



**America's
Credit Unions**

February 2, 2024

AI E.O. RFI Comments
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899–8900

**RE: NIST's Assignments under Sections 4.1, 4.5 and 11 of Executive Order 14110
Assignment; Docket No. 231218-0309**

Dear Sir or Madam:

On behalf of America's Credit Unions, we are writing in response to the request for information (RFI) issued by the National Institute of Standards and Technology (NIST) regarding certain obligations under Executive Order 14110, titled "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (the E.O.). America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the industry to effectively meet the needs of their nearly 140 million members nationwide. America's Credit Unions supports efforts to promote and encourage responsible innovation across all technological domains, including through the deployment of artificial intelligence (AI).

While new standards and guidelines for AI can help achieve regulatory clarity, they should be tailored to avoid excessive burden, competitive imbalance between regulated and unregulated institutions, or the imposition of unreasonable supervisory expectations for credit unions.¹ To avoid misalignment, duplication, or conflict with existing standards, NIST should consult with federal banking regulators to determine how any future statements or best practices published in response to the E.O. might be interpreted in the context of existing financial regulatory frameworks.

General Comments

As not-for-profit, member-owned financial institutions, the mission of credit unions is to serve their communities. AI-based technologies can help drive that mission forward, allowing credit unions to expand access to credit, improve member service, and streamline operations in a

¹ See Credit Union National Association, Letter to NCUA re: Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, available at https://www.cuna.org/content/dam/cuna/advocacy/letters-and-testimonials/2021/070121_CUNA%20AI%20Comment.pdf; see also National Association of Federally-Insured Credit Unions, Letter to NCUA re: Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, available at <https://www.nafcu.org/system/files/files/NAFCU%20-%20RFI%20on%20Artificial%20Intelligence%207.1.2021.pdf>.

competitive marketplace.² As highly regulated financial institutions, credit unions are aware of the potential legal and operational risks associated with AI. The scope of existing federal consumer financial law is not bounded by any technological limit; whether decisions are made by humans or machines, the outcome cannot be discriminatory, unfair, or dangerous for consumers.

The National Credit Union Administration (NCUA) and other federal banking regulators have long considered how rules governing banking services should account for new technology.³ The Federal Financial Institutions Examination Council (FFIEC) has specifically considered the consequences of financial institution use of AI.⁴ Credit unions must undertake risk assessments, perform due diligence, and undergo regular examination as part of a rigorous supervisory process. In this context, credit union use of AI is already subject to significant scrutiny, just like any other new technology. Accordingly, layering conflicting or overly prescriptive AI regulation on top of the myriad rules and guidelines already applicable to credit unions will only serve to chill adoption of a useful technology.

As NIST considers its obligations under the E.O., it should be mindful of how broadly defined guidance might hinder innovation. A one-size-fits-all approach for defining AI explainability or promoting AI safety (as those concepts are described in the E.O.) could correspond with excessive regulatory burden for credit unions, and potentially deprive credit union members of better service or more affordable products. NIST should also be aware that its guidance, even when proffered as a set of voluntary best practices, can still find its way into influential toolsets used by financial regulators.⁵ Accordingly, NIST should calibrate future statements and guidance by considering existing supervisory expectations for credit unions, with the goal of avoiding duplication or conflict with existing standards or laws.

NIST Should Avoid Duplication and Overlap with Existing Federal Financial Law

The RFI seeks input on NIST's obligations under sections 4.1, 4.5 and 11 of the E.O. In general, section 4 of the E.O. covers the development of guidelines, standards, and best practices for AI

² See CFPB, Advisory Committee Meeting Minutes, 4, (December 6, 2018) (“staff [from the CFPB’s Office of Consumer Lending, Reporting, and Collection Markets] noted that artificial intelligence use may help ‘thin file’ consumers reach mainstream credit”), *available at* https://files.consumerfinance.gov/f/documents/cfpb_advisory-committee-meeting-minutes_122018.pdf.

³ See e.g., Federal Financial Institutions Examination Council, IT Examination Handbook Infobase, *available at* <https://ithandbook.ffiec.gov/>; see also FFIEC, Guidance on Risk Management of Outsourced Technology Services (November 8, 200), *available at* https://www.ffiec.gov/exam/infobase/documents/02-ffi-risk_mang_outsourced_tech_services-001128.pdf.

