conducting business in an E-commerce environment. Since then, there have been significant growth, changes, and advancements in information technology (IT) and the System's use of technology to conduct business. For example, in the year 2000, just half of Americans had broadband access at home. Today, that number sits at more than 90%. As more individuals access and utilize information technology and online services to conduct their business, the System has responded accordingly. It is the responsibility of the FCA, as the System's regulator and examiner, to see that the System's use of information technology is consistent with operating in a safe and sound manner.

To that end, we propose to revise the current E-commerce regulations at Part 609 to codify existing expectations concerning risk management practices, corporate governance, and internal control systems for conducting business in an electronic environment. These expectations have been and are

continually communicated to System institutions through the FCA's role as examiner of the System. By codifying expectations through these proposed regulations, we ensure each System institution fully understands the responsibility to operate under a comprehensive cyber risk framework. This proposed rule gives stakeholders an opportunity to comment on these important expectations.

Information security refers to the policies, procedures, and technologies used to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability of information and data, no matter its form. Cyber security is the process of protecting information assets and data by preventing, detecting, and responding to cyber-attacks. Cyber risk is any risk associated with financial loss, disruption, or damage to the reputation of an organization due to the failure or unauthorized or erroneous use of its information systems. The policies, procedures, and internal controls implemented to manage cyber risk should incorporate information security and cyber security concepts and sound business practices. Appropriate governance and controls over cyber risk can help guide future decision-making about how to mitigate risk while focusing on an institution's strategic goals and objectives.

A. Recissions:

We propose to rescind sections 609.910, 609.915, 609.920, 609.925, 609.940, and 609.950. The rescissions will delete all references to E-SIGN and FRB Regulations B, Z, and M. E-SIGN and the FRB regulations do not establish independent requirements of System institutions. Furthermore, we believe the reminder of the applicability of E-SIGN and the FRB regulations is no longer necessary. The substantive content of Section 609.940, Internal systems and controls has been absorbed by the proposed revisions of Section 609.930 below.

B. Revisions:

We also propose to revise sections 609.905, 609.930, and 609.935. We do not propose any changes to 609.945 (Records retention). We also propose to revise the name of Part 609 to Cyber Risk Management and rename the subsections, consistent with the proposed revisions. These revisions will codify FCA's expectations for System institutions when considering and documenting cyber risk policies and procedures, commensurate with the size and complexity of each individual association.

Most notably, we propose to revise Part 609 to require an institution to implement a board-approved cyber risk plan that helps an institution manage the risk by:

1. Assessing institution risk and identifying potential points of vulnerability;

2. Establishing a risk management program for the institution's identified risks;

3. Considering privacy and legal compliance issues surrounding cyber risk;

4. Developing an incident response plan;

5. Developing a cyber risk training program;

6. Setting policies for managing third-party relationships;

7. Maintaining robust internal controls; and

8. Establishing institution board reporting requirements.

FCA seeks to maintain maximum flexibility for System institutions, including the Federal Agricultural Mortgage Corporation (FAMC), given our understanding that there are varying degrees of size and complexity across the System. Institutions must strive to maintain industry standards. We note our Office of Examination frequently consults the Federal Financial Institutions Examination Council (FFIEC) guidance when examining for safety and soundness as it relates to institutions' cyber risk. We believe 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.

Comments are sought on all the provisions in the regulation.

**List of Subjects**

**12 CFR Part 609**

Agriculture, Banks, Banking, Computer technology, Reporting and recordkeeping requirements, Rural areas.

PART 609 — CYBER RISK MANAGEMENT

Subpart A — General Rules

Sec.

609.905 In general

Subpart B — Standards for Boards and Management

Sec.

609.930 Cyber risk management

609.935 Business planning

609.945 Records retention

Part 609 – CYBER RISK MANAGEMENT

1. The authority citation is proposed to be revised to read:

   **Authority:** Section 5.9 of the Farm Credit Act (12 U.S.C. 2243).

2. For the reasons stated in the preamble, part 609 of title 12 of the Code of Federal Regulations is proposed to be revised to read as follows:

Subpart A – General Rules

**§ 609.905 In general**

System institutions must engage in appropriate risk management practices to ensure safety and soundness of their

operations. A System institution's board and management must maintain effective policies, procedures, and controls to mitigate cyber risks. This includes establishing an appropriate vulnerability management program to monitor cyber threats, mitigate any known vulnerabilities, and establish appropriate reporting mechanisms to the institution's board and FCA.

