OMB GUIDANCE ON AGENCY AI COMPLIANCE PLANS PER M-25-21

September 16, 2025

Overview

The AI in Government Act of 2020[1] and Office of Management and Budget (OMB) Memorandum M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*,[2] direct each agency to submit to OMB and post publicly on the agency's website either a plan to achieve consistency with M-25-21, or a written determination that the agency does not use and does not anticipate using covered AI.

This document outlines the minimum information required from agencies in their compliance plans, which will satisfy the requirements of Section 3(b)(ii) of the Appendix to OMB Memorandum M-25-21 and Section 104(c) of the AI in Government Act. Agencies will report compliance with the case-specific practices mandated in Section 4 of the M-25-21 Appendix separately, through the annual AI use case inventory.

Instructions

If an agency does use or does anticipate using covered AI:

a. The agency must finalize its compliance plan within 180 days of the issuance of OMB Memorandum M-25-21, which is September 30, 2025.
b. The compliance plan must contain, at a minimum, responses to the questions identified in the Appendix of this document. Agencies must also update their compliance plans within 180 days of any update to OMB Memorandum M-25-21. OMB will revise this format as appropriate throughout the lifetime of this requirement.
c. Agency compliance plans must be publicly released and should be posted at [agency].gov/ai.

If an agency does not use and does not anticipate using covered AI:

a. The agency must send a signed letter from the agency Chief AI Officer (CAIO) to OFCIO_AI@omb.eop.gov with a written determination by September 30, 2025. The signed letter should describe the process by which the agency assessed that it does not use and does not anticipate using covered AI,[3] and also the frequency with which the agency will reassess its enterprise environment for active AI uses.
b. The agency must also post a notice at [agency].gov/ai with a statement indicating no current or anticipated use of AI technology. Notices should be posted in HTML format.
c. Upon notification that the agency does use or anticipates using covered AI, an agency CAIO must produce and post publicly a compliance plan within 180 days.

---

[1] 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.

[2] 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.

[3] The assessment should include a description of the process by which the agency consulted relevant officials such as Chief Data Officers, Chief Information Officers, Chief Technology Officers, Chief Acquisition Officials and Senior Procurement Executives, and other officials responsible for certain agency functions that may encompass the use of AI. The assessment must encompass a review of all sub-agencies, components, or bureaus within the agency.

COURT SERVICES AND OFFENDER SUPERVISION AGENCY (CSOSA)
COMPLIANCE PLANS
for
OMB Memorandum M-25-21
September 2025

- Prepared by Richard Wainwright, Chief Information Security Officer
- Issued by William Kirkendale, Chief Information Officer & Chief AI Officer

WILLIAM KIRKENDALE

Digitally signed by WILLIAM KIRKENDALE
Date: 2025.10.03 11:40:52 -04'00'

1. Driving AI Innovation

Removing Barriers to the Responsible Use of AI

- Describe any barriers to your agency's responsible use of AI, and any steps your agency has taken (or plans to take) to mitigate or remove these identified barriers.

  There are no explicit barriers to the responsible use of AI at CSOSA. However, some pressures exist to slow the adoption of new capabilities that apply broadly and are not exclusive to AI:
  - AI use cases compete for funding and staffing with other important priorities at the agency, including non-IT investments in core CSOSA capabilities, cybersecurity, and different use cases in our modernization agenda.
  - A planning process to line up work against funding and resources that typically requires a budget cycle to implement significant new initiatives.

  CSOSA simultaneously has some advantages in the adoption of AI and currently has a posture that is relatively permissive concerning the adoption of non-high-impact AI:
  - The agency predominantly deals with moderate sensitivity, open source, and commercially provided information. Many promising use cases being explored avoid safety and rights-impacting domains, reducing barriers to implementation.
  - The agency's technology is dominated by commercial off-the-shelf capabilities, rapidly accreting beneficial AI as a natural extension of its capabilities.
  - As a small agency, decision-making is relatively nimble and speedy compared to larger organizations.

Sharing and Reuse

- Explain how your agency coordinates internally to promote the sharing and reuse of AI code, models, and data assets. Describe the resources needed to enable this type of activity further.

  CSOSA's current technology footprint is almost exclusively based on commercial software products, with few modifications tailored to CSOSA's needs. In the few places that CSOSA is responsible for software development, the systems are primarily transaction processing and do not currently rely on AI capabilities. As such, CSOSA does not currently have use cases that are relevant to Section 4(d) of M-25-21.

AI Talent

- Describe any planned or in-progress initiatives from your agency to enhance AI talent. In

particular, identify the AI skillsets needed at your agency and where individuals with technical talent could have the most impact.

Building and maintaining a skilled AI workforce is crucial for advancing responsible AI innovation. CSOSA's initiatives in this area include:

- *Talent/Human Resource Planning*: As part of its annual human capital process, CSOSA identifies strategic trends and emerging talent, as well as the human resources required to support CSOSA's strategy. In this year's technology team planning, although no specific positions were identified as exclusive to AI, several roles required incorporating AI skills as part of their natural evolution.
- *Internal Training Programs*: CSOSA's AI governance body curates and promotes training programs to enhance AI skills within our workforce. These programs cover a range of topics, from basic AI literacy to advanced concepts in cyber and generative AI.

