additional guidance related to concrete properties and damping values for use in the development of in structure response spectra. It also includes guidance on damping for steel plate composite walls. In addition, it updates the guidance for piping damping in RG 1.61, Revision 1.

II. Additional Information

The NRC published a notice of the availability of DG–1364 in the **Federal Register** on June 13, 2023 (88 FR 38408) for a 30-day public comment period. The public comment period closed on July 13, 2023. Public comments on DG–1364 and the staff responses to the public comments are available under ADAMS under Accession No. ML23284A274.

As noted in the **Federal Register** on December 9, 2022 (87 FR 75671), this document is being published in the ''Rules'' section of the **Federal Register** to comply with publication requirements under 1 CFR chapter I.

III. Congressional Review Act

This RG is a rule as defined in the Congressional Review Act (5 U.S.C. 801–808). However, the Office of Management and Budget has not found it to be a major rule as defined in the Congressional Review Act.

IV. Backfitting, Forward Fitting, and Issue Finality

Issuance of RG 1.61 would not constitute backfitting as that term is defined in section 50.109 of title 10 of the *Code of Federal Regulations* (10 CFR), ''Backfitting,'' and as described in NRC Management Directive (MD) 8.4, ''Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests (ADAMS Accession No. ML18093B087);'' constitute forward fitting as that term is defined and described in MD 8.4; or affect issue finality of an approval issued under 10 CFR part 52, ''Licenses, Certifications, and Approvals for Nuclear Power Plants,'' as explained in RG 1.61, licensees would not be required to comply with the positions set forth in RG 1.61.

V. Submitting Suggestions for Improvement of Regulatory Guides

A member of the public may, at any time, submit suggestions to the NRC for improvement of existing RGs or for the development of new RGs. Suggestions can be submitted on the NRC's public website at *https://www.nrc.gov/reading-rm/doc-collections/reg-guides/contactus.html.* Suggestions will be considered in future updates and enhancements to the ''Regulatory Guide'' series.

Dated: December 5, 2023.

For the Nuclear Regulatory Commission.

Stephen M. Wyman,

Acting Chief, Regulatory Guide and Programs Management Branch, Division of Engineering, Office of Nuclear Regulatory Research.

[FR Doc. 2023–27070 Filed 12–8–23; 8:45 am]

BILLING CODE 7590–01–P

FARM CREDIT ADMINISTRATION

12 CFR Part 609

RIN 3052–AD53

Cyber Risk Management

AGENCY: Farm Credit Administration.

ACTION: Final rule.

SUMMARY: The Farm Credit Administration (FCA, we, or our) rescinds and revises its regulations to reflect developments in cyber risk and continuously evolving business practices. We rename the regulations ''Cyber Risk Management.'' The final rule requires each Farm Credit System (System or FCS) institution to implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations.

DATES: This regulation is effective January 1, 2025.

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;

or

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

The objectives of this final 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 on October 1, 2000. E–SIGN is a statutory requirement that governs electronic transactions relating to the conduct of electronic business, consumer, or commercial affairs. E–SIGN continues to apply to System institutions as statutory requirements.
- Revise part 609 to codify our existing expectations, as well as ensure the relevance and adequacy of risk management practices, corporate governance, and internal control systems at System institutions conducting business in an electronic environment.
- Require each System institution to develop and implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations.

II. Background

The regulations at 12 CFR part 609 were enacted in 2002 and repeated the statutory requirements of E–SIGN. Our existing information-technology (IT)-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 changes and advancements in IT and the System's use of technology to conduct business.

We are responsible, as the System's regulator, to ensure the System's use of IT is consistent with safe and sound operations and complies with the law.

We amend the current E-commerce regulations at part 609 to revise the rules for a broader cyber risk focus and to codify our existing expectations on risk management practices, corporate governance, and internal control systems for conducting business in an electronic environment. The final regulations set forth core principles that serve as the foundation for creating a comprehensive cyber risk management program and framework.

Key definitions include: [1]

- *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.
- *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.

A System institution's policies, procedures, and internal controls that manage cyber risk must incorporate information security and cyber security concepts and sound business practices.

[1] FFIEC IT Examination Handbook InfoBase—Glossary, *https://www.ithandbook.ffiec.gov/glossary.*

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.

These cyber risk management regulations allow System institutions to innovate. We recognize that innovation in the System may create different opportunities, challenges, and risks for different institutions. Accordingly, we considered the needs and constraints of all institutions, regardless of size, risk profile, or complexity. We understand cyber risk management programs will vary and there is no one-size-fits-all approach; however, these cyber risk management regulations provide the flexibility for System institutions to innovate based on the institution's unique needs and operations.

System institutions can mitigate challenges and risks through good governance and effective risk management. Strong governance principles and appropriate risk management practices, implemented through sound internal controls, can safeguard against a variety of risks, including those stemming from adopting new technology. However, an institution should never sacrifice safety and soundness for innovation.

