Compliance Plan for OMB Memorandum M-25-21

September 26, 2025

Version: 1.0

Prepared and Issued by: Chris Chilbert, Chief Information Officer and Acting Chief AI Officer

1. Background

The Consumer Financial Protection Bureau (CFPB) is committed to adopting artificial intelligence (AI) technologies in a responsible, transparent, and tailored manner. While the CFPB's AI adoption is currently limited in scope and scale, we recognize the importance of aligning with OMB Memorandum M-25-21, the AI in Government Act of 2020, and the Advancing American Artificial Intelligence Act of 2022. This compliance plan outlines our strategy for overcoming barriers to responsible AI use, implementing effective governance structures, and fostering public trust through transparent and accountable practices.

2. Driving AI Innovation

2.1. Removing Barriers to the Responsible Use of AI

The CFPB is working to develop strategies that allow for the responsible, safe, secure, and effective use of artificial intelligence (AI) and related technologies. The work underway includes developing CFPB's AI compliance plan, standing up a collaborative AI Governance Board, leveraging existing governance processes, and hosting a CFPB AI Community of Practice group.

Our innovation strategy prioritizes low-risk, incremental use of AI within mission support and administrative functions. We aim to utilize AI to automate document classification, enhance internal workflows, and facilitate limited data analysis tasks. Our approach emphasizes leveraging Federal shared services such as USAi.gov, acquiring FedRAMP-authorized AI tools, and maximizing the reuse of government-wide models and solutions where feasible. Innovation at the CFPB will focus on efficiency, cost-effectiveness, and experimentation with existing technologies under proper oversight.

The CFPB faces several challenges in adopting AI responsibly and securely. These challenges include limited technical, legal, cybersecurity, and privacy resources for vetting and implementing AI use cases. We are addressing these barriers by collaborating with the Small Agency Chief Information Officer (CIO) and Chief Information Security Officer (CISO) Councils to identify shared resources and contract vehicles, and by prioritizing low-risk AI experiments within our existing cloud environment. We also seek to leverage existing partnerships with GSA and CISA for guidance and infrastructure support.

2.2. Sharing and Reuse

Most AI tools that CFPB adopts will be acquired or pre-integrated into existing software platforms. We have begun coordination among IT, cybersecurity, privacy, and legal staff to track use cases and metadata standards that support reuse and documentation. We also plan to engage with USAi.gov, Code.gov, and GSA's AI Community of Practice to align our efforts with federal guidance.

We aim to develop a centralized cloud-based knowledge and tool management platform that provides standard tools and resources for securely building, training, and deploying all AI capabilities across the Bureau.

2.3. AI Talent

The CFPB has dedicated teams in data science, data analytics, data management, and data engineering teams. Within these teams, there are experts in artificial intelligence (AI), machine learning, and AI Strategy.

Our goal is to build awareness and accelerate adoption of AI across the entire CFPB workforce. We are prioritizing training in risk management and legal compliance as they relate to vendor-provided artificial intelligence as well as using AI to increase productivity and automate manual processes. We also support interagency training events and rotational assignments to temporarily bring in technical expertise.

We have also established an AI Community of Practice (AI COP) to provide bureau-wide outreach, connect employees with training resources, and to create a collaborative forum for knowledge sharing, peer learning, and accelerating AI adoption. The AI COP will help identify gaps in AI skillsets and support the CFPB's Chief Artificial Intelligence Officer (CAIO) in addressing those gaps.

3. Improving AI Governance

3.1. AI Governance Board

The CFPB has existing Information Technology (IT) governance bodies that facilitate technology and data management. The CFPB is standing up a similarly structured governance body for AI. We have designated a small cross-functional working group led by the CIO/CAIO to review and approve the use of AI and associated risks. This body coordinates internal policy alignment, cybersecurity risk review, privacy impact assessments, and cross-agency collaboration. Our approach is designed to ensure appropriate scrutiny, documentation, and compliance without creating unnecessary administrative burden. This group will include representatives from IT, acquisition, legal, cybersecurity, privacy, and civil rights to review and approve new AI use cases. When relevant, the AI governance boards will include representatives from the following disciplines: agency management, human capital, procurement, and officials responsible for implementing AI within an agency's program office(s). The group will consult with federal guidance and external subject matter experts (SMEs) as needed and participates in relevant interagency communities.

3.2. Agency Policies

The CFPB is updating its IT acquisition standard operating procedures (SOPs) to require AI use case review and documentation before procurement. The CFPB is also updating its IT deployment and development SOPs to address AI use cases. We have revised our internal IT policy to reflect FedRAMP and OMB guidance on data provenance and the use of machine learning-based tools. A draft policy on generative AI is currently underway, focusing on appropriate use guidelines, transparency, and employee training. We will finalize this policy by January 2026.

In addition, we will leverage forthcoming policy guidelines and documents being developed under the leadership of the Federal CIO and the Chief AI Officer's Council. These resources will help ensure our internal AI policies remain aligned with government-wide standard and best practices as they are rolled out this year.

3.3. AI Use Case Inventory

The CFPB is developing a streamlined process to collect input from each program office on any planned or existing AI use cases, including the use of embedded AI in commercial software. The CIO office will maintain the central inventory. For each use case, staff will document its purpose, inputs, outputs, and whether it meets the definition of high impact. Updates will be solicited annually and at the time of significant changes. CFPB will submit the inventory to OMB and post a public version on the CFPB website in accordance with forthcoming OMB guidance and the requirements of the Advancing American Artificial Intelligence Act of 2022.

4. Fostering Public Trust in Federal Use of AI

4.1. Determinations of Presumed High-Impact AI

The CIO/CAIO will review all new and existing AI use cases against the high-impact criteria in M-25-21. As a baseline, we will consider any AI used in program decisions, public interactions, or oversight activities for further scrutiny.

4.2. Implementation of Risk Management Practices and Termination of Non-Compliant AI

The CIO/CAIO will ensure that all AI use cases, and software obtain an authority to operate prior to deployment, and AI impact assessments are conducted for any high-impact use cases. If we lack source access to proprietary models, we will implement alternative evaluation methods such as output monitoring and vendor attestations. Any AI use that fails to meet minimum safeguards will be suspended, and a remediation plan will be developed. The CIO maintains the

authority to approve or revoke the use of AI, with input from our the CFPB AI Governance board. To address the risk of AI use cases that program offices fail to report, or don't realize are AI use cases, the Office of Cybersecurity monitors IT activity to discover potential use of unauthorized AI using the same approach as "Shadow IT" discovery.

APPENDIX A:

TERMS AND DEFINITIONS

Technology Resources – means hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including, but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

Artificial Intelligence - (1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks. (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task. (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

References

https://www.nist.gov/artificial-intelligence/ai-research/nists-ai-standards-zero-drafts-pilot-project-accelerate NIST's AI Standards "Zero Drafts" Pilot Project to Accelerate Standardization, Broaden Input

https://www.nist.gov/itl/ai-risk-management-framework NIST's AI Risk Management Framework

Pub. L. No. 116-260, div. U, title 1, § 104 (40 U.S.C. § 11301 note), https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf.

OMB Memorandum M-25-21, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust (Apr. 3, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf.