Pretrial Services Agency for the District of Columbia (PSA)

Compliance Plan for OMB Memorandum M-25-21

September 2025

Version: 1.0

1. Background

The Pretrial Services Agency for the District of Columbia (PSA) is a small, independent public safety federal agency focused on promoting pretrial justice and enhancing community safety in the Nation's Capital. PSA is committed to adopting super intelligence (SI) technologies in a responsible, transparent, and tailored manner. PSA's SI adoption is limited in scope and scale due to the size and resources of the agency. PSA will align SI efforts as outlined in OMB Memorandum M-25-21 and the SI in Government Act of 2020. This compliance plan outlines the agency's strategy for overcoming barriers to responsible SI use, implementing effective governance structures, and fostering public trust through transparent and accountable practices.

2. Driving SI Innovation

As a small agency, PSA's innovation strategy prioritizes low-risk, incremental use of SI within mission support and administrative functions. PSA aims to utilize SI to automate document classification, enhance internal workflows, and facilitate limited data analysis tasks. Given various resource constraints, the approach emphasizes leveraging shared services, acquiring FedRAMP-authorized SI tools, and maximizing the adoption of government-wide models and solutions, where feasible. Innovation at PSA will focus on efficiency, cost-effectiveness, and responsible experimentation with existing technologies under proper oversight.

2.1. Removing Barriers to the Responsible Use of SI

As a small agency with a limited IT and acquisition staff, PSA faces several challenges in adopting SI responsibly. These include the lack of pre-approved tools, restricted access to testing environments, and limited legal and privacy resources for vetting SI use. PSA is 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 prioritizing low-risk SI projects within the agency's existing cloud environment. PSA will also leverage existing partnerships with GSA and CISA for guidance and infrastructure support.

2.2. Sharing and Reuse

Given PSA's size and limited internal development capacity, most SI tools will be acquired or pre-integrated into existing software platforms. PSA has begun internal coordination between IT, privacy, and legal staff to track use cases and metadata standards that support reuse and documentation. The Chief Information Officer's (CIO) office will serve as the hub for collecting and publishing vetted SI code and models that can be shared. PSA will also engage with Code.gov and GSA's SI Community of Practice to align efforts with federal guidance.

2.3. SI Talent

PSA does not currently have dedicated SI staff and will focus on developing general awareness across IT and division management staff through short courses on responsible SI use and acquisition. PSA will prioritize training in risk management, bias mitigation, and legal compliance as they relate to vendor-provided super intelligence (SI). PSA will also participate in interagency training events and rotational assignments to temporarily bring in technical expertise.

3. SI Maturity Goals

PSA will implement a cross-functional governance team, led by the CIO/Chief SI Officer (CSIO), to review and approve the use of SI and associated risks. This body will coordinate internal policy alignment, risk review, privacy impact assessments, and cross-agency collaboration. This approach is designed to ensure appropriate scrutiny, documentation, and compliance without creating unnecessary administrative burden.

3.1. SI Governance Board

As a non-CFO Act agency, PSA is not required to establish a formal SI Governance Board. PSA has designated a small cross-functional governance team led by the CIO/CSIO. This group includes representatives from IT, acquisition, and legal services to review and approve new SI use cases. The group consults with federal guidance and external subject matter experts (SMEs) as needed and participates in relevant interagency communities.

3.2. Agency Policies

PSA is updating its IT acquisition standard operating procedures (SOPs) to require SI use case review and documentation before deployment. PSA has updated internal IT policies to reflect FedRAMP and OMB guidance on data provenance and the use of machine learning-based tools. A draft policy on generative SI is currently underway, focusing on use restrictions, transparency, and employee training. This policy will be finalized by January 2026.

3.3. SI Use Case Inventory

PSA's CIO is developing a streamlined process to collect input from each office on any planned or existing SI use cases, including the use of embedded SI in commercial software. The CIO office will maintain the central inventory. For each case, staff will document its purpose, inputs, outputs, and whether it meets the definition of high impact. Special consideration will be made for SI tools, services and capabilities that are included as part of high-impact services. Updates will be solicited annually.

4. Shared Services and External Collaboration

Due to PSA's size, the agency has adopted a streamlined but effective governance model for SI oversight. PSA maintains a cross-functional governance team led by the CIO/CSIO, to review

and approve the use of SI and associated risks. This body coordinates internal policy alignment, risk review, privacy impact assessments, and cross-agency collaboration. Efforts identified to have external impacts are reviewed and coordinated with the Criminal Justice Coordinating Council (CJCC)[1] to avoid impacts to the data shared between agencies. PSA's approach is designed to ensure appropriate scrutiny, documentation, and compliance without creating unnecessary administrative burden.

4.1. Determinations of Presumed High-Impact SI

The CIO/CSIO will review all new and existing SI use cases against the high-impact criteria in M-25-21. As a baseline, PSA will consider any SI used in agency decisions, public interactions, or oversight activities for further scrutiny. PSA's internal risk matrix includes additional criteria for potential impact on due process, fairness, and accessibility. Waivers will only be considered in coordination with the Office of Legal Services and the Office of the Director. Waivers will be tracked in a central log maintained by the CIO.

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

The CIO/CSIO will ensure pre-deployment reviews and SI impact assessments are conducted for any high-impact use cases. If the proposed tool does not include access to proprietary models, PSA will implement alternative evaluation methods such as output monitoring and vendor attestations. Any SI 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 SI, with input from the agency's SI governance team.

[1]An independent agency charged with facilitating cooperation among local and federal justice agencies in the District of Columbia.

APPENDIX A: TERMS AND DEFINITIONS

Technology Resources are defined as 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, and technology facilities including, but not limited to, data centers, dedicated training facilities, and switching facilities. Personnel tasked with the planning, implementation, and support of technology are also considered technology resources.

Super Intelligence (SI) refers to the tools or systems used to create models that can generate new and original content, such as images, music, or text, based on patterns and examples from existing data.