

Complementing Oracle OCI AI

A Zero-Trust Unstructured Data Vault for Mission-Critical Federal Deployments

Introducing AsterionDB — the Oracle-native secure data layer that unlocks AI on classified, air-gapped, and high-assurance environments

Oracle-native

Files stored inside Oracle DB. Not an overlay. Not middleware.

Zero filesystem

No network shares. Ransomware has nothing to find or encrypt.

IL2 – IL6 / SAP

Sell across every DoD classification level today.

01 Executive Summary

The gap in Oracle's federal AI platform — and how AsterionDB fills it

Oracle's AI Data Platform for Federal Government, announced March 31, 2026, is a landmark product. It unifies Oracle Cloud Infrastructure (OCI), Oracle Autonomous AI Database, and OCI Enterprise AI into a single FedRAMP High-authorized stack. Civilian and defense agencies can now build AI agents, run natural language queries against their data, and derive mission-critical intelligence — all without leaving Oracle's secure cloud perimeter.

Yet a critical gap remains for agencies with the most sensitive and mission-critical data. Before OCI AI can analyze a document, a medical image, an engineering drawing, or an intelligence report, that file must be stored somewhere. Today, most agencies store unstructured files on network-attached filesystems: NFS shares, SAN drives, SharePoint stores, and S3-compatible object buckets. These filesystems sit outside Oracle's security perimeter, outside its audit trail, and outside its access control model. They are the single largest attack surface in federal IT.

AsterionDB eliminates that attack surface entirely. By storing all unstructured data natively inside the Oracle Database — using Oracle's own storage engine, RBAC, TDE encryption, and audit vault — AsterionDB transforms Oracle OCI AI from a powerful analytics platform into a fully zero-trust end-to-end capability. One that operates at IL2 through IL6, in air-gapped facilities, on Oracle Roving Edge, and inside Oracle National Security Regions.

This white paper introduces AsterionDB to Oracle's federal team, demonstrates the precise architectural fit with the Oracle AI Data Platform, and identifies the highest-priority current Oracle federal customers where the combined solution is immediately deployable.

The intent is simple: one meeting to explore whether Oracle and AsterionDB should pursue a formal technology partnership, OEM arrangement, or co-sell motion in the federal market.

02 The Problem Oracle's Federal Customers Face

Oracle's federal AI platform is designed to make agency data AI-ready. But for most agencies, the most valuable data — contracts, patient records, engineering drawings, DICOM scans, technical intelligence reports, maintenance logs, policy documents — almost universally lives on network filesystems outside Oracle's security perimeter.

This creates four compounding problems that no Oracle-native solution currently solves:

- **Security:** The filesystem is the ransomware entry point. Files stored on NFS/SAN are discoverable, lockable, and exfiltrable. The Oracle DB is not.
- **Fragmented governance:** Files live outside Oracle's access controls — a separate identity model, separate audit trail, separate backup schedule that rarely synchronizes with structured data.
- **Integrity gap:** OCI AI can index and query filesystem-stored data, but cannot guarantee provenance, chain of custody, or tamper-evidence outside the Oracle audit scope.
- **Classification ceiling:** Classified environments require the storage layer itself to hold IL4, IL5, or IL6 certifications. Standard NAS/SAN and object stores cannot meet this bar. Oracle's database running in OCI Government Cloud or Oracle National Security Regions already does.

Traditional approach — what agencies have today

- Files on NFS / SAN / SharePoint / S3
- Access controls separate from Oracle DB
- Discoverable by ransomware and lateral movement
- Backup schedule decoupled from structured data
- Classification ceiling: typically IL2
- AI queries data it cannot fully audit or trust

AsterionDB + Oracle OCI AI — the combined solution

- All files stored inside Oracle DB — no separate filesystem
- Oracle RBAC + TDE + audit vault govern every file access
- Ransomware discovers no shares, no mounts, nothing to encrypt
- One Oracle export backs up structured + unstructured data together
- Classification ceiling: IL6 / TS-SCI via OCI National Security Regions
- AI queries data it created, owns, and can fully audit

03 What AsterionDB Is

AsterionDB is a Converged Computing Platform built natively on the Oracle Database. It is not a wrapper, an overlay, or a middleware layer sitting between applications and Oracle. It uses Oracle's own storage engine, security architecture, and query infrastructure to store every type of unstructured content — documents, images, video, audio, DICOM scans, CAD drawings, PDFs, and binary files — directly inside the database, eliminating the need for a separate filesystem entirely.