⁴ See FFIEC, Architecture, Infrastructure and Operations, Section VII.D, *available at* <https://ithandbook.ffiec.gov/it-booklets/architecture-infrastructure-and-operations/vii-evolving-technologies/viid-artificial-intelligence-and-machine-learning/>.

⁵ See FFIEC, Cybersecurity Assessment Tool, <https://www.ffiec.gov/cyberassessmenttool.htm>.

safety and security.⁶ Section 4.5 covers standards for establishing the provenance of synthetic digital content. Each section has potentially broad applicability that could intersect with existing financial regulatory policy. In cases where future standards and guidelines might influence the application of existing federal financial law or supervisory expectations, NIST should consult with the heads of the federal banking regulators, including the NCUA, to avoid conflict or overlap.

Section 4.1(i)(C) of the E.O. directs NIST to “create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm.”⁷ The term “harm” can be broadly interpreted. In some regulatory contexts, the term “harm” may be used to describe a likelihood of substantial injury, inconvenience or a standard of materiality. The E.O. itself does not offer a precise benchmark, which could invite policymakers to adopt tolerances for AI risk that are not aligned with existing regulatory standards or definitions, or which vary arbitrarily between different regulators. NIST should strive to anticipate and avoid such misalignment.

With respect to potential cybersecurity implications for AI, the generality of section 4(i)(C) creates a high likelihood of overlap or conflict with existing NCUA standards for maintaining a comprehensive information security program.⁸ NIST should avoid endorsing standards that might impose, either directly or indirectly, conflicting or additional cybersecurity obligations on credit unions, whether in the form of new red-teaming requirements or similar audit features.

Credit unions receive regular examinations which include a comprehensive review of IT security. Consideration of specific controls, policies and procedures is not limited to any particular subset of technology. While AI risks may be unique, the purpose of the NCUA’s information security standards is not to anticipate every threat or vulnerability, but rather to direct attention to governance, risk management, and monitoring as threats evolve. In other words, if AI-related risks to the credit union are credible, credit unions have an obligation to adapt information security programs in response.⁹ NIST should consult with the NCUA and Treasury before promulgating standards that might bear upon how financial institution systems should be safeguarded or managed in response to potential AI threats. Such consultation would be consistent with section 4.3(ii) of the E.O., which assigns a primary responsibility to Treasury for identifying AI-specific cybersecurity risks and best practices relevant to financial institutions.

With respect to rights-impacting use of AI, federal consumer financial law already prohibits discrimination in the provision of credit through the Equal Credit Opportunity Act and

⁶ See NIST, Request for Information (RFI) Related to NIST's Assignments Under Sections 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence (Sections 4.1, 4.5, and 11), 88 Fed. Reg. 88368 (December 21, 2023).

⁷ E.O. 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75191 (November 1, 2023).

⁸ See Appendix A to 12 CFR Part 748

⁹ See Appendix A to 12 CFR Part 748, Section III.E (“Each credit union should monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology.”)

Regulation B.¹⁰ Furthermore, credit score models are subject to validation standards, and consumers are entitled to adverse action notices explaining why they have been denied credit.¹¹ For other types of AI-related activity that might be deemed harmful to individual rights, NIST should be aware that the Consumer Financial Protection Bureau (CFPB) maintains a broad and continuously evolving prohibition against unfair, deceptive, and abusive acts and practices (UDAAP) applicable to financial institution conduct.¹²

Most significant in the UDAAP context is the threshold for “harm” itself. The standard for unfairness requires a likelihood of “substantial injury;” however, no such condition exists with respect to practices that might be deemed abusive or deceptive. Furthermore, the CFPB has broadly classified certain AI-related risks, such as misleading chatbot interactions, as potentially harmful without establishing any thresholds for materiality or monetary injury.¹³ Defining AI-related harm broadly could vastly expand the scope of what the CFPB considers harmful under its own rules, which in turn might prompt credit union disengagement from AI to avoid heightened regulatory scrutiny.

