SUBCHAPTER B—FARM CREDIT SYSTEM

PART 609—CYBER RISK MANAGEMENT

Subpart A—General Rules

Sec.
609.905 In general.

Subpart B—Standards for Boards and Management

609.930 Cyber risk management.
609.935 Business planning.
609.945 Records retention.

AUTHORITY: Sec. 5.9 of the Farm Credit Act (12 U.S.C. 2243); 5 U.S.C. 301; Pub. L. 106–229 (114 Stat. 464).

SOURCE: 88 FR 85832, Dec. 11, 2023, unless otherwise noted.

Subpart A—General Rules

§ 609.905 In general.

Farm Credit System (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 and document 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 the Farm Credit Administration (FCA). The vulnerability management programs should be commensurate with the size, risk profile, and complexity of the institution and based on sound industry standards and practices.

Subpart B—Standards for Boards and Management

§ 609.930 Cyber risk management.

(a) *Cyber risk management program.* Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect 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.* 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) Determine necessary expertise for executing the cyber risk management plan and, where practical, delegate day-to-day responsibilities to 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 based on risk, and perform timely remediation. The particular security measures an institution adopts will depend upon the size, risk profile, 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. An institution's incident response plan must be reviewed and updated periodically, but at least annually, to address new threats, concerns, and evolving technology. The 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, or unauthorized access to financial institution information including proprietary 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) Negotiate contract provisions, when feasible, that facilitate effective risk management and oversight and specify the expectations and obligations of both parties;

(iii) Conduct a vendor risk assessment on all vendors; and

(iv) Monitor its IT and cyber risk management related vendors to ensure they have satisfied agreed upon expectations and deliverables. Monitoring may 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.* At a minimum, each institution must report quarterly to its board or an appropriate committee of the board. The report must contain material matters 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 subpart J of part 618 of this chapter, and § 652.60 of this chapter for System institutions and the Federal Agricultural Mortgage Corporation, respectively, must include a technology plan that, at a minimum:

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

(b) Details the technology budget;

(c) Identifies and assesses the adequacy of the institution's entire cyber risk management program, including proposed technology changes;

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

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

§ 609.945 Records retention.

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

Subpart D—General Requirements for Electronic Communications

§ 609.950 Electronic communications.

(a) *Agreement.* In accordance with E-SIGN, System institutions may communicate electronically in business, consumer, or commercial transactions. E-commerce transactions require the agreement of all parties when you do business.

(b) *Communications with consumers.* E-SIGN and Federal Reserve Board Regulations B, M, and Z (12 CFR parts 202, 213, and 226) outline specific disclosure requirements for communications with consumers.

(c) *Communications with parties other than consumers.* The consumer disclosure requirements of E-SIGN and of Federal Reserve Board Regulation B (12 CFR part 202) do not apply to your communications with parties other than consumers. (Federal Reserve Board Regulations M and Z (12 CFR parts 213 and 226) apply to consumers only.) Nonetheless, you must ensure that your communications, including those disclosures required under the Act and the regulations in this part, demonstrate good business practices in the delivery of credit and closely related services and in your obtaining goods and services.

PART 610—REGISTRATION OF MORTGAGE LOAN ORIGINATORS

AUTHORITY: Secs. 1.5, 1.7, 1.9, 1.10, 1.11, 1.13, 2.2, 2.4, 2.12, 5.9, 5.17, 7.2, 7.6, 7.8 of the Farm Credit Act (12 U.S.C. 2013, 2015, 2017, 2018, 2019, 2021, 2073, 2075, 2093, 2243, 2252, 2279a–2, 2279b, 2279c–10); and secs. 1501 *et seq.* of Pub. L. 110–289, 122 Stat. 2654.

SOURCE: 78 FR 51048, Aug. 20, 2013, unless otherwise noted.

§ 610.101 Cross reference.

The rules formerly at 12 CFR part 610 have been recodified by the Consumer Financial Protection Bureau at 12 CFR part 1007, ''S.A.F.E. Mortgage Licensing Act—Federal Registration of Residential Mortgage Loan Originators (Regulation G)''.

PART 611—ORGANIZATION

Subpart A—General

Sec.
611.100 Definitions.
611.110 Meetings of stockholders.

Subpart B—Bank and Association Board of Directors

611.210 Director qualifications and training.
611.220 Outside directors.

Subpart C—Election of Directors and Other Voting Procedures

611.310 Eligibility for membership on bank and association boards and subsequent employment.
611.320 Impartiality in the election of directors.
611.325 Bank and association nominating committees.
611.326 Floor nominations for open Farm Credit bank and association director positions.
611.330 Disclosures of Farm Credit bank and association director-nominees.
611.340 Confidentiality and security in voting.
611.350 Application of cooperative principles to the election of directors.
611.360 [Reserved]

Subpart D—Compensation Practices of Farm Credit Banks and Associations

611.400 Compensation of bank board members.
611.410 [Reserved]

Subpart E—Transfer of Authorities

611.500 General.
611.501 Procedures.
611.505 Farm Credit Administration review.
611.510 Approval procedures.
611.515 Information statement.
611.520 Plan of transfer.
611.525 Stockholder reconsideration.

Subpart F—Bank Mergers, Consolidations and Charter Amendments

611.1000 General authority.