

plus an amount that transitions linearly for each business day during that period from:

(1) The difference between SOFR and overnight LIBOR determined as of the day immediately before the LIBOR replacement date; to

(2) The tenor spread adjustment identified in paragraph (c)(1) of this section; or

(B) In place of the one-, three-, six-, or 12-month tenors of LIBOR, the benchmark replacement shall be the corresponding one-, three-, six-, or 12-month CME Term SOFR plus an amount that transitions linearly for each business day during that period from:

(1) The difference between the relevant CME Term SOFR and the relevant LIBOR tenor determined as of the day immediately before the LIBOR replacement date; to

(2) The applicable tenor spread adjustment identified in paragraph (c) of this section.

(ii) On the date one year after the LIBOR replacement date and thereafter:

(A) In place of overnight LIBOR, the benchmark replacement shall be SOFR plus the tenor spread adjustment identified in paragraph (c)(1) of this section; and

(B) In place of one-, three-, six-, or 12-month tenors of LIBOR, the benchmark replacement shall be the corresponding one-, three-, six-, or 12-month CME Term SOFR plus the applicable tenor spread adjustment identified in paragraph (c) of this section.

(iii) The rates published or provided by Refinitiv Limited as “USD IBOR Cash Fallbacks” for “Consumer” products shall be deemed equal to the rates identified in paragraphs (b)(2)(i) and (ii) of this section.

(3) For a covered contract that is a covered GSE contract—

(i) In place of overnight LIBOR, the benchmark replacement shall be SOFR plus the tenor spread adjustment identified in paragraph (c)(1) of this section; and

(ii) In place of one-, three-, six-, or 12-month tenors of LIBOR, the benchmark replacement shall be the 30-day Average SOFR plus the applicable tenor spread adjustment identified in paragraph (c) of this section.

(c) *Tenor spread adjustments.* The following tenor spread adjustments shall be included as part of the Board-selected benchmark replacements as indicated in paragraphs (a) and (b) of this section:

(1) 0.00644 percent for overnight LIBOR;

(2) 0.11448 percent for one-month LIBOR;

(3) 0.26161 percent for three-month LIBOR;

(4) 0.42826 percent for six-month LIBOR; and

(5) 0.71513 percent for 12-month LIBOR.

(d) *Date for determining Board-selected benchmark replacement.* For purposes of this part, any Board-selected benchmark replacement shall be determined as of the day that, under the covered contract, would have been used to determine the LIBOR-based rate that is being replaced or, if the Board-selected benchmark replacement is not published on the day indicated in the covered contract, the most recently available publication should be used.

§ 253.5 Benchmark Replacement Conforming Changes.

(a) *Benchmark replacement conforming changes.*

(1) The Board may, in its discretion, by regulation or order, require any additional technical, administrative, or operational changes, alterations, or modifications in LIBOR contracts based on a determination that such changes, alterations, or modifications would address one or more issues affecting the implementation, administration, and calculation of a Board-selected benchmark replacement in LIBOR contracts.

(2) Solely with respect to a LIBOR contract that is not a consumer loan, a calculating person may make any additional technical, administrative, or operational changes, alterations or modifications that, in that person’s reasonable judgment, would be necessary or appropriate to permit the implementation, administration, and calculation of the Board-selected benchmark replacement under or with respect to a LIBOR contract after giving due consideration to any changes, alterations, or modifications otherwise required by the Board in this part or pursuant to paragraph (a)(1) of this section.

§ 253.6 Preemption.

(a) Pursuant to section 107 of the Adjustable Interest Rate (LIBOR) Act, this part supersedes any provision of any state or local law, statute, rule, regulation, or standard—

(1) Relating to the selection or use of a benchmark replacement or related conforming changes; or

(2) Expressly limiting the manner of calculating interest, including the compounding of interest, as that provision applies to the selection or use of a Board-selected benchmark replacement or benchmark replacement conforming changes.

By order of the Board of Governors of the Federal Reserve System.

Ann Misback,

Secretary of the Board.

[FR Doc. 2022–15658 Filed 7–27–22; 8:45 am]

BILLING CODE 6210–01–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 our regulations to reflect developments in cyber risk and continuously evolving business practices concerning electronic business (E-business) and to rename the regulations “Cyber Risk Management”.

DATES: Comments on this proposed rule must be submitted on or before September 26, 2022.

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 website. 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:

- *Email:* Send us an email at reg-comm@fca.gov.

- *FCA website:* <https://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 website at <https://www.fca.gov>. Once you are in the website, 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 email 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 at 12 CFR parts 202, 213, and 226 (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 CFR 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. Rescissions

We propose to rescind §§ 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 § 609.940 (Internal systems and controls) has been absorbed by the proposed revisions of § 609.930 below.

B. Revisions

We also propose to revise §§ 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 sections, 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 in 12 CFR Part 609

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

For the reasons stated in the preamble, FCA proposes to revise part 609 of title 12 of the Code of Federal Regulations to read as follows:

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.

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

PART 609—CYBER RISK MANAGEMENT

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 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).

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 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; and

(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 subpart J of part 618 of this chapter, and § 652.60 of this chapter for the Federal Agricultural Mortgage Corporation, 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 business risk of proposed technology changes and assesses the adequacy of the institution's cyber risk program;

(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.

Dated: July 19, 2022.