The CFPB also enjoys significant latitude when interpreting its UDAAP prohibitions—a power that could chill pursuit of AI innovation among regulated institutions given the current Director’s warnings about such technology.¹⁴ NIST should recognize that the CFPB’s expansive authority can be magnified by NIST’s own statements, which have sometimes been cited as justification for new regulatory interpretations.¹⁵ To avoid the inadvertent creation of onerous or inconsistent standards specific to financial institution use of AI, NIST should consult with the FFIEC agencies and Treasury to determine how certain statements or best practices developed by NIST might be relied upon or interpreted by federal financial regulators.

Notwithstanding the extent of future interagency collaboration, NIST should not prescribe or endorse overly burdensome procedures for evaluating AI systems based on an amorphous

¹⁰ See generally, 12 CFR Part 1002 (Regulation B)

¹¹ See 12 CFR § 1002.2(p) (describing an “empirically derived, demonstrably and statistically sound, credit scoring system.”); § 1002.9 (adverse action notifications); see also Fair Housing Administration, Validation and Approval of Credit Score Models, 84 Fed. Reg. 41886 (August 16, 2019).

¹² See CFPB, Examination Manual, Unfair, Deceptive, or Abusive Acts or Practices, available at https://files.consumerfinance.gov/f/documents/cfpb_unfair-deceptive-abusive-acts-practices-udaaps_procedures_2023-09.pdf

¹³ See CFPB, Chatbots in Consumer Finance (June 6, 2023), available at <https://www.consumerfinance.gov/data-research/research-reports/chatbots-in-consumer-finance/chatbots-in-consumer-finance/>. Notably, the CFPB provides the caveat that its analysis of AI usage in chatbots “is not intended to impose any obligations or define any rights and is not intended as a CFPB interpretation of any regulation or statute.”

¹⁴ See CFPB, Director Chopra’s Prepared Remarks on the Interagency Enforcement Policy Statement on “Artificial Intelligence” (April 25, 2023) (“While machines crunching numbers might seem capable of taking human bias out of the equation, that’s not what is happening.”)

¹⁵ See CFPB, Consumer Financial Protection Circular 2022-04, FN.25 (August 11, 2022), available at <https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/> (citing NIST’s Digital Identity Guidelines to support the statement that an institution lacking multifactor authentication or similar security measures is unlikely to demonstrate “countervailing benefits to consumers or competition outweigh the potential harms, thus triggering liability”).

standard of “harm.” A balance must be struck between regulatory curiosity and what is practical in terms of how institutions demonstrate that their use of AI is responsible and safe. For most credit unions, the deployment of AI will involve third parties who may not share proprietary code for underlying models or training algorithms. Requiring end-users of AI to attest to the innerworkings of third-party models will be impractical in such circumstances. To preserve credit unions’ ability to meaningfully leverage AI, particularly when resources for in-house development are lacking, analysis of AI decision making should emphasize outcome-based assessments or self-testing—activities credit unions already perform to comply with antidiscrimination laws.

Adoption of onerous criteria for establishing AI explainability could also have the unintended effect of rewarding the largest, incumbent users of such technology. Such an outcome would stand in contrast with the goal outlined in section 5.3 of the E.O., which is to promote competition in AI. The typical credit union has less than \$56 million in total assets, a size that stands in stark contrast to the trillion-plus footprint of the four largest U.S. banks.¹⁶ AI could help smaller, community institutions such as credit unions compete with the largest banks by granting outside advantages in efficiency, automation, and analytics.¹⁷ But these advantages can only be fully realized in a regulatory environment that acknowledges the resource limitations of smaller, community based institutions. AI cannot realistically provide a benefit to members if the regulatory costs of adoption are disproportionately high. Ultimately a range of methods for assessing the safety of AI may depend on the type of industry involved and the extent of existing federal oversight. Accordingly, NIST should distinguish between the use of AI by unregulated institutions versus those that are subject to regular supervision, such as credit unions.