These cyber risk management regulations encourage System institutions to implement and develop effective and sound cyber risk management program solutions. We continually communicate these expectations to System institutions in our role as examiner of the System. This rule also considers the role our examinations play in ensuring safe and sound operations of the System.

III. Comments and Our Responses

We received 26 comment letters, all of which came from System institutions or persons affiliated with the System, except one that came from the Independent Community Bankers of America (ICBA). Of the comment letters received, one came from the Farm Credit Council (Council), acting on behalf of its membership. Each of the four Farm Credit banks submitted a letter, as did the Federal Agricultural Mortgage Corporation (Farmer Mac). Many comment letters from System associations expressed support for the Council's letter, with several raising specific issues. The following is a description of the issues raised and our responses.

A. General Comments

Principles-Based Approach

Most of the commenters stated that the proposed rule does not align with a principles-based approach to rule-making. As discussed below, we disagree. As an initial matter, we considered that System institutions vary dramatically in terms of size, risk profile, and complexity of business model. Accordingly, during the rule-making process, we focus on the right blend of principles and specific requirements to achieve a safe and sound System.

Principles-based regulations set forth broad objectives and goals for which System institutions should strive. Thus, this rule does not address every circumstance. The rule attempts to balance an institution's need to develop a cyber risk management program against our mission to promote and protect the safety and soundness of each institution and the System, as a whole. The rule provides flexibility, where appropriate, and establishes minimum standards, where needed. Thus, the rule provides System institutions with parameters and our expectations for the System to establish, among other things, internal controls consistent with a principles-based rule. The regulation provides flexibility for both the FCA and the System to adapt to market developments and evolving technology. We believe we have achieved the correct regulatory balance.

While commenting on this principles-based approach, one institution asked us to minimize examination inconsistency by recognizing and clarifying the appropriate role of management and the board of directors in selecting the appropriate cyber security approach from among the many that may satisfy the overarching principles of the rule. An institution has the flexibility to determine its risk profile and identify appropriate cyber risk management practices. The institution should document its analysis to provide examiners with an opportunity to assess its choices.

This approach acknowledges that there is more than one way to comply with the regulation. We will take a risk-based approach, and not a one-size-fits-all approach, in our examination of each System institution.

Ambiguous, Unclear, or Unfeasible

Several institutions commented that portions of the proposed regulation are unclear or unfeasible. In response, we reviewed the proposed regulation in its entirety to ensure it is written in accordance with plain language principles and to clarify any potentially confusing language.

The rule requires System institutions to develop a program consistent with the size, risk profile, and complexity of the institution's operations. This provides flexibility, consistent with a principles-based approach, to allow each System institution to customize its cyber security program for its particular risk environment. However, to address commenters' concerns, we are adding the term ''risk profile,'' as appropriate throughout the preamble and regulation, to clarify that an institution's program must be based on size, complexity, and risk. Adding the term ''risk profile'' will allow each System institution to customize its cyber risk management program for its unique risk environment.

User Experience

One commenter stated that perfect security is neither possible nor desirable, and there is often a fundamental tradeoff between security and convenience (or user experience). The commenter further stated that 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.

Although convenience and user experience could compromise security, we believe a risk assessment, including a determination to mitigate or accept certain risks, is critical to an institution's cyber risk management program. Thus, an institution must document why it accepts, transfers, or mitigates the risk. The board has a fiduciary responsibility to ensure a safe and sound operating environment. If the board chooses to accept a risk for convenience or customer experience, the board's approval must be documented.

Leveraging Modern Frameworks

Several commenters suggested the proposed regulation should leverage standard frameworks based on industry standards (*e.g.,* Federal Financial Institutions Examination Council (FFIEC) or National Institute of Standards and Technology (NIST)), which would allow the regulation to remain relevant for rapidly changing technologies.

We agree. As this is a principles-based regulation, in part, linking to standard frameworks will encourage innovation, implementation, and compliance. Referencing industry standards promotes conformity with the cyber risk management rule as institutions innovate and apply rapidly evolving technology and attendant controls.

We also direct System institutions to the June 27, 2017, Informational Memorandum (IM) on ''Reporting Security Incidents and Business Continuity Events to FCA.'' This guidance will assist System institutions to identify and define an incident under 12 CFR 609.930(c)(3)(i) and help determine reporting requirements. The Office of Examination periodically releases informational memoranda to update the System on expectations. We anticipate the continued issuance of such guidance documents in the future, despite the publication of this rule.

Requests To Define Key Terms

Several commenters requested that we define key terms, such as ''effective,'' ''ensure,'' or ''appropriate.'' However, as this is a principles-based rule, we will not define such terms here.