Ashley Waldron,

Secretary, Farm Credit Administration.

[FR Doc. 2022-15747 Filed 7-27-22; 8:45 am]

BILLING CODE 6705-01-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA-2022-0979; Project Identifier MCAI-2022-00171-T]

RIN 2120-AA64

Airworthiness Directives; Embraer S.A. (Type Certificate Previously Held by Yaborá Indústria Aeronáutica S.A.; Embraer S.A.) Airplanes

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: The FAA proposes to supersede Airworthiness Directive (AD) 2019-25-16, which applies to certain Embraer S.A. Model ERJ 170-100 LR, -100 STD, -100 SE, and -100 SU airplanes; and Model ERJ 170-200 LR, -200 SU, -200 STD, and -200LL airplanes. AD 2019-25-16 requires revising the existing maintenance or inspection program, as applicable, to incorporate new or more restrictive airworthiness limitations. Since the FAA issued AD 2019-25-16, the FAA has determined that new or more restrictive airworthiness limitations are necessary. This proposed AD would continue to require the actions in AD 2019-25-16 and require revising the existing maintenance or inspection program, as applicable, to incorporate additional new or more restrictive airworthiness limitations and incorporate certain structural modifications, as specified in an Agência Nacional de Aviação Civil (ANAC) AD, which is proposed for incorporation by reference. The FAA is proposing this AD to address the unsafe condition on these products.

DATES: The FAA must receive comments on this proposed AD by September 12, 2022.

ADDRESSES: You may send comments, using the procedures found in 14 CFR 11.43 and 11.45, by any of the following methods:

- *Federal eRulemaking Portal:* Go to www.regulations.gov. Follow the instructions for submitting comments.

- *Fax:* 202-493-2251.

- *Mail:* U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590.

- *Hand Delivery:* U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

For ANAC material that will be incorporated by reference (IBR) in this AD, contact National Civil Aviation Agency (ANAC), Aeronautical Products Certification Branch (GGCP), Rua Dr. Orlando Feirabend Filho, 230—Centro Empresarial Aquarius—Torre B—Andares 14 a 18, Parque Residencial Aquarius, CEP 12.246-190—São José dos Campos—SP, Brazil; telephone 55 (12) 3203-6600; email pac@anac.gov.br; internet www.anac.gov.br/en/. You may find this material on the ANAC website at <https://sistemas.anac.gov.br/certificacao/DA/DAE.asp>. For Embraer service information identified in this proposed AD, contact Embraer S.A., Technical Publications Section (PC 060), Av. Brigadeiro Faria Lima, 2170—Putim—12227-901 São José dos Campos—SP—Brasil; telephone +55 12 3927-5852 or +55 12 3309-0732; fax +55 12 3927-7546; email distrib@embraer.com.br; internet www.flyembraer.com. You may view this material at the FAA, Airworthiness Products Section, Operational Safety Branch, 2200 South 216th St., Des Moines, WA. For information on the availability of this material at the FAA, call 206-231-3195. The ANAC AD is also available in the AD docket at www.regulations.gov by searching for and locating Docket No. FAA-2022-0979.

Examining the AD Docket

You may examine the AD docket at www.regulations.gov by searching for and locating Docket No. FAA-2022-0979; or in person at Docket Operations between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The AD docket contains this NPRM, the mandatory continuing airworthiness information (MCAI), any comments received, and other information. The street address for Docket Operations is listed above.

FOR FURTHER INFORMATION CONTACT:

Krista Greer, Aerospace Engineer, Large Aircraft Section, FAA, International Validation Branch, 2200 South 216th St., Des Moines, WA 98198; telephone 206-231-3221; email krista.greer@faa.gov.

SUPPLEMENTARY INFORMATION:

Comments Invited

The FAA invites you to send any written relevant data, views, or arguments about this proposal. Send your comments to an address listed under **ADDRESSES**. Include “Docket No. FAA-2022-0979; Project Identifier MCAI-2022-00171-T” at the beginning of your comments. The most helpful comments reference a specific portion of the proposal, explain the reason for any recommended change, and include supporting data. The FAA will consider all comments received by the closing date and may amend this proposal because of those comments.

Except for Confidential Business Information (CBI) as described in the following paragraph, and other information as described in 14 CFR 11.35, the FAA will post all comments received, without change, to www.regulations.gov, including any personal information you provide. The agency will also post a report summarizing each substantive verbal contact received about this NPRM.

Confidential Business Information

CBI is commercial or financial information that is both customarily and actually treated as private by its owner. Under the Freedom of Information Act (FOIA) (5 U.S.C. 552), CBI is exempt from public disclosure. If your comments responsive to this NPRM contain commercial or financial information that is customarily treated as private, that you actually treat as private, and that is relevant or responsive to this NPRM, it is important that you clearly designate the submitted comments as CBI. Please mark each page of your submission containing CBI as “PROPIN.” The FAA will treat such marked submissions as confidential under the FOIA, and they will not be placed in the public docket of this NPRM. Submissions containing CBI should be sent to Krista Greer, Aerospace Engineer, Large Aircraft Section, FAA, International Validation Branch, 2200 South 216th St., Des Moines, WA 98198; telephone 206-231-3221; email krista.greer@faa.gov. Any commentary that the FAA receives which is not specifically designated as CBI will be placed in the public docket for this rulemaking.