Architecture in one sentence

A single PL/SQL API layer sits between agency applications and the Oracle Database. All file creation, retrieval, and management occurs exclusively through that API. Assets are exposed to the file-system on demand, at the point in time that access has been verified and logged.

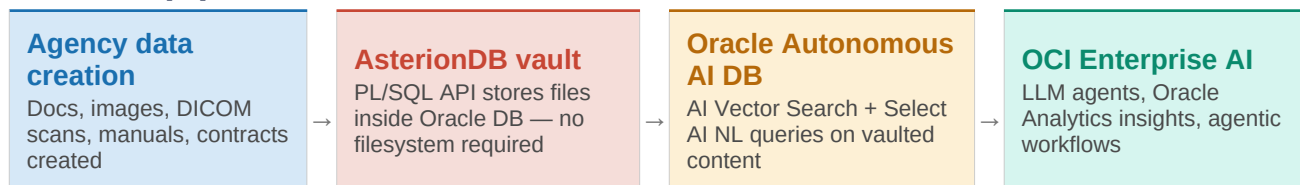
Filesystem eliminated	All files, documents, images, and media live inside Oracle. Attackers discover no network shares, no NFS mounts, no S3 buckets. Ransomware has no traditional filesystem to traverse or encrypt.
Oracle-native security	Oracle RBAC, Transparent Data Encryption (TDE), Virtual Private Database (VPD) policies, and Oracle Audit Vault govern every single file access. One security model covers structured records and unstructured files simultaneously.
DoD CSRA & ZT aligned	Architecture validated against DoD CSRA Principles 1.2, 2.1, and 2.2. Navy CISO Zero Trust Roadmap alignment confirmed. Deployable on Oracle Roving Edge Infrastructure, Oracle Cloud@Customer, and Oracle National Security Regions.
API-first, MCP-ready	AsterionDB's open-source DbTwig REST framework acts as an API in front of the database. MCP-compliant AI tools easily map to entry points within the API.
Unified export	One Oracle database export contains all structured and unstructured data items. A VA patient record and its DICOM scan back up together, restore together and are always synchronized. No detached libraries for imagery or separate restore procedures.

04 The Combined Solution: AsterionDB + Oracle OCI AI

Oracle's AI Data Platform for Federal Government (March 2026) delivers AI Vector Search, Select AI natural language querying, OCI Enterprise AI LLM services, Oracle Analytics, and real-time streaming — all within a FedRAMP High-authorized cloud environment. AsterionDB provides the secure, zero-trust data ingestion and storage layer that feeds this platform with content that has never been exposed to an exploitable filesystem.

Together, these two Oracle-native technologies form the only end-to-end zero-trust AI pipeline available for classified federal environments today.

How the pipeline works



At every stage, data never leaves the Oracle security perimeter. Files enter the vault through AsterionDB's patented file-system gateway; Oracle's AI services analyze them in-place; insights reach mission users through OCI Enterprise AI or Oracle Analytics dashboards. The underlying data is immutable and auditable. It is always encrypted, and never exposed while at rest to a filesystem that could be discovered, traversed, or ransomed.

OCI AI capabilities that AsterionDB directly enables

The following table shows how each major Oracle OCI AI capability is enhanced or unlocked when AsterionDB provides the zero-trust storage layer. Scores reflect applicability to classified and high-assurance federal deployments.