CSOSA does not currently have an explicit strategy for recruiting individual AI talent. However, it plans to identify specific duties within position descriptions that are important for CSOSA's adoption of ethical and safe AI use. This plan includes the Office of Information Technology (OIT) partnering with the Agency's Office of Human Resources (OHR) recruitment, staffing, and classification team to complete an analysis of positions to identify the AI and AI-enabling roles, upon determining the roles, assessing and updating the position descriptions, and creating related internal training opportunities. If gaps in the workforce are identified, OIT, in conjunction with the Agency leadership, establishes new positions and implements a targeted recruitment strategy to attract top talent for these roles.

One of the training paths is role-based (e.g., focusing on leadership, acquisition workforce, hiring teams, software engineers, administrative personnel, or others). In FY25, CSOSA anticipates launching a baseline assessment of agency AI skills to track progress as part of its program to develop AI capabilities within the Agency.

2. Improving AI Governance

<u>AI Governance Board</u>

- Describe your agency's AI governance body and the plan to achieve its expected outcomes. In particular, identify the offices that are represented on your agency's AI governance board and describe how, if at all, your agency's AI governance board plans to consult with external experts or across the Federal Government.

  Key CSOSA officials are members of federal user groups and private sector organizations that, like the technology community, share developing AI best practices, risks, and innovation through the lens of their function and professional area of responsibility.

  As a non-Chief Financial Officers Act (CFO Act) agency, CSOSA is not required to report on AI Governance Boards.

<u>Agency Policies</u>

- Describe any planned or current efforts within your agency to update any existing internal

AI principles, guidelines, or policies to ensure consistency with M-25-21.

- Updated CSOSA's mandatory annual Security Awareness Training to include a discussion of AI security issues, focusing on using AI in decision-making, protecting agency confidential information, employee accountability for work products, and IP ownership.
- Updated the Agency's Technology Review Process, codified in CSOSA's Capital Planning and Investment Control process and System Development Life Cycle (SDLC) policy, highlighting AI governance.
- Established IT Security Officer (CISO) and IT Security Office as the clearinghouse for questions, concerns, and related guidance regarding AI use within the Agency. This includes AI use under the control of CSOSA and AI use by stakeholders and customers, as well as how the agency should interact with those capabilities.

- Identify whether your agency has developed (or is in the process of creating) internal guidance for the use of generative AI.
  - Issued the Use of Generative AI Tools Guidance in March 2024.
  - Updated and released the IT Rules of Behavior to all Agency employees as part of the FY 2025 annual certification to strengthen employees' understanding of the safe and ethical use of Agency technology and their obligations to protect Agency information
  - OIT, in conjunction with the Office of Policy Analysis (OPA), is developing the Generative AI policy to be completed within 270 days of the M-25-21 issuance.
  - OIT and OPA are engaged in discussions with the Office of Administration (OA) on how best to approach AI acquisition guidelines that are consistent with M-25-21 & M-25-22 requirements and the pending revisions to Federal Acquisition Regulations (FARs).

AI Use Case Inventory

- Describe your agency's process for soliciting and collecting AI use cases across all subagencies, components, or bureaus for the inventory. In particular, address how your agency plans to ensure your inventory is comprehensive, complete and encompasses updates to existing use cases.

  Creating and maintaining AI use case inventories is essential to ensure that CSOSA understands how AI technologies are used across the Agency. This inventory process allows CSOSA to manage AI deployments effectively, ensuring alignment with our mission, ethical standards, and regulatory requirements.

  Process for Soliciting and Collecting AI Use Cases

  CSOSA has developed new AI guidelines and updated other key Agency IT protocols to:
  - Ensure a clear understanding of what constitutes AI and its use cases;
  - Periodic survey of the organization's AI use cases and routine review of use cases for their alignment with requirements;
  - Assign responsibility for submitting and publishing use cases;
  - Identify use cases that require special attention (e.g., those that impact rights and benefits);
  - Ensure previously excluded use cases are revisited periodically, as appropriate, for

later inclusion; and
- Formalize a process of issuing, denying, revoking, and tracking use cases and certifying waivers.

Due to CSOSA's size and current posture regarding AI, CSOSA is leveraging robust, well-established technology review processes within OIT under the leadership of the Chief Information Officer (CIO). These processes review the introduction of any new technology at CSOSA and periodically review all existing IT investments. When these activities detect any existing or planned introduction of AI, OIT engages the AI governance body for appropriate follow-up.