§ 609.910 [Removed]

§ 609.915 [Removed]

§ 609.920 [Removed]

§ 609.925 [Removed]

Subpart B – Standards for Boards and Management

**§ 609.930 Cyber Risk Management**

(a) Cyber Risk Management Program. Each Farm Credit System (System) institution must implement a comprehensive, written cyber risk management program consistent with the size and complexity of the institution's operations. The program must ensure the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.

(b) Role of the Board and Management. Each year, the board of directors of each System institution or an appropriate committee of the board must:

(1) Approve a written cyber risk program. The program must be consistent with industry standards to ensure the institution's safety and soundness and compliance with law and regulations;

(2) Oversee the development, implementation, and maintenance of the institution's cyber risk program; and

(3) Assign roles and responsibilities and determine necessary expertise for the institution's board, management, and employees.

(c) Cyber Risk Program. Each institution's cyber risk program must, at a minimum:

(1) Include an annual risk assessment of the internal and external factors likely to affect the institution. The risk assessment, at a minimum, must:

i. Identify and assess internal and external factors that could result in unauthorized disclosure, misuse, alteration, or destruction of current, former, and potential customer and employee information or information systems; and

ii. Assess the sufficiency of policies, procedures, internal controls, and other practices in place to mitigate risks.

(2) Identify systems and software vulnerabilities, prioritize the vulnerabilities and the affected systems in order of risk, and perform timely remediation. The particular security measures an institution adopts will depend upon the risks presented by the size of the institution and the nature, scope, and complexity of the institution's operations and activities.

(3) Maintain an incident response plan that contains procedures the institution must implement when it suspects or detects unauthorized access to current, former, or potential customer, employee, or other sensitive or confidential information. At a minimum, an institution's incident response plan must contain procedures for:

i. Assessing the nature and scope of an incident, and identifying what information systems and types of information have been accessed or misused;

ii. Acting to contain the incident while preserving records and other evidence;

iii. Resuming business activities during intrusion response;

iv. Notifying the institution's board of directors when the institution learns of an incident involving unauthorized access to or use of sensitive or confidential customer and/or employee information;

v. Notifying FCA as soon as possible or no later than 36 hours after the institution determines that an incident has occurred; and

vi. 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.

(4) Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.

(5) Include policies for vendor management and oversight. Each institution, at a minimum, must:

i. Exercise appropriate due diligence in selecting vendors;

ii. Require its vendors, by contract, to implement appropriate measures designed to meet the objectives of the institution's cyber risk program;

iii. Monitor its vendors to ensure they have satisfied agreed upon expectations and deliverables. Monitoring must include reviewing audits, summaries of test results, or other equivalent evaluations of its vendors.

(6) Maintain robust internal controls by regularly testing the key controls, systems, and procedures of the cyber risk management program.

i. The frequency and nature of such tests are to be determined by the institution's risk assessment.

ii. Tests must be conducted or reviewed by independent third parties or staff independent of those who develop or maintain the cyber risk management program.

iii. Internal systems and controls must provide reasonable assurances that System institutions will prevent, detect, and remediate material deficiencies on a timely basis.

(d) Privacy. Institutions must consider privacy and other legal compliance issues, including but not limited to, the privacy and security of System institution information; current, former, and potential borrower information; and employee

information, as well as compliance with statutory requirements for the use of electronic media.

(e) Board reporting requirements. Each institution must report quarterly to its board or an appropriate committee of the board. The report must contain material matters and metrics related to the institution's cyber risk management program, including specific risks and threats.

**§ 609.935 Business planning**

The annually approved business plan required under part 618 of this chapter, subpart J, and § 652.60 for the Federal Agricultural Mortgage Corporation, must include a technology plan that, at a minimum:

(1) Describes the institution's intended technology goals, performance measures, and objectives;

(2) Details the technology budget;

(3) Identifies and assesses the business risk of proposed technology changes and assesses the adequacy of the institution's cyber risk program;

(4) Describes how the institution's technology and security support the current and planned business operations; and

(5) Reviews internal and external technology factors likely to affect the institution during the planning period.

§ 609.940 [Removed]

§ 609.945 **Records retention**

Records stored electronically must be accurate, accessible, and reproducible for later reference.

§ 609.950 [Removed]

Dated:

*Ashley Waldron*,
*Secretary*,
*Farm Credit Administration.*