FIDUCIARY COMMONS VERSION 2.2

Model Procurement Specification

Functions, not generalized informational power | 11 September 2026

1. Procurement Principle

Government should procure functions, not generalized informational power. A Vendor is not a governmental fiduciary merely by contracting with government. Government's duties remain nondelegable, and Vendor obligations arise from applicable law, procurement requirements, contract, agency principles where applicable, and direct statutory duties where imposed.

2. Mandatory Capability Disclosure

- All information domains the product can read, query, compare, correlate, infer from, disclose, export, retain, resolve, or act upon.
- All administrator, support, developer, service-account, agentic, and emergency capabilities.
- All cross-tenant, cross-program, cross-purpose, identity-resolution, knowledge-graph, vector-search, AI, and enrichment functions.
- All Vendor telemetry, prompt/output retention, training, product-improvement, profiling, subprocessors, onward disclosure, and commercial-data integrations.
- All interfaces, APIs, connectors, export paths, logs, backups, recovery mechanisms, and dormant or license-activatable capabilities.
- Whether materially broader capability can be disabled technically, contractually, by configuration, by tenant boundary, or only by operator policy.

3. Legitimate Informational Authority Schedule

For every procured material capability, the solicitation and resulting contract SHALL identify the governmental function, Positive Legal Authority, Originating Informational Purpose, Authorized Object or predicate, information domains, permitted operations, Informational Justification Level, permitted consequence, duration, and the boundary beyond which Materially Renewed Authorization is required.

4. Mandatory Architecture Requirements

1. Standing Technical Informational Capability shall not materially exceed Standing Legitimate Informational Authority.

2. Generalized statutory or program authority shall not substitute for purpose and question particularity.

3. Cross-purpose capability shall be technically unavailable through ordinary access absent a renewed authorization state.

4. Authorized Answer and Least Informational Power patterns shall be supported where materially feasible.

5. Purpose sequestration shall be functional, not merely organizational or policy-based.

6. Administrative privilege shall not function as a universal informational backdoor.

7. AI, agents, tools, embeddings, vector stores, learned artifacts, and model state shall inherit the governmental legitimacy boundary.

8. Vendor or commercial possession, aggregation, correlation, inference, or commercial availability shall not enlarge governmental authority.

9. Intergovernmental interoperability shall preserve recipient-specific authority and purpose.

10. Metadata, identity resolution, authorization infrastructure, audit, and orchestration shall be assessed for functional integration.

11. Emergency access shall be invocation-specific, bounded, expiring, attributable, and reviewable.

12. Preservation and backup shall not restore expired operational authority.

13. Material changes to sources, features, models, interfaces, permissions, or Vendor services shall trigger conformance review.

14. Subcontractors and downstream services shall receive equivalent contractual restrictions.

15. Government shall retain regulator and assessor access sufficient to test actual capability, subject to lawful protection of trade secrets and security-sensitive material.

16. Government shall retain portability, transition, deletion/return, learned-artifact disposition, and termination rights.

17. Acceptance testing shall include negative-capability testing and red-team reconstruction.

18. Contracts shall identify and prohibit independent Vendor reuse unless independently authorized by law and contract.

19. Capabilities that are bundled but not legitimately required shall be removed, disabled, segregated, or made unavailable to the governmental tenant where reasonably feasible.

20. Conformance shall be continuous and configuration-specific; certification of a product family shall not substitute for assessment of the deployed configuration.

5. Evaluation Questions

- What is the most extensive individualized or relational knowledge the proposed system can construct under ordinary permissions?
- Which of those capabilities are actually necessary to the procurement's governmental function?
- What Positive Legal Authority supports each capability, and what Legitimate Informational Authority justifies its source and scope?
- Could the same function be performed with a less informationally powerful architecture?
- Does the Vendor's platform create an Authority-Capability Delta merely because broader functionality is commercially bundled?
- Would an authorized insider, acting entirely within granted permissions, be able to construct a materially comprehensive cross-purpose profile?

6. Model Contract Clauses

Clause	Model requirement
Capability Representation	Vendor represents that the capability disclosure schedule accurately describes all material informational and computational capabilities available to government through the contracted configuration and ordinary support arrangements.
No Independent Authority	Nothing in the contract, subscription, license, product functionality, or Vendor possession of information creates Governmental Informational Authority or Legitimate Informational Authority.
Configuration Covenant	Vendor shall maintain agreed technical restrictions that prevent government from exercising materially broader standing capability than the contracted legitimate function requires.
Change Notice	Vendor shall provide advance notice of material changes to data sources, model behavior, features, integrations, permissions, telemetry, retention, subprocessors, or other capability relevant to FCGIAS conformance.
Independent Reuse	Vendor shall not independently train upon, profile, sell, enrich, redisclose, or reuse governmental information or derived outputs except where independently authorized by law and expressly permitted by contract.
Regulator Access	Vendor shall provide information reasonably necessary for lawful governmental conformance assessment and oversight. Trade-secret protection shall not prevent authorized confidential regulator access.
Remediation	Where capability is found materially excessive, the parties shall apply the Least-Power Remediation sequence before relying on policy-only compensating controls.
Termination and Exit	Government shall be able to terminate a nonconforming capability and recover governmental records, audit evidence, and necessary continuity without preserving unauthorized learned or derivative capability.

7. Vendor Certification Schedule

The Vendor certification shall identify product and version, deployed configuration, governmental tenant, interfaces, data sources, AI/model components, external services, administrators/support roles, retained telemetry, learned artifacts, known exceptions, and all material changes since the prior certification.