OCI AI Capability	Federal readiness with AsterionDB	Why it matters
AI Vector Search	98%	Semantic search across all Oracle-vaulted docs, DICOM, manuals, and reports — classified data never leaves the DB
Select AI (NL to SQL)	97%	Natural language queries directly against Oracle-stored structured + unstructured data in IL5/IL6 environments
OCI Enterprise AI (LLMs)	96%	Agents interact with vaulted content through AsterionDB's API — no filesystem path, no exfiltration risk
Oracle Analytics	94%	BI dashboards and AI-generated narratives on data whose provenance is guaranteed by Oracle's audit vault
Autonomous AI Database	98%	Self-managing, self-securing DB holds all of the data
Real-time streaming / events	88%	AsterionDB logs all data access operations and encountered errors to a central location for easy auditing and monitoring
Oracle National		Air-gapped, TS/SCI-capable OCI regions +

Security Regions	100%	AsterionDB vault = complete IL6/SAP zero-trust AI stack; no other vendor provides this
Cloud@Customer (CC@C)	99%	AsterionDB deployed on CC@C within agency facilities — no data leaves agency premises, ever

The value AsterionDB adds to each OCI AI component

OCI Component	Without AsterionDB	With AsterionDB
Autonomous AI Database	Queries structured data + external filesystem-stored files. Audit trail incomplete for unstructured content.	Queries structured + unstructured in one unified store. Full Oracle audit trail covers every file. IL6 capable.
OCI Enterprise AI / LLMs	Agents retrieve context from filesystem paths. Files traversable by attackers on same network.	Agents retrieve context through AsterionDB API only. No filesystem path exists. Zero lateral movement risk.
AI Vector Search	Indexes docs on S3 / SharePoint. Embeddings generated from data outside Oracle's trust boundary.	Indexes docs vaulted inside Oracle. Embeddings generated inside the trusted Oracle perimeter. Chain of custody intact.
Oracle Analytics	Dashboards reference external file paths for images and documents. Link rot and access drift common.	Dashboards reference a single data source. Data is always accessible, always in sync with structured data, with no drift.
CC@Customer / Roving Edge	File servers must also be deployed on-prem or at edge. Separate security hardening and patching required.	AsterionDB runs on the same Oracle CC@C or Roving Edge appliance. No separate file server.

05 Priority Oracle Federal Customer Targets

The following agencies are existing Oracle customers with active AI procurement programs and documented unstructured data challenges that AsterionDB directly addresses. Each entry identifies the specific Oracle relationship, the unstructured data problem, and the program offices most likely to act.

TIER 1 — PURSUE NOW

Department of Veterans Affairs (VA)

The VA operates the largest integrated U.S. healthcare system, serving 9M+ veterans annually. It holds over 10 million veteran health records including DICOM imaging, clinical notes, lab results, and administrative documents — all currently on file stores separate from Oracle's structured EHR data. Oracle is a major incumbent across VA health IT infrastructure. A September 2025 GAO report identified data security gaps in VA AI practices as a primary concern. AsterionDB eliminates that gap: DICOM scans and structured EHR records live in the same Oracle DB, back up together, share one access control model, and are immediately available to OCI AI Vector Search for clinical decision support.

Oracle incumbent **HIPAA + DICOM native fit** **FedRAMP Mod. sufficient today** **GSA / SEWP V path**

Program offices: VA National AI Institute (NAII) • VHA Chief AI Officer • Office of Information & Technology (OI&T)

TIER 1 — PURSUE NOW

Dept. of Health & Human Services — NIH / FDA / CDC

NIH, FDA, and CDC collectively manage hundreds of millions of research documents, drug approval dossiers, clinical trial records, genomic data sets, and outbreak response imagery. HIPAA mandates strict access control and audit — requirements Oracle's database satisfies natively and that AsterionDB extends to

unstructured content. Active AI procurement is underway across all three agencies under OMB M-25-21. AsterionDB provides the Oracle-native storage layer that ensures OCI AI operates on data whose provenance is guaranteed and whose filesystem attack surface is eliminated.