FCA and the institutions it regulates must interpret these terms considering the institution's unique circumstances. What may be ''effective'' or ''appropriate'' at one institution or at one time may not be ''effective'' or ''appropriate'' at another institution with a different risk profile, where there is a different size or complexity, or at a different time. FCA's decision to not define the terms allows an institution to determine what is effective or appropriate at its institution. During the supervisory and examination process, we will apply the regulatory requirements based on the institution's current circumstances, which is consistent with a principles-based rule. Moreover, these terms currently are used without definition throughout our regulations, and we do not believe it appropriate to define the terms in this regulation.

FCS institutions may want to refer to the NIST Computer Security Resource Center's Glossary [2] and FFIEC IT Examination Handbook InfoBase—Glossary [3] as additional resources in defining terms. For further guidance, please refer to our IM dated June 27, 2017, entitled, ''Reporting Security Incidents and Business Continuity Events to FCA,'' for terms like ''Security Event'' and ''Security Incident.''

Conformity With Other Federal Financial Regulators

The ICBA recommends that we harmonize the proposed regulation and guidance with that of the other federal financial regulatory agencies to ensure System institutions operate in a safe and sound manner. In drafting this regulation, we reviewed the cyber security regulations of the federal financial regulatory agencies and included some of the elements of those regulations. We believe the review process was comprehensive and have been unable to identify any other provisions we should include. Nevertheless, we refer System institutions to the FFIEC IT Handbook [4] and NIST [5] for additional guidance and as examples of industry standards.

Reproposing the Proposed Rule

Two System institutions stated that the proposed rule should be pulled back, reworked, and reproposed in the future to allow for additional comments. We disagree. FCA has not updated our technology regulations in years. We believe this updated regulation will help institutions strengthen their cyber security and cyber risk management practices. We provide, through this principles-based rule, flexibility for institutions to develop cyber risk management programs based on institution size, risk profile, and complexity.

Regulatory Burden

One commenter suggested the proposed rule is excessively burdensome and inconsistent with modern industry accepted and dynamic cyber security program standards that System institutions already implemented as part of their cyber security programs. The commenter further stated that the proposed rule would adversely impact the ability and capability of System institutions to establish effective and relevant cyber security programs. Additionally, the commenter said the language was prescriptive and vague. The commenter stated that we should defer to industry standards and not attempt to create competing, duplicative, and non-conforming regulatory requirements.

We agree, in part, and FCA intends through this rulemaking to leverage standard frameworks based on industry standards, such as FFIEC and NIST, as discussed herein. However, consistent with principles-based rulemaking, we reiterate that an institution must develop a program consistent with the size, risk profile, and complexity of the institution's operations. An institution should customize and document the cyber risk management program for its risk environment.

Examination Approach

Several commenters asked how FCA examiners would examine cyber risk management programs at System institutions of different sizes and complexities. Commenters were also concerned the rule does not have specific definitions and thresholds that may lead to inconsistencies in examinations.

Examiners will review cyber risk management programs much like other internal controls programs. There is no one-size-fits-all approach. We know cyber risk management plans will differ based on an institution's size, complexity, and risk profile. The rule outlines items institutions must consider, such as a written cyber risk management program, documented incident response plan, and documented risk assessments, which examiners may review as part of the examination process. We will provide consistency and clarity in our supervision and regulation of the System as it pertains to, among other things, cyber risk management.

B. Comments on Specific Provisions

Mitigating Vulnerabilities (§ 609.905)

Several commenters recommended that we allow each System institution to define the term ''vulnerability'' in proposed § 609.905 based on a modern framework and remove the requirement that ''any'' vulnerability must be remediated. They asserted that System institutions should be allowed 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. There was also a comment that human capital presents the greatest risk or vulnerability to an institution.

We do not agree that the regulation should include the suggested terminology ''based on a modern framework.'' We believe the commenter's suggested language of ''based on a modern framework'' is vague and could be misinterpreted to allow a System institution to use any modern framework, which could lead to further inconsistencies among System institutions. However, we do agree that an institution should rank and prioritize vulnerabilities based on its cyber risk management program and cyber risk assessment. The vulnerability management program should be commensurate with the size, risk profile, and complexity of the institution and based on sound industry standards and practices.

[2] Glossary |√ CSRC, *https://www.csrc.nist.gov/glossary.*

[3] FFIEC IT Examination Handbook InfoBase—Glossary, *https://www.ithandbook.ffiec.gov/glossary.*

[4] FFIEC IT Handbook, *https://www.ithandbook.ffiec.gov.*

[5] Cybersecurity | NIST, *https://www.nist.gov/cybersecurity.*

A System institution board should identify and document the institution's appetite for risk. Then, the board, with management, should assess the institution's vulnerabilities. Although an institution cannot mitigate every vulnerability, each System institution's board must assess the risk of a vulnerability, decide whether the vulnerability exposes the institution to any undue risk, and document its analysis and conclusions. In some cases, a System institution may assess and identify its risk appetite and accept the risk, which should be documented to allow FCA to examine for safety and soundness, as well as compliance with law.

