Court Services and Offender Supervision Agency
For the District of Columbia
Office of Information Technology

POLICY STATEMENT

Artificial Intelligence (AI)
Number: 2040
Effective Date: 12/20/2025
Review Due Date: 12/20/2027

MARCUS HODGES
Digitally signed by MARCUS HODGES
Date: 2025.12.14 19:23:41 -05'00'

Marcus Hodges
Interim Director

Table of Contents

Overview

Background

Executive Order (EO) 14179, Removing Barriers to American Leadership in Artificial Intelligence, issued on January 23, 2025, establishes the framework for responsible generative artificial intelligence (AI) implementation across federal agencies. The Court Services and Offender Supervision Agency (CSOSA or Agency) strategically integrates these cutting-edge AI technologies to boost productivity, streamline operations, and elevate service delivery while safeguarding the privacy rights of employees, supervisors, and the public.

This policy statement (PS) establishes comprehensive guidelines that empower the Agency to leverage AI's potential while ensuring strict compliance with the EO implementation requirements. Through these efforts, CSOSA strengthens leadership and contributes to sustaining and enhancing America's competitive edge in the global AI landscape.

Coverage

This PS covers all employees and interns, and contractors with access to CSOSA data and information systems.

Authorities

- The Privacy Act of 1974.
- Federal Information Security Management Act (FISMA) of 2014
- Office of Management and Budget (OMB) M-21-31 Zero Trust Architecture
- National Institute of Standards and Technology (NIST) AI Risk Management Framework
- Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) AI Guidelines
- OMB M-25-21 Accelerating Federal Use of AI through Innovation, Governance, and Public Trust

Supersedes

This policy supersedes Guidance Memorandum: Use of Generative Artificial Intelligence (AI)Tools *dated March 18, 2024.*

Continued on next page

Overview, Continued

Disclaimer

The contents of this guidance do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to clarify existing requirements under the law or agency policies to the public.

References

- PS 2036 Information Technology Security
- PS1113 Privacy
- PS 2100 Controlled Unclassified Information (CUI)
- M-25-21 Accelerating Federal Use of AI through Innovation, Governance, and Public Trust
- EO14179 Removing Barriers to American Leadership in Artificial Intelligence
- M-25-21 Accelerating Federal Use of AI through Innovation, Governance, and Public Trust
- CSOSA AI Compliance Plan

Administrator

The Office of Information Technology (OIT) is responsible for the contents and administration of this policy.

Policy

Principles

The Agency must:

- Provide AI training during onboarding to ensure all personnel develop proficiency in the safe, ethical, and effective utilization of AI technologies.
- Adhere to comprehensive parameters that guide AI implementation in alignment with Agency policies, federal mandates, and cybersecurity best practices to ensure responsible innovation.
- Commit to leveraging AI technologies exclusively for activities that directly advance the Agency's core functions and official responsibilities (Mission-Aligned Application).
- Recognize the spectrum of engagement options, from anonymous interactions that minimize data collection to authenticated sessions that enhance functionality while carefully balancing convenience with privacy considerations (Privacy-Preserving Access).
- Acknowledge that authenticated access enhances capabilities while requiring heightened vigilance regarding personal data protection and compliance with information security standards (Responsible Authentication).
- Commit to implementing secure, FedRAMP-certified AI solutions seamlessly integrated with existing infrastructure to support mission-critical functions while maintaining compliance with federal security standards and maximizing return on technological investment (Strategic Technology Integration).

Prohibitions When Using AI

The Agency *prohibits* employees from entering sensitive, confidential, controlled Unclassified Information (CUI) or Personal Identifiable Information (PII) into AI tools, regardless of access method, unless OIT authorizes specific business purposes. CSOSA requires verification of all AI-generated content before employees include it in official documents.