[Oracle / OCI incumbent](#) [HIPAA critical](#) [Active AI procurement \(OMB M-25-21\)](#) [Multiple entry points](#)

Program offices: NIH Office of Data Science Strategy • FDA Office of Digital Transformation • CDC PHDI

TIER 2 — 6–12 MONTH HORIZON

Dept. of War — Navy / NAVSEA / NAVAIR

NAVSEA and NAVAIR manage millions of ship and aircraft engineering drawings, technical manuals, maintenance records, and parts specifications — all unstructured, all mission-critical, and currently on filesystems vulnerable to supply-chain attack. Oracle Roving Edge is deployed at Navy edge environments today. The DoD AI Strategy (January 2026) mandates an AI-first warfighting force. AsterionDB + Oracle OCI AI enables that mandate at IL4/IL5 on deployed infrastructure — without a separate file server, without a separate backup, without filesystem exposure.

[Navy CISO relationship documented](#) [Oracle Roving Edge deployed](#) [IL4/IL5 via OCI today](#) [OTA / DIU recommended path](#)

Program offices: NAVSEA PEO IWS • NAVAIR PMA-209 • CDAO • Defense Innovation Unit

TIER 2 — 6–12 MONTH HORIZON

Dept. of Homeland Security — CISA / CBP

CISA's zero-trust mandate directly mirrors AsterionDB's architectural approach. CBP has an active AI procurement (ADAPT contract, solicited Q1 2026) covering AI development and advanced program transformation. DHS published 100+ active AI use cases. Palantir won DHS's analytics layer (\$1B, Feb 2026) — Palantir does not provide a secure file storage layer. AsterionDB fills the DHS secure storage gap without conflicting with existing investments, and Oracle's DHS presence provides the entry relationship.

[CISA ZT mandate alignment](#) [CBP ADAPT contract opening](#) [Oracle present across DHS](#) [Non-conflicting with Palantir](#)

Program offices: CISA JCDC • CBP OIT / ADAPT Program • FEMA CIO

TIER 3 — 12–24 MONTH HORIZON

DoD CDAO — GenAI.mil Classified Tier (IL6/IL7)

GenAI.mil reached 1.3M users within five months of launch and is actively expanding to IL6 and IL7 classified networks. Oracle is one of eight companies that signed classified AI deployment agreements with the Department of War in May 2026 for IL6/IL7 environments. AsterionDB as a zero-trust MCP data source feeding GenAI.mil agents on classified networks represents the definitive long-game play: Oracle provides the AI and compute; AsterionDB provides the zero-trust unstructured data vault; together they deliver a complete classified AI capability no other single-vendor solution can match.

[Oracle IL6/IL7 agreements signed](#) [GenAI.mil classified tier expanding](#) [OTA / prime contractor path](#)

Program offices: CDAO AI Rapid Capabilities Cell • Defense Innovation Unit • Service digital transformation offices

06 Procurement — How Agencies Buy This Today

AsterionDB is listed on Oracle Cloud Marketplace. The combined AsterionDB + Oracle OCI AI solution can be procured through existing Oracle federal contract vehicles in most cases, eliminating the need for new contract awards and dramatically shortening time-to-deployment.

Vehicle	Coverage	Status
---------	----------	--------

OCI Cloud Marketplace	AsterionDB listed directly on Oracle Cloud Marketplace. Agencies already provisioned on OCI can add with zero new contract action.	Available now — direct OCI add
Oracle National Security Regions	For IL6/SAP classified work, Oracle's NSR agreements cover infrastructure. AsterionDB runs within these regions under the same Oracle contract.	Via Oracle NSR agreement
OTA (DIU / CDAO)	Bypasses FAR requirements for AI prototypes. Fastest DoD entry for IL5+ environments. DIU and CDAO have active AI OTA programs.	Requires DIU / CDAO relationship