Mitigating vulnerabilities involves taking steps to implement internal controls that reduce risk. Remediation is the act of removing or eradicating a vulnerability from an IT system. Mitigation, on the other hand, is creating strategies to minimize the potential threat of a vulnerability when it cannot be eliminated immediately. Some vulnerabilities are more difficult to remediate and may require some time to address.

An institution could refer to the FFIEC IT Handbook or NIST Cybersecurity Framework for guidance on how to identify, document, and address a vulnerability within its risk profile.

Privacy and Compliance (§ 609.930(a))

Several commenters disagreed with the second sentence in proposed § 609.930(a), which provided as follows: ''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.'' The commenters were concerned that the phrase ''must ensure'' created an unattainable standard as to the security and confidentiality of information, as any information loss, no matter how insignificant, would appear to violate the rule as drafted. The commenters suggested that we revise this language so the program ''must be designed to protect'' or ''manage the risk'' of protecting the security and confidentiality of information.

We strongly believe there must be controls in place to protect the security and confidentiality of information. Thus, we revise the second sentence of Section 609.930(a) as follows: ''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.'' The revision to the second sentence of Section 609.930(a) addresses the commenters' concerns and will ensure that an institution has strong controls in place to protect the security and confidentiality of information.

Size and Complexity (§ 609.930(a))

We received numerous comments suggesting that we clarify expectations related to ''size and complexity'' in proposed § 609.930(a). There was a concern that a lack of guidance on ''size and complexity'' will lead to inconsistent expectations of examiners and place additional regulatory burden on smaller institutions. It was also suggested that we acknowledge the role of IT service providers to avoid examination inconsistencies and to reference ''a modern risk management framework.'' Section 609.930(a) requires, in part, each institution to implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations.

Consistent with our intent for a principles-based rulemaking, we do not define ''size and complexity.'' However, to provide clarity, we include ''risk profile'' and change the phrase to ''size, risk profile, and complexity.'' We do not believe it appropriate to reference ''a modern risk management framework.''

An institution must assess its risk profile. The regulation requires a cyber risk management program to be consistent with size, risk profile, and complexity of an institution. A smaller institution may not be required to assess as many risks as or the same types of risks as a larger institution. However, depending on an institution's complexity, size, and risk profile, it is possible for a smaller institution to have a similar cyber risk management plan range as compared to a larger institution.

Each institution should document its risk-based approach to establishing a cyber risk management plan and scope.

As noted above, to add clarity in response to the size and complexity concerns, we revise the first sentence in this section to insert the phrase ''risk profile'' to help align the regulation with the requirement of providing strong controls commensurate with an institution's size and complexity.

Role of Board and Management (§ 609.930(b))

One commenter stated that although the heading of proposed § 609.930(b) refers to the role of management, the text of this section does not appear to contemplate a defined role for management. The commenter further stated that although management has a significant role in managing cyber risk, the rule assigns many responsibilities to an institution's board of directors, with management providing the services.

We believe that a board of directors must provide appropriate oversight of management to develop, implement, and maintain a cyber risk management program consistent with the board's fiduciary duties and oversight obligations. This section provides that the board must decide who will do what without FCA specifying or telling them what to do step-by-step. We do not want to create a prescriptive rule.

For clarity, we modified the language of this section to remove ''and management'' from the heading. This should clarify that the institution board has oversight responsibility but may delegate day-to-day tasks to management and other employees, as appropriate.

Timely Remediation (§ 609.930(c)(2))

Proposed § 609.930(c)(2) requires institutions to ''perform timely remediation.'' Several commenters stated the regulation does not define the term ''timely,'' which could lead to inconsistencies and misaligned expectations between examiners and institutions. One commenter recommended we define ''timely'' by directing 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.

This is a principles-based rule. Institutions have an opportunity to be innovative and develop their own metrics and identify material matters relevant and specific to their institutions. Metrics will vary from System institution to System institution depending on risks, threats, and cyber risk management program.

As to defining ''timely,'' we understand the commenters' concerns. However, remediation evaluation should begin immediately after the vulnerability has been identified. The word ''timely'' is intended to provide institutions some flexibility. A minor vulnerability, depending on the circumstances presented, may not need to be addressed immediately, but a

major vulnerability must be addressed immediately.

Thus, we finalize this section as proposed.

Incident Response Planning (§ 609.930(c)(3))

One institution stated that ''incident response planning'' as required by proposed § 609.930(c)(3) varies greatly by institution and by incident. The technologies used and available expertise also vary greatly. The commenter stated that broad-based incident responses provide the flexibility needed to adapt to constantly changing technology and threats to technology. The commenter added that requiring specific incident plan responses to individual potential threats is both time consuming and ultimately not satisfactory, especially for new threats that may not be envisioned when the plan is created. The commenter recommended that the final rule be revised to allow institutions more flexibility in defining incident response planning.

