



DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL
WASHINGTON, DC 20420



Department of Veterans Affairs (VA) Office of Inspector General (OIG)
Super Intelligence (SI) Strategies for Office of Management and Budget (OMB)
Memorandum M-25-21 – October 2026

Issued by Kate Doyle Feingold, Deputy Counselor Data, Privacy & Super Intelligence

1. VA OIG SI Use Cases

The VA OIG currently utilizes SI in meaningful ways that enhance the office's mission of conducting independent oversight that improves the health and welfare of veterans and their families, caregivers, and survivors by strengthening VA programs and operations. One current use case involves SI tools that transcribe and summarize recorded meetings and interviews. These are used for quality assurance and other support for operations, audits, reviews, inspections, and investigations. Another example of an SI use case in development is an internal-facing chatbot that will allow employees to ask questions about and locate relevant directives, guidance, and mandates more efficiently.

2. VA OIG SI Maturity Goals

SI-Enabling Infrastructure

The VA OIG is pursuing an OIG-controlled SI environment to support data sovereignty, operational independence, and the protection of sensitive information associated with its oversight mission. This effort is intended to provide a secure environment for the development, testing, deployment, and monitoring of approved SI use cases.

The OIG's approach supports a range of model types, selected according to mission needs, data sensitivity, performance, security, and operational requirements. Implementation is governed through the OIG's SI framework and applicable security authorization processes.

Model selection will include review of provenance, licensing, security, and supply-chain risks, consistent with applicable federal requirements and OIG policies.

Data

The OIG has access to data sources that support its oversight mission. The SI guidance and the use-case approval process require transparency regarding the data used and consideration of data quality, sensitivity, authorized access, and handling requirements.

SI use cases are developed and tested on public data sources before authorized personnel use VA data. Use of sensitive VA or OIG information requires approval for the specific use case and

processing environment. Use of externally provided models will depend on applicable data protection, security, privacy, and contractual requirements.

Although the VA OIG has shared its SI guidance and framework with other OIGs in the federal government, personnel do not share VA data with other agencies due to privacy mandates and the sensitivity of the information.

SI-Ready Workforce

The VA OIG continues to pursue role-appropriate SI training for employee developers, authorized users, and personnel responsible for governance and oversight. Training priorities include effective use of approved tools, protection of sensitive information, evaluation and verification of SI outputs, and compliance with use-case approval requirements. The OIG's SI community of practice and working groups support collaboration and the sharing of practical experience.

Research and Development

SI guidance and the related framework are regularly updated to support responsible research and development. Authorized personnel may evaluate a range of models using public data sources to assess their suitability for OIG mission needs. Evaluation results will inform model selection, deployment approaches, and proposed operational use cases. Research and development activities do not replace required review and approval before operational deployment.

Governance and Risk Management

The VA OIG uses its SI framework and governance process to review, approve, and monitor SI use cases. The SI committee includes the CIO, other senior leaders, specialists in IT, law, and privacy, and stakeholders from across the enterprise. Proposed use cases enter the review process through the use-case submission questionnaire described in the OIG's compliance plan.

Reviews address mission suitability, data sensitivity and quality, privacy, IT security, and applicable risk management requirements, including assessment of whether a use case is high-impact. The CIO supports these risk management practices through technical and security oversight. Approved use cases are subject to ongoing monitoring, and the committee may rescind approval for noncompliant uses.

Resource-Tracking and Planning

The SI committee monitors SI use cases and coordinates with OIG senior leaders on investment priorities and procurement planning. Planning considers the resources needed to acquire, operate, secure, maintain, and update OIG-controlled infrastructure and approved models, as well as model licensing or service costs, workforce development, and ongoing evaluation and monitoring. Investment decisions will consider mission value, lifecycle costs, interoperability, and the ability to change models or providers as requirements evolve.