Ensuring Comprehensive and Complete Inventory

The Agency ensures the completeness of the AI use case inventory by:
- Providing basic education on compliance requirements for AI, which are incorporated into New Employee Orientation (NEO) for onboarding and annual Security Awareness Training;
- Engaging in ongoing discussions and dialogues with key stakeholders, including the Chief Data Officer, CIO, Chief Technology Officer, component office Associate Directors, and program managers, to identify AI use cases;
- Collaborating with various component offices to ensure that all potential AI applications are captured and evaluated, and
- Documenting and tracking all AI use cases to ensure they are accurately represented in the inventory.

Criteria for Excluding Use Cases from Inventory

While CSOSA aims to maintain a transparent inventory of AI use cases, specific use cases may be excluded if they:
- Could negatively impact or create risks to the Agency's mission, employees, customers, or the public, if disclosed;
- Are subject to confidentiality agreements with other agencies, customers, employees, or stakeholders; or
- Involve sensitive or classified information that cannot be publicly disclosed.

Because of CSOSA's mission, CSOSA does not anticipate that M-25-21's Reporting on AI Use Cases Not Subject to Inventory (M-25-21 3(a)(v)) would apply; therefore, it has not identified any use cases for exclusion.

Process for Periodic Review and Validation

CSOSA is committed to periodically revisiting and validating AI use cases in its inventory to ensure accuracy and relevance. This process includes:
- Periodic reviews of the inventory, no less than annually, to identify any changes or updates needed;
- Reassessment of cases using the predetermined criteria to determine whether previously excluded instances should be included or if any new cases meet the exclusion criteria; and
- Review and validation of the cases by the CAIO and the AI governance body to

ensure accountability and transparency.

Use Cases and Transparency

CSOSA will publish AI use case inventories, as per the reporting guidance, on its website. The inventory will be updated at least annually to reflect new AI use cases and any changes to existing ones. CSOSA's public inventory will include:

- Clear and concise explanations of each AI use case, including its purpose, scope, and expected outcomes; and
- The designated compliance information as outlined in M-25-21 and subsequent standards.
-

3. Fostering Public Trust in Federal Use of AI

Determinations of Presumed High-Impact AI

- Explain your agency's process to determine which AI use cases are high-impact.

  To ensure the responsible deployment of AI, CSOSA has established a process for determining which AI use cases are considered high-impact. This determination process includes:
  - Review of current and planned AI use cases to assess whether it falls within the definitions of high-impact AI as defined in Section 6 of OMB Memorandum M-25-21;
  - Establishment of assessment criteria that include the potential for physical harm, the impact on civil rights, and the degree of automation in decision-making processes; and
  - Potential development of additional criteria tailored to the Agency-specific operations to guide high-impact AI decisions.

  As described above, the Agency AI governance body is tasked with ensuring the proper development and implementation of use case identification and review, including rights and safety-impacting scenarios. The AI policy and related guidance documents provide a comprehensive review by the Agency stakeholders.

- If your agency has developed its own distinct criteria to guide a decision to waive one or more of the minimum risk management practices for a particular use case, describe the criteria.

  CSOSA has no AI use cases requiring a waiver. As part of our standard policy review process, our AI policy and associated risk management practices will be updated as we mature.

- Describe your agency's process for issuing, denying, revoking, certifying, and tracking waivers for one or more of the minimum risk management practices.

  CSOSA is currently in the process of developing an AI policy. Upon approval of the policy, the Agency will establish an operational instruction that includes distinct processes for use case identification and inventorying to formalize the issuance, denial, revocation, and tracking of high-impact AI, as well as certifying waivers as appropriate.

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

- Identify how your agency plans to document and validate the implementation of the minimum risk management practices.

  The Agency may issue waivers for one or more of the minimum risk management practices under limited circumstances. CSOSA, as part of its AI governance protocol, has outlined a straightforward process for issuing waivers:

  - Using the criteria established by the CAIO, the decision to waive risk management practices is granted only when necessary and justified.
  - The CAIO is responsible for issuing, denying, revoking, and tracking, using a standardized process.
  - All CAIO decisions are documented and preserved per the Agency's record management practices.

- Elaborate on the controls your agency has put in place to prevent non-compliant high-impact AI from being deployed to the public.

  The agency will issue guidance to agency staff regarding the contents of M-25-21, emphasizing the importance of its clauses that outline obligations to protect the agency from the deployment of non-compliant, safety-impacting, or rights-impacting AI to the public.

- Describe your agency's intended process to terminate, and effectuate that termination of, any non-compliant AI.

  If needed, CSOSA will terminate any AI that fails to meet compliance standards, including:

  - Incident Response Plans: Develop and maintain incident response plans tailored explicitly for AI systems, outlining the roles and responsibilities, communication protocols, and remediation actions.
  - Redress Mechanisms: Establish mechanisms for redress to address any harm caused by AI systems, ensuring that affected individuals or entities can report issues and seek resolution.
  - Continuous Improvement: Regularly review and update incident response and redress protocols based on lessons learned from past incidents and emerging best practices.

  In addition to CSOSA's existing information technology, security, and governance procedures, these processes help ensure the safe and responsible use of AI internally at CSOSA. CSOSA currently does not have any AI use cases deployed to the public.