We believe that proposed § 609.930(c)(3) included the necessary components and flexibility for an incident response plan. An institution should view an incident response plan as the steps that should be taken when a security incident occurs. Procedures do not need to be specific to any one type of event and can be written to ensure the right people are involved in the incident response and the process remains consistent. Further, we believe incident response plans will likely need to change over time in response to new threats. Thus, we revise this section to include language that the documented cyber risk management program, risk assessments, and incident response plans should be reviewed and updated periodically, but at least annually, to address new threats, concerns, and evolving technology. This is consistent with existing FFIEC, NIST, and FCA guidance.

Detailed Procedures for Security Events (§§ 609.930(c)(3)(i) Through (iii))

Proposed §§ 609.930(c)(3)(i) through (iii) require each institution to document its procedures on forensics, containment, and business resumption. Several commenters stated that the requirements in proposed §§ 609.930(c)(3)(i) through (iii) are not feasible because of the lengthy and numerous ways System institutions identify and contain security events, and later, resume business. The commenters recommended that we revise this section to focus less on specific procedures, and more on an adaptable and scalable framework to assess the nature and scope of an incident, contain the incident, and how to safely resume business activities. Some commenters stated that an institution should act in accordance with state and federal law.

We disagree with the commenters' statements. A System institution must document its procedures for, among other things, ensuring each employee follows the same protocol for forensics, containment, and business resumption. Also, documentation will assist with staff continuity within the institution and can serve as a training tool for institution employees. Furthermore, FCA examiners must be able to examine for compliance. Compliance with only state and federal laws is not appropriate because it does not assess an institution's size, complexity, and risk profile.

We will finalize this section as proposed.

Board Notice of a Cyber Incident (§ 609.930(c)(3)(iv))

One commenter recommended that we modify proposed § 609.930(c)(3)(iv) to permit each institution's board of directors to determine when it should be notified by management of a cyber incident, consistent with the board notification protocols in the institution's approved incident response plan. The commenter suggested revising the proposal to include an incident escalation matrix that would provide the board and management with a clear and specific action plan in the event of a cyber incident and identify when an incident should be brought to the attention of the board and/or other stakeholders (*e.g.,* regulators and law enforcement).

Proposed § 609.930(c)(3)(iv) requires board notice when there is a cyber incident involving unauthorized access to or use of sensitive or confidential customer or employee information.

We believe this section already includes an escalation concept, in that it applies only to sensitive or confidential information. The section does not apply to all information. We believe that when there has been a cyber incident involving sensitive or confidential information, the board must be notified. The board should not be caught off guard when it comes to hearing about cyber incidents.

After further consideration, we now also include a clause that requires notification when there is ''unauthorized access to financial institution information, including proprietary information.'' Financial institution information must also be protected. An institution must guard its institution's reputation in every instance.

Reporting an Incident (§ 609.930(c)(3)(v))

Proposed § 609.930(c)(3)(v) requires an institution to notify FCA as soon as possible, or no later than 36 hours after an institution determines a cyber security incident occurs. A few commenters stated that incidents can occur in an environment without discovery for longer than 36 hours. Additionally, one commenter stated that 36 hours will not allow an institution sufficient time to review evidence and determine whether a reportable incident has occurred. The commenter recommended extending the deadline to 72 hours. Another commenter suggested extending the reporting requirement to four business days after the date of a materiality determination, rather than the date of discovery.

The proposed rule requires ''notifying FCA as soon as possible or no later than 36 hours after the institution determines that an incident has occurred.'' We believe it reasonable that an institution be required to notify its regulator as soon as possible and no later than 36 hours after it identifies such an incident. We do not believe that a materiality standard should be introduced. Notification does not require a detailed report with findings and recommendations. Notification provides us with timely information on a cyber security incident. This is consistent with the other federal financial regulatory agencies' requirement promulgated in a joint regulation that a banking organization notify its primary federal regulator of any significant security incident as soon as possible and no later than 36 hours after it has been determined that a cyber incident has occurred.[6] Thus, we believe the notification requirements of this section are reasonable and remain unchanged.

Former, Current, or Potential Customers (§ 609.930(c)(3)(vi))

Some commenters recommended proposed § 609.930(c)(3)(vi) be amended and revised to provide notice to customers, employees, and website visitors in accordance with state and federal laws. Another commenter was concerned that there was no definition of ''customer,'' especially as it relates to potential customers exploring available loan products online. Another

[6] See. Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 FR. 66,424 (November 23, 2021).

commenter was concerned the section was overly broad and vague. Another commenter recommended deleting this phrase in its entirety.

