



Artificial Intelligence Compliance Plan for OMB Memorandum M-25-21

September 2025

Contents

Introduction	3
1. Driving AI Innovation	3
1.1. Removing Barriers to the Responsible Use of AI	3
1.2. Sharing and Reuse	3
1.3. AI Talent	4
2. AI Maturity Goals.....	4
2.1. AI Governance Board.....	4
2.2. Agency Policies.....	4
2.3. AI Use Case Inventory.....	4
3. Shared Services and External Collaboration	5
3.1. Determinations of Presumed High-Impact AI.....	5
3.2. Implementation of Risk Management Practices.....	5

Introduction

The U.S. Election Assistance Commission (EAC) is an independent, bipartisan federal agency charged with supporting the administration of elections for federal office by developing guidance, adopting voluntary voting system guidelines, and serving as a national clearinghouse of information on election administration. As artificial intelligence (AI) technologies rapidly evolve, the EAC is committed to adopting AI in a responsible manner that enhances operational efficiency, safeguards the public trust, and upholds the highest standards of transparency, ethics, and accountability. This compliance plan outlines the EAC's approach to AI governance in accordance with Executive Order 14179, titled "Removing Barriers to American Leadership in Artificial Intelligence" and implementing guidance provided by OMB Memorandum M-25-21, emphasizing responsible experimentation, risk management, and interagency collaboration.

1. Driving AI Innovation

1.1. Removing Barriers to the Responsible Use of AI

Under the direction of the EAC Commissioners and Executive Director, the EAC will enable compliant AI adoption under M-25-21. As part of this effort, the EAC will operate a standardized AI intake and pre-deployment review managed by the CAIO in coordination with the office of the Chief Information Officer (OCIO), the office of General Counsel (OGC), the office of the Chief Financial Officer (OCFO). Every proposed use will be logged in the central AI use case inventory and will require a pre-deployment checklist, minimal documentation sufficient for required assessments (purpose, inputs, outputs, safeguards), and output monitoring to validate controls. Acquisition and terms of service documentation will be captured at intake to support oversight activities.

To remove procedural and resourcing hurdles, the EAC is updating acquisition SOPs and standard clauses to require the transparency and documentation necessary for M-25-21 (e.g., performance metrics, data/model portability and rights, and information needed to complete required assessments); leveraging shared services and technical guidance from interagency partners (GSA, CAIO Council, and Small Agency CIO/CISO Councils); and aligning staff training and an approved AI systems list with the agency's Staff AI Use Policy. These steps streamline compliant adoption while ensuring the EAC can meet OMB's plan, finalization, posting, and inventory timelines.

1.2. Sharing and Reuse

Given the EAC's small size and limited internal development capacity, most AI tools will be acquired or pre-integrated into existing software platforms. The CAIO will coordinate with OCIO to track use cases and metadata standards that support reuse and documentation. If AI code and models are created by the agency, OCIO will serve as the central repository for sharing any data where it is contractually and legally permissible to do so. Where possible, the EAC will publish assets in line with federal open-source and data-sharing practices, and update

acquisition procedures to require deliverables that enable reuse and portability. The EAC also plans to engage with GSA's AI Community of Practice to align the agency's efforts with federal guidance, ensuring transparency and maximizing the value of AI resources.

1.3. AI Talent

Beyond the Chief AI Officer, the EAC does not currently have dedicated AI staff. The EAC is building practical, role-based AI literacy across OCIO and program teams through short, targeted training on responsible use, risk management, bias mitigation, privacy, and acquisition of vendor provided AI. The agency will leverage federal resources (e.g., OPM's AI Fundamentals and GSA's AI Community of Practice) and, when needed, bring in technical depth through interagency training. Additionally, internal staff may support AI activities through work details or other short-term rotational assignments. These actions enable the agency to evaluate, acquire, and oversee AI systems in line with OMB guidance and the agency's internal policy.

2. AI Maturity Goals

2.1. AI Governance Board

In accordance with M-25-21, the EAC established a cross functional AI Governance Board, chaired by the CAIO and including the Executive Director, CIO/CISO, CFO, CEIO, CETO, and General Counsel to review proposed AI use cases. This body meets regularly to discuss OMB criteria, coordinate required assessments, and route any high impact determinations to the commissioners for elevated review. The CAIO, as directed by the AI Governance Board, may consult interagency communities and external subject matter experts on an as-needed basis. This structure provides accountability for approvals and ensures consistent implementation of governance practices across programs.

2.2. Agency Policies

To align with OMB guidance, the EAC is updating internal policies and acquisition procedures to require AI-specific documentation at intake (purpose, inputs, outputs, safeguards), use of FedRAMP-authorized environments, and vendor transparency sufficient to complete required assessments. The Staff AI Use Policy defines key terms, establishes roles, and outlines prohibited uses of approved systems. The EAC will finalize generative-AI policies focused on use restrictions, transparency, and workforce training. Contract language will address data and model portability, performance tracking, data privacy and security, and support ongoing oversight.

2.3. AI Use Case Inventory

OCIO will maintain a centralized inventory that captures all AI use cases. For each entry, the CAIO will document business purpose, inputs/outputs, data provenance, safeguards, and

whether the use meets OMB's high impact definition. Required updates will be made when significant changes occur. Inventory data supports required public reporting and internal gating (e.g., pre-deployment checks for higher risk uses) The CAIO will ensure this inventory is complete and track any necessary updates. The EAC will inventory its AI use cases at least annually, submit the inventory to OMB, and post a public version on the agency's website.

3. Shared Services and External Collaboration

3.1. Determinations of Presumed High-Impact AI

The CAIO will review any proposed or pre-existing AI use cases against the high-impact criteria in M-25-21 and flag any AI used in program decisions, public interactions, or oversight activities for further scrutiny. The EAC will document the implementation of the minimum practices in Section 4(b) of M-25-21 for high impact uses of AI and be prepared to report them to OMB, as part of periodic accountability reviews, the annual AI use case inventory, or upon request as determined by OMB.

The Chair or their designee, in coordination with the AI Governance Board, may waive one or more of the requirements in this section for a specific covered AI application or component after making a written determination, based upon a system-specific and context-specific risk assessment, that fulfilling the requirement would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations. Waivers will be tracked in a central log maintained by the CAIO. The CAIO, in coordination with other relevant officials, must certify to OMB the ongoing validity of each waiver on an annual basis, and may also revoke a previously issued waiver at any time.

3.2. Implementation of Risk Management Practices

The CAIO will ensure pre-deployment reviews and testing procedures, as well as AI impact assessments that are conducted for any high-impact use cases. If the EAC lacks source access to proprietary models, the agency will implement alternative evaluation methods such as output monitoring and vendor attestations. Any AI use that fails to meet minimum safeguards will not be deployed or will be suspended and a remediation plan will be developed. The CIO/CISO maintains the authority to approve or revoke the use of AI, with input from the EAC's AI Governance Board and EAC Commissioners. The EAC will conduct testing and periodic human review of AI use cases, where feasible, to identify any adverse impacts to the performance and security of AI functionality, including those that may violate laws governing privacy, civil rights, or civil liberties. The EAC will implement appropriate mitigations and ensure proper system and use documentation; and where possible, develop processes enabling traceability and transparency in this evaluation.