

NiaShield

GSAR 552.239-7001 — what we handle for you.

For federal contractors and their integrators. The line items in the GSA AI clause that **NiaShield** discharges directly — so your contract doesn't have to. Highlighted rows are the four clauses your Contracting Officer opens the meeting with.

CLAUSES	WHAT IT REQUIRES	HOW NiaShield HANDLES IT	STATUS
(d)(1)(i)	Government owns all Data Inputs and Outputs.	Nothing is retained by Heaviside AI . Zero data plane, zero custody of customer keys. Ownership attaches to the customer's tenant where the data lives.	ENT · GTW ✓
(d)(3)(i)	No training, fine-tuning, or improving any AI model using Government Data.	Architecturally impossible: prompts and responses live in volatile memory only, scrubbed at session end. Nothing reaches a training pipeline. GPT models run only via Azure OpenAI — never the consumer OpenAI endpoint, which retains and trains by design.	ENT · GTW ✓
(d)(3)(ii)	No use of Government Data for advertising, marketing, or business decisions.	Heaviside AI operates no data plane. There is no data to use.	ENT · GTW ✓
(d)(4)(ii)	"Eyes-off" data handling; restrict human review; log any human access.	Heaviside AI has no read access to prompts, responses, or upstream credentials. The customer's Managed Identity controls everything.	ENT · GTW ✓
(d)(4)(v)	Logical segregation; no commingling with other customers.	Each deployment is a single-tenant install in the customer's own Azure subscription. There is no shared tier.	ENT · GTW ✓
(d)(4)(vi)	Securely delete all Government Data at contract end and certify in writing.	Every session ends with the SDIP-6 incineration protocol and emits a signed Certificate of Incineration — the document you hand the Contracting Officer. Ed25519 issuance with a customer-resident key: non-repudiable, not just tamper-evident. An auditor verifies with one command; Mode C ties the COI to a credential from the customer's own IdP.	ENT · GTW ✓
(e)(2)	Only American AI Systems. U.S.-developed software.	Routing is locked at the binary level to four U.S.-headquartered providers — Anthropic, Google, Azure OpenAI, and Groq. Non-U.S. SDKs are not in the bundle. SBOM-verifiable. GPT models are reached through Azure OpenAI inside the customer's tenant, not the consumer OpenAI endpoint.	ENT · GTW ✓
(e)(3)	Summarize intermediate processing steps (retrieval, routing) with citations.	Gateway records the API call; the customer's application owns retrieval. NiaShield renders citations and excerpts inline on every response.	ENT · GTW ✓
(e)(6)	Documentation on demand: system cards, NIST AI RMF docs, bias testing, decision logic.	Source-available remediation record, smoke test, and architecture docs ship in the release archive. NIST SP 800-53 Rev. 5 cross-walk shipped in the bundle. System cards templated per deployment.	