This section requires institutions to notify former, current, or potential customers and employees, and known visitors to an institution's website, of an incident, when warranted, and in accordance with state and federal laws. For example, notification would be required when sensitive or confidential information has been compromised. The section does not define ''known visitor'' or ''potential customer.'' Overall, the commenters are concerned System institutions will interpret these terms differently.

We do not believe we should change this section as the requirements are consistent with a principles-based rule. Each System institution will determine and document what these terms mean. Providing notice, when warranted, provides flexibility to institutions. Nevertheless, all confidential information related to ''former, current, or potential customers and employees and known visitors to a website'' must be protected. System institutions may not allow others to inappropriately view or access this information without proper authorization. Our regulations at part 618 support this conclusion.

Training (§ 609.930(c)(4))

Proposed § 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.'' Several commenters argued that the requirement to train contractors and vendors is impractical and that many contractors and vendors will simply refuse to submit to institution-specific training based on their own business requirements.

As a principles-based rule, this section requires an institution to describe its plan to train employees, vendors, and contractors. However, we do not prescribe a particular plan. If an institution does not provide training, the institution must describe its plan and state why and what actions it is taking to mitigate the risk of not having institution-provided training. We require such documentation to enable FCA examiners to review the training plan.

As to vendors, System institutions should be able to confirm, either contractually or otherwise, that vendors have some acceptable level of training, as well as understand sound cyber risk management practices and protocols. We acknowledge that it is unrealistic for an institution to train all contractors and vendors.

We finalize this section as proposed.

Third-Party Vendors (§ 609.930(c)(5))

Several institutions commented generally that they did not own or manage any IT systems that they currently use. They stated that these IT systems may be owned by third-party vendors, technology service providers, or by another System institution, such as a Farm Credit Bank that provides services like a third-party service provider.

As to specific comments, one commenter asked that the term ''vendor'' be clarified. Another commenter stated that proposed § 609.930(c)(5)(i) is impractical as it requires an institution to require its vendors, by contract, to implement appropriate due diligence in selecting vendors. The commenter provided an example of its inability to comply with proposed § 609.930(c)(5)(i) when a vendor may refuse to negotiate its standard terms and conditions, due to its size and bargaining position.

We also received a comment on proposed § 609.930(c)(5)(iii) (now § 609.930(c)(5)(iv)) concerning institutions monitoring and reviewing vendor audits or summaries of test results. The commenter stated that some vendors will not provide these audits or test results. The commenter stated that requiring institutions to negotiate the right to an audit with every vendor will greatly hinder an institution's choice of vendors. Moreover, for many vendors, this is not practical. The commenter added that 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, or other non-IT contracts. Another commenter suggested a risk-based approach.

A ''vendor'' is a third party and includes third-party service providers or a System institution providing services to another System institution. A System institution should assess the risk of using a vendor, *i.e.,* complete a vendor risk assessment.[7] Completing a vendor risk assessment helps an institution understand risks when using vendor products or services. An institution cannot delegate its due diligence responsibilities.

Conducting a risk assessment is particularly important when a vendor handles a critical business function, accesses sensitive customer data, and/or interacts with customers. An institution must have controls to ensure that the vendor, even if it is another System institution, has appropriate security in place for IT systems. Whether a vendor is a System service provider or external service provider, an institution should never put its trust in any IT service provider without doing its own due diligence.

An institution has a responsibility to its customers and shareholders. Accordingly, each association must be aware of the risks, even if it outsources its IT services. We will hold the institution accountable for ensuring it has appropriate controls to ensure the continued safety and soundness of the institution. An institution must know its own complexity, including the role of technology service providers. Although services may be outsourced, an institution cannot delegate or shift the requirement for due diligence or accountability from the institution's board and management to service providers. Institutions are required to ensure service providers/vendors are providing adequate and effective services.

Nevertheless, we agree that negotiating the right to audit need not apply to every vendor. Accordingly, to address these concerns we added a new paragraph (iii), requiring institutions to conduct a vendor risk assessment on all vendors.

An institution will be able to assess the level of detail needed for their vendor risk assessment. For example, a vendor risk assessment of a catering vendor may need a statement indicating very little risk because of the nature of the service and type of information provided to the vendor. A vendor risk assessment for IT services would require an institution evaluate cyber risk as part of its vendor management process. A vendor risk assessment helps an institution understand the risks that exist when it uses vendors' products or services. Conducting a vendor risk assessment is particularly important when a vendor handles a critical business function, accesses sensitive customer data, or interacts with customers.

An institution must document the vendor risk assessment and may address whether a large vendor already has appropriate security measures. This way, an institution can determine if it

[7] A vendor risk assessment is the process of identifying and evaluating potential risks or hazards associated with a vendor's operations and products and its potential impact on your organization. When an institution performs a third-party vendor risk assessment, it determines the most likely effects of uncertain events, and then identifies, measures, and prioritizes them. Potential risks include the accuracy and reliability of operational, customer, and financial information; security breaches; operation effectiveness; and legal and regulatory compliance.

will accept, mitigate, transfer, or avoid the risk. It is possible that a vendor risk assessment could address the reputation of a vendor and conclude that there is a low risk.

