

Federal Deposit Insurance Corporation (FDIC) Compliance Plan for OMB Memorandum M-25-21 – September 2025

Prepared by Michael W. Simon, Chief Artificial Intelligence (AI) Officer

The following information is provided in response to the requirements for a Compliance Plan as outlined in Memorandum M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust."

1. Driving Al Innovation

REMOVING BARRIERS TO THE RESPONSIBLE USE OF AI:

The Chief Artificial Intelligence Officer (CAIO) and Chief Data Officer (CDO) have not identified any unique barriers to the responsible use of AI at the FDIC. The FDIC has proactively taken steps to enhance access to the necessary software tools, open-source libraries, and deployment and monitoring capabilities needed to rapidly develop, test, and maintain AI applications. To this end, and among other activities, the FDIC has implemented a secure suite of integrated enterprise cloud capabilities to meet enterprise advanced data analytic and AI business modernization needs.

SHARING AND REUSE:

At the FDIC, the CAIO and CDO centrally oversee the Divisions' and Offices' use of AI. The FDIC maintains an AI Coordination Committee (AICC) – with representatives selected by Division and Office Directors – to develop, document, and share AI governance and risk management procedures. These representatives are responsible for updating and maintaining the AI use case inventory for their respective Divisions and Offices. Collaboration is further supported by the FDIC's AI Community of Practice, which routinely brings together AI practitioners who train, educate, document and share best practices regarding AI innovation. In addition, various Divisions and Offices, geographic areas, and other working groups pursue training, education and sharing of AI best practices in a variety of settings. Beyond the aforementioned efforts, sharing and reuse of AI code, models, and data assets occurs on a situational basis.

AI TALENT:

In 2024, FDIC developed an enterprise level AI workforce development plan and is currently conducting internal training in AI fundamentals for practitioners and AI enablers. Specific training will be made available for new AI tools and capabilities, as well as customized training that is tailored to individual learning experiences to meet organizational needs and goals. FDIC staff also participate regularly in government-wide AI training events. Aided by continued collaboration, AI expertise is maintained across numerous Divisions and Offices, where talent and recruitment decisions are made. Individuals with technical talent make major contributions in all parts of the Corporation.

2. Improving AI Governance

AGENCY POLICIES:



Consistent with M-25-21, the FDIC is reviewing its internal policies on IT infrastructure, data, cybersecurity, and privacy to maintain alignment with the requirements of M-25-21, Executive Order 14179, Executive Order 13960, and applicable law. Among other activities, FDIC is updating the existing Acceptable Use Policy for FDIC Information Technology to cover the use by FDIC staff of generative AI to encourage innovation while also including safeguards and oversight mechanisms to address key risks. Certain acceptable use policies relating to specific generative AI use cases are already in place for tools that have undergone generative AI risk assessment to address specific, identified risks, and mitigants (e.g., coding assistance).

AI USE CASE INVENTORY:

The CAIO and CDO provide the AICC with a uniform template that is compliant with OMB use case inventory instructions and technical assistance as needed. Use case listings are vetted within each Division and Office to ensure comprehensiveness; particular attention is paid to existing use cases to determine whether updates are necessary. Responses to the inventory questions are reviewed by appropriate subject-matter experts within FDIC to ensure accuracy, such as the coordination of privacy-related questions with the FDIC's Privacy Program and Chief Privacy Officer. In addition, FDIC may conduct audits of IT platforms that include AI tools.

3. Fostering Public Trust in Federal Use of AI

DETERMINATIONS OF PRESUMED HIGH-IMPACT AI:

In addition to the ongoing process to inventory AI use cases, each Division and Office maintains an OMB-compliant template in which potential high-impact uses are documented. The CAIO consults as necessary with other stakeholders, subject matter experts, and the Privacy Program to determine whether these use cases are high-impact.

The FDIC will conduct an AI impact assessment before deploying any high-impact AI use case. The assessments will document and address: (a) the intended purpose for the AI, (b) the expected benefit of the AI, (c) the quality and appropriateness of relevant data and model capability, (d) the potential impacts of using or not using AI, including impacts on privacy, civil rights, and civil liberties, (e) reassessment scheduling and procedures, (f) related costs analysis with documentary support, (g) the results of an independent, intra-agency review, and (h) risk acceptance, signed by the individual at the FDIC accepting the risk.

In consultation with relevant officials – including the Privacy Program, the CAIO, and CDO – staff develop tailored risk mitigation procedures for each high-impact use case. As part of their AI assessments, relevant FDIC executives evaluate the risk mitigation procedures, as well as the need to ensure the stability and continuity of FDIC operations. After they conduct this evaluation, they decide whether to proceed with the AI use case (via a waiver of one or more of the OMB risk management practices, or by following the proposed risk mitigation procedures) or terminate the AI use case.

The FDIC seeks to ensure that AI operators receive sufficient training, assessment, and oversight regarding the specific AI functionality at issue to interpret output and manage associated risks. Where any potential high-impact use cases are involved, the FDIC will appropriately provide for human oversight, intervention, and accountability and, as needed, will consider including a fail-safe to minimize the risk of significant harm. The FDIC recognizes the importance of ensuring that, when appropriate, individuals affected by AI-enabled decisions receive timely human review and a chance to appeal negative impacts. In that regard, the FDIC will consider



whether and how to develop remedies and design appeal procedures to avoid unnecessary burdens on individuals. The FDIC is also reviewing ways to solicit feedback from end users and the public on AI use cases.

The CAIO and CDO staff will, as necessary, request and centrally track any waivers, reassess them if there are significant changes to the conditions or context, and report to OMB on the scope and justification for waivers or revocations. With respect to any waivers that may be requested, the CAIO will also certify the ongoing validity of, or revoke, each waiver on an annual basis. The CAIO and CDO staff will also, where permissible, publicly release a summary describing each individual determination and waiver, along with a justification and publicly indicate if the FDIC has no active determinations or waivers.

IMPLEMENTATION OF RISK MANAGEMENT PRACTICES AND TERMINATION OF NON-COMPLIANT AI:

For approved high-impact use cases, in coordination with other appropriate officials, such as the Chief Privacy Officer and the Chief Information Security Officer, the CAIO and CDO will oversee the implementation of risk mitigation procedures. On an annual basis, relevant executives will renew or update their decisions on whether to terminate the AI use cases and if so, coordinate with the Office of the Chief Information Security Officer to discontinue the terminated AI use case.

Through testing and periodic human review, the FDIC will monitor AI performance and potential adverse impacts. Such monitoring is designed to detect unforeseen circumstances or changes to the AI, the context, or the data. The FDIC's monitoring will implement appropriate mitigations and require proper system and use documentation. Wherever possible, the FDIC will develop processes that enable traceability and transparency.