Synthetic Content Generated by Financial Institutions

Section 4.5 of the E.O. is aimed at reducing the risks posed by “synthetic content,” which is broadly defined as information that has been significantly modified or generated by algorithms, including by AI. An algorithm, while undefined in the E.O., can be any set of rules that if followed will generate a prescribed result, potentially encompassing automated decisions that depend on simple business logic. While the focus of the E.O. and NIST’s RFI appears narrowly focused on the output of generative AI models, section 4.5(a)(vi) asks the Secretary of Commerce to consider techniques for “auditing and maintaining synthetic content.” NIST should clarify that the scope of this section does not extend to the use of consumer-facing chatbots used for automating consumer interactions with financial institutions.

Use of chatbots by financial institutions has traditionally relied upon rules-based systems; however, recent research suggests that some institutions are moving towards large language

¹⁶ “Typical” is used to mean the median asset size. See NCUA, Quarterly Credit Union Data Summary 2023 Q3, available at <https://ncua.gov/files/publications/analysis/quarterly-data-summary-2023-Q3.pdf>.

¹⁷ See OECD, Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers, 7 (2021), available at <https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf>.

models (LLMs).¹⁸ The output of these models could be considered synthetic content. The CFPB has noted certain risks applicable to both rules-based and LLM powered chatbots with a common theme being a failure to provide responsive customer service and the absence of a human agent as backup—issues outside the scope of this RFI. However, some risks unique to LLM-based chatbots could implicate section 4.5(a)(vi) of the E.O. The CFPB has asserted that ingestion of sensitive consumer information by AI agents must be subject to appropriate guardrails. Despite this position, the CFPB has not proposed new standards or regulation specific to AI use, preferring instead to monitor the market for these services.

Development of standards for “auditing and maintaining” the synthetic output of financial institution AI services, including chatbots, is best reserved to the NCUA and other federal banking agencies, whose supervisory authority puts them in a better position to understand their regulated institutions’ use of these services. Chatbots used by financial institutions are highly orchestrated services and are not designed to deviate from narrowly defined parameters. As with other AI services, chatbots are also subject to existing consumer financial laws—meaning they cannot perpetuate unfair, misleading or abusive practices. Accordingly, NIST should focus its efforts on identifying ways to manage the risk of synthetic outputs of models offered by unregulated companies—not credit unions.

Government Transparency and Supervisory Use of AI

NIST should consider developing standards to enable financial institutions to better understand actions taken by their regulators which are the result of AI-drive decisions or assessments, consistent with section 4.5(c) of the E.O. The CFPB’s FY 2023 Annual Performance Report states that the CFPB continues “to assess sources and capabilities that will provide an enhanced data-driven approach to its areas of supervisory focus.”¹⁹ The report provides the specific insight that the CFPB is now “[I]everaging additional data sources as well as artificial intelligence within the supervisory prioritization process.”²⁰ To date, the CFPB has shared very little information about its use of AI to perform supervisory prioritization.

Credit unions and other regulated financial institutions deserve to know how they are being evaluated by the CFPB and other government agencies for compliance with federal law. Algorithms that dictate supervisory focus should be disclosed to regulated institutions, and NIST should consider ways to enhance disclosure of AI-based supervisory tools or processes for all federal financial regulators.

Conclusion

AI can enhance credit unions’ ability to serve their communities with safe and affordable financial products and services. Yet to fully realize this potential, credit unions must have

¹⁸ See *supra* note 13.

¹⁹ See CFPB, FY 2023 Annual Performance Report, 85 (February 2023)

²⁰ *Id.*

confidence that innovation will not be penalized with heavy-handed regulation. Credit unions are already subject to rules governing nearly every facet of their operations—from advertising to extensions of credit. NIST should consider this context and the broad applicability of federal consumer financial law as it considers how best to execute its obligations under the E.O. NIST should also consult with the NCUA and other federal banking agencies to avoid duplication and conflict with existing laws and standards, and to promote greater transparency regarding the use of AI as a supervisory tool.

Thank you for the opportunity to provide comments in response to this request for information. If you have any questions, please do not hesitate to contact me at 703-842-2266 or amorris@americascreditunions.org.

Sincerely,

A handwritten signature in black ink that reads "Andrew Morris". The signature is written in a cursive style with a horizontal line at the end.

Andrew Morris
Senior Counsel for Research and Policy