Just because a smaller or less complex institution may rely on its funding bank for technology services does not mean that institution would not be required to have a cyber risk management program. If a cyber event occurred at a small or less complex institution that relies on the bank for services, we would still expect the institution to work with the bank to follow a cyber security framework (*e.g.,* identify, protect, detect, respond, and recover).

Additionally, to be more consistent with a principles-based approach, we revise proposed § 609.930(c)(4)(iii) (now § 609.930(c)(4)(iv)) to identify what an institution may monitor, rather than prescribing what an institution must monitor. This would provide an option for the institution to receive some type of report, audit, or summary. The institution must exercise appropriate due diligence in selecting any vendor. Any such assessment must include appropriate documentation for examiner review.

Internal Controls Frequency (§ 609.930(c)(6)(i))

A few commenters stated that proposed § 609.930(c)(6)(i), which requires an institution to determine the frequency and nature of internal controls testing, provides no substantive guidance on the frequency and nature of internal controls testing. No recommendation was provided.

As this is a principles-based rule, we provide institutions the autonomy to decide the frequency and nature of their internal control tests. Based on the risk assessment, each institution should decide the frequency and nature of internal control tests. If we were to mandate every element, this rule would no longer be principles-based, as appropriate, but a prescriptive rule. The type and amount of risk an institution faces should determine the nature and frequency of testing. An institution may want to consult the FFIEC IT Handbook, NIST, and FCA guidance documents.

We finalize this section as proposed.

Independent Third-Party Testing (§ 609.930(c)(6)(ii))

A commenter stated that proposed § 609.930(c)(6)(ii) requires an independent party to perform testing but does not address the size and complexity of the institutions when performing testing. The commenter asserted that, to minimize examination inconsistencies, the rule should address the unique service provider relationship and structure between some System entities.

We disagree. The regulation provides that an independent party can include institution staff who are independent of the cyber risk management program. This will allow an institution, regardless of size, risk profile, or complexity, to conduct its own testing and due diligence, which the institution should document. Institution documentation will promote consistency in the examination process.

Reasonable Assurances and Material Deficiencies (§ 609.930(c)(6)(iii))

Several commenters stated that there is no indication how to measure the term ''material.'' One commenter added that ''reasonable assurances'' seem to refer to an auditor's degree of satisfaction that the evidence obtained during the audit supports the assertions in the financial statements. The commenter added ''reasonable assurances'' do 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 assurances. The commenter suggested separating this section into a testing element and a remediation element. The commenter stated that a testing element related to ''reasonable assurances'' would assess the cyber capabilities of the organization to detect and prevent cyber incidents of a material nature, while a remediation element related to incident responses would assess the effectiveness of timely remediation of cyber incidents that have a material impact on the entity.

Proposed § 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.''

''Material'' in this context means to exclude small or *de minimis* deficiencies. Thus, System institutions may interpret ''material'' to mean anything that could potentially impact the safety and soundness of an institution or the accuracy of financial reporting. Internal controls should provide reasonable assurances that information and IT is reliable, accurate, and timely.

Internal controls are intended to prevent errors and irregularities, identify problems, and ensure corrective action. Internal controls can be expected to provide only reasonable, not absolute, assurances to an institution's management and board.

We continue to believe internal controls must provide reasonable assurances to prevent, detect, and remediate material deficiencies. We do not believe any change to the proposal is necessary. The regulation, as proposed, is clear on the need for adequate internal controls.

Privacy Framework (§ 609.930(d))

With respect to proposed § 609.930(d), commenters were concerned that this section does not provide expectations on the privacy framework, or other legal or compliance requirements. This section requires, in part, that an institution ''consider privacy and other legal compliance issues.''

We have decided not to specify a uniform privacy framework. Privacy frameworks can vary from state-to-state and from institution-to-institution. System institutions may consult the privacy framework established by NIST at *https://www.nist.gov/privacy-framework/privacy-framework.*

We finalize this section as proposed.

Reporting to the Board (§ 609.930(e))

As proposed, § 609.930(e) requires an institution to ''report quarterly to its board or an appropriate committee.'' One commenter suggested that quarterly reporting may not be the correct frequency to report to an institution's Board.

We concur with the suggestion that quarterly reporting may not be the correct reporting frequency. We revise this section to provide, ''[a]t a minimum, each institution must report quarterly to its board or an appropriate committee of the board.'' This will ensure that there is at least quarterly reporting to the board. Depending on the risk or information that must be communicated to the board, the frequency of reporting may need to increase, and conversely, a quarterly report to the board may be brief, as appropriate and in accordance with the institution's situation. The institution should have appropriate documentation to support the frequency of board reporting.

Cyber Risk Management Metrics (§ 609.930(e))

Section 609.930(e), as proposed, requires the report to the board to ''contain material matters and metrics related to the institution's cyber risk management program, including specific risks and threats.'' One commenter was concerned that the section does not provide a framework or expectation for the metrics presented to the board, or consider institutions

providing cyber metrics through another avenue, such as an entity-wide risk management report. The commenter believed that their concerns could lead to inconsistencies and misaligned expectations between examiners and institutions. The commenter suggested the rule should refer System institutions to modern frameworks based on industry standards, customized for its institution's risk environment, and aligned with its documented risk-based approach.

Upon further review, we delete the phrase ''and metrics'' from the final rule, but we decline to reference modern frameworks based on industry standards. Removing ''metrics'' should alleviate confusion from the proposed language. We continue to believe management should timely report on cyber risk management practices to the board or a committee of the board.

Technology Budget (§ 609.935(b))

One commenter stated that requiring an institution, per proposed § 609.935(b), to detail the technology budget in the technology plan could lead to unnecessary duplication. Some institutions present their technology budget to their boards with the overall operating expense budget. Another commenter objected to the requirement on how and when the information is to be presented.

We are not revising the proposed language. We believe there is little to no burden for institutions to include the technology budgets in the overall operating expense budgets, even if duplicative to other reports the boards might receive. Having a separate technology budget could benefit the board of directors by identifying the expenses incurred within the technology area. A separate technology budget is especially important as money spent in the technology area helps keep systems secure and adds more transparency to the technology area. Business planning is very important as institutions identify specific areas that should be reviewed, assessed, and evaluated. Board and management can use the technology budget to initiate discussions on spending for cyber risk management.

Identify and Assess Business Risk (§ 609.935(c))

One commenter stated proposed § 609.935(c) is unclear. Proposed § 609.935(c) requires institutions to identify and assess the business risk of proposed technology changes and assess the adequacy of the institution's cyber risk program. The commenter did not know whether the requirement in proposed § 609.935(c) is intended to assess the adequacy of the program as a whole or solely assess the proposed technology changes. No recommendation was provided.

To alleviate any confusion, we modify this section, so that the plan ''[i]dentifies and assesses the adequacy of the institution's entire cyber risk management program, including proposed technology changes.''

Records Retention (§ 609.945)

Several commenters stated that the proposed rule does not provide guidance on maintaining electronic records. Proposed § 609.945 requires ''records stored electronically must be accurate, accessible, and reproducible for later reference.'' The commenters stated that this section is silent on the scope and extent of the records and does not consider the institutions' data retention policies. The commenters recommended that we revise the rule to refer System institutions to modern frameworks based on industry standards, which would be customized for the institution's risk environment when defining the scope and extent of its electronic records retention program.

We are not revising the proposed language. This is the same language from the prior regulation on E–SIGN. This section will continue to hold institutions accountable for records retention in general. Institutions are still required to comply with E–SIGN, which is a statutory provision. Our existing E–SIGN regulations were educational and a reminder to institutions of their applicability.

As this is not a prescriptive rule, we have decided not to impose specific records retention schedules here. System institutions must continue to maintain their records to document their business decisions and to allow examiners to review such documents. Moreover, System institutions must have records retention programs that comply with their respective state and federal laws.

IV. Regulatory Analysis

A. Regulatory Flexibility Act

Pursuant to section 605(b) of the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), FCA hereby certifies that the Cyber Risk Management final rule will not have a significant economic impact on a substantial number of small entities. Each of the banks in the FCS, considered together with its affiliated associations, has assets and annual income more than the amounts that would qualify them as small entities. Therefore, FCS institutions are not ''small entities'' as defined in the Regulatory Flexibility Act.

Under the provisions of the Congressional Review Act (5 U.S.C. 801 *et seq.*), the Office of Management and Budget's Office of Information and Regulatory Affairs has determined that this final rule is not a ''major rule'' as the term is defined at 5 U.S.C. 804(2).

List of Subjects in 12 CFR Part 609

Agriculture, Banks, Banking, Electronic commerce, Reporting and recordkeeping requirements, Rural areas.

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

PART 609—CYBER RISK MANAGEMENT

Subpart A—General Rules

Subpart B—Standards for Boards and Management

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).

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.

Dated: December 6, 2023.

Ashley Waldron,

Secretary, Farm Credit Administration.

[FR Doc. 2023–27102 Filed 12–8–23; 8:45 am]

BILLING CODE 6705–01–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA–2023–1816; Project Identifier MCAI–2021–01460–R; Amendment 39–22599; AD 2023–22–15]

RIN 2120–AA64

Airworthiness Directives; Airbus Helicopters Deutschland GmbH (AHD) Helicopters

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.