Continued on next page

Policy, Continued

Safe and Ethical Use of AI Tools

All employees and contractors and interns, who have access to and use the Agency applications and system, are ***required*** to engage in safe and ethical use of AI tools, which include, but is not limited to, the following:

- Avoid generating content that is biased, discriminatory, or offensive;
- Never enter sensitive, confidential, or CUI into AI tools;
- Never process PII or mission-sensitive data using AI tools;
- Use AI tools in anonymous (not logged-in) mode whenever possible for work-related tasks;
- AI tools that require user accounts must be accessed exclusively through agency-approved platforms and processes. Under no circumstances should users register or access work-related AI tools using a personal email address;
- Never use AI-generated outputs as authoritative guidance for policy, law, or regulatory matters;
- Use AI chatbots exclusively for authorized work-related tasks in accordance with approved guidelines, such as:
  - Drafting routine correspondence and emails;
  - Summarizing publicly available research and reports;
  - Creating training materials and presentations; and
  - Brainstorming professional development ideas;
- Verify all AI-generated content before inclusion in official documents; and
- Use only the Generative AI applications approved by the Agency for business purposes, as published in the Agency's AI Use Case Inventory.

Continued on next page

Policy, Continued

AI Governance Framework Components

The following outlines the structural elements that define how AI tools are managed and monitored within the organization:

- Access Control Framework:
  - *Anonymous vs. Registered Use Policy*: Establishes different tiers of AI tool access based on user authentication and data sensitivity requirements, with specific protocols for each access level.
  - *Risk-Based Access Permissions*: Defines which AI capabilities are available under each access tier and the approval processes required for elevated permissions.
- Compliance and Enforcement Measures:
  - *Monitoring and Audit Procedures*: Outlines systematic review processes for AI tool usage, including automated logging requirements and periodic compliance assessments.
  - *Violation Response Protocol*: Establishes graduated consequences for policy non-compliance and standardized remediation procedures to restore compliant usage.

Accountability

Agency employees' failure to comply with this PS may result in disciplinary action, up to and including removal.

Definitions

Artificial Intelligence (AI)	A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to: • Perceive real and virtual environments; • Abstract such perceptions into models through analysis in an automated manner; and • Use model inference to formulate options for information or action.
AI Use Case Inventory	A structured repository that catalogs the specific applications of artificial intelligence within an organization, detailing how AI is used to address particular problems or enhance operations.
Controlled Unclassified Information (CUI)	Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle, using safeguarding or dissemination controls.
High-Impact AI	Refers to an AI system that has the potential to significantly impact society, the economy, or individuals at scale, where its output serves as a principal basis for decisions or actions with legal, material, binding, or otherwise substantial effects. The impacts may involve an individual's rights and access – including: • Civil rights, civil liberties, privacy; • Access to education, housing, insurance, credit, employment, government programs; • Critical services impacting human health and safety, including impacts on critical infrastructure or public safety; or • Strategic assets, including high-value property, sensitive information, or classified government materials.

Continued on next page

Definitions, Continued

Mission-Sensitive Data	Information that is critical to CSOSA operations and **must not** be entered into AI tools. Examples include, but are not limited to: • Personally identifiable Information (PII); • Offender specific/ identifiable information; and • Sensitive law enforcement information.
Personally Identifiable Information (PII)	• Any information about an individual maintained by an agency, including any information that: • Can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and • Is linked or linkable to an individual, such as medical, educational, financial, email, telephone, and employment information.
Sensitive PII	A subset of PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data is compromised. • *Examples of Sensitive PII* include, but are not limited to: – Alien Registration numbers; – Biometric identifiers; – Driver's license or state identification numbers; – Financial account numbers; – Passport numbers; and – Social Security numbers (SSN). • *Other data*, when combined, may also constitute Sensitive PII, such as: • Account passwords; • Citizenship or immigration status; • Date of birth; • Ethnic or religious affiliation; • Medical information; • Mother's maiden name; • Personal email address, address, and phone; and Salary.

Roles and Responsibilities

Employees, Interns, and Contractors	• Complete comprehensive AI Training workshops focused on secure, ethical, and efficient AI utilization practices, with mandatory participation at onboarding and through on an as-needed basis, as determined by IT Security, CAIO, OHR-TCDC, and the CIO. • Ensure information integrity across all operations through consistent review processes. • Exercise critical oversight of AI-generated content through human verification protocols. • Maintain full compliance with Office of Management and Budget (OMB), Department of Homeland Security (DHS), and CSOSA PS and operational instructions (OIs) when using or interacting with AI technology. • Safeguard confidentiality and privacy by not inputting sensitive data or PII into AI tools. Such actions would compromise sensitive information by exposing it to the public domain. • Exercise continuous critical oversight of all AI-generated content, maintaining human verification protocols to address potential inaccuracies and ensure information integrity across all operations.
Supervisors and Managers	• Complete required AI training. • Identify and provide program-level AI use cases to the Chief AI Officer (CAIO), upon request. • Implement risk management practices while supporting employees. • Train and report AI-related concerns to appropriate personnel. • Provide oversight on AI use by employees.
Office of Human Resources, Training and Development Center (OHR-TCDC)	In collaboration with OIT, provides training in the safe, ethical, and effective utilization of AI technologies to all new hires during onboarding and through ongoing training on AI.

Continued on next page

Roles and Responsibilities, Continued

Office of Information Technology (OIT)	• Collaborates with TCDC to develop and deliver training on safe and effective AI utilization. • Implements technical safeguards for AI tool usage where possible. • Monitors compliance with AI usage policies. • Guides proper AI tool usage within security and compliance parameters. • Provides technical support for approved AI tool usage. • Serves as the primary contact for AI-related questions and issues. • Ensures AI systems and applications meet Federal security and privacy requirements (e.g., FISMA, FedRAMP, and any other mandates-).
Office of General Counsel (OGC)	Conducts legal analysis of the Agency's AI systems and their use by: • Balancing requirements with objectives while documenting efforts. • Ensuring cross-jurisdictional regulatory compliance. • Implementing remedies and accessible appeals processes. • Incorporating privacy, civil rights, and intellectual property protections. • Monitoring legal standards and providing operational guidance.
Agency AI Governance Board	• Membership is listed in the Agency's AI Compliance Plan • Oversees AI system development, ensuring ethical use, and risk mitigation. • Continuously monitors AI systems to ensure alignment with the Agency's objectives and regulatory requirements.
Chief IT Security Officer (CISO)	• Establishes governance structures and ensures resource allocation while championing an AI-ready workforce. • Implements safeguards across all agency IT resources to ensure safe use of AI. • Oversees protection of all digital assets, information systems, and data.

Continued on next page

Roles and Responsibilities, Continued

Chief AI Officer (CAIO)	• Leads organization's artificial intelligence strategy, governance, and implementation across all business units. • Maintains the Agency's high-impact AI use case inventory. • Oversees the ethical development of AI systems while maximizing business value and managing associated risks, in coordination with the AI Governance Board.
Chief Information Officer (CIO)	• Serves as the subject matter expert in digital technologies, improving their operations' cost-effectiveness and accelerating growth and efficiency driven by new technological opportunities. • Oversees the Agency's information technology strategy, implementation, and operations. • Ensures compliance with federal IT regulations and security standards. • Makes decisions on the purchase of IT equipment from suppliers for the creation of new IT systems to support safe and effective utilization of AI technologies. • Responsible for the implementation of information technology and computer systems by ensuring that: - The hardware and software are adequate for the Agency's needs; and - The online infrastructure is sufficient to support the Agency's operations. • Works closely with the CISO to implement security policies and procedures, to monitor potential security breaches, and conduct security audits. • Supports the Agency's growth and its progress as a data-driven enterprise.
Agency Director	• Authorizes the use of AI to meet the Agency's mission and operational needs. • Defines the types of AI available and establishes the parameters for the proper uses of this technology. • Directs the Agency AI policy and program in compliance with EOs and associated OMB memoranda, as well as all applicable laws, regulations, rules, and mandates.