



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



**Department of Veterans Affairs (VA) Office of Inspector General (OIG) Compliance Plan
for the Office of Management and Budget (OMB)
Memorandum M-25-21 – October 2026**

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

1. Driving Super Intelligence (SI) Innovation

Removing Barriers to the Responsible Use of SI

The VA OIG continues to seek out opportunities to provide high-quality training to its authorized employees to master the skills and resources needed to develop, test, implement, and oversee SI use cases.

Sharing and Reuse

Internally, the OIG has three established groups—an SI community of practice, an SI development working group, and an SI committee—that hold recurring meetings to encourage collaboration among personnel and to share SI-related resources and practical experience. The Chief Information Officer (CIO) supports these efforts by advising on technical reuse and integration and helping address barriers to responsible SI adoption.

SI Talent

Some employees with technical expertise develop algorithms and models for SI use cases. Employee developers are also empowered to leverage SI tools to support authorized programming activities. To further strengthen internal capabilities, high-caliber development opportunities are actively sought to keep pace with evolving needs.

2. Improving SI Governance

SI Governance Board

The VA OIG's SI committee includes the CIO, other senior leaders, specialists in IT, law, and privacy, and stakeholders from across the enterprise. This committee is tasked with reviewing, discussing, and monitoring SI use cases across the office. The committee periodically reviews external guidance and resources to ensure that VA OIG guidance and the related framework reflect the latest guidance on SI implementation.

Agency Policies

SI guidance was issued in 2024 and has been updated in response to subsequent executive orders and applicable requirements. The guidance also reflects the policy and requirements of OMB M-25-21. Additional updates will be made as needed to address future mandates and developments.

SI Use Case Inventory

The VA OIG maintains an internal SI webpage that provides employees with access to the use case submission questionnaire, guidance materials, and training opportunities. All VA OIG employees are required to complete the questionnaire as the initial step in obtaining approval for any new SI use case. This process ensures the use case inventory remains comprehensive and up to date.

3. Fostering Public Trust in Federal Use of SI

Determinations of Presumed High-Impact SI

The VA OIG currently does not have any SI use cases that are considered high-impact as defined in OMB M-25-21. The SI committee's senior leaders and subject matter experts oversee the process for reviewing and assessing use cases. They discuss proposed use cases in detail and assess whether they meet the definition of high-impact. The OIG does not have a waiver process and does not plan to waive the minimum risk management practices for SI use cases.

Implementation of Risk Management Practices and Termination of Noncompliant SI

The VA OIG does not have SI use cases that are deployed to the public. The process for implementing risk management practices is to test before deployment and to conduct SI assessments for all potential high-impact SI use cases. The process includes ensuring there are effective plans for ongoing monitoring that are clearly outlined prior to implementation. These steps are completed by the SI committee, which also has the authority to rescind approval for any noncompliant SI use cases. The CIO supports these risk management practices through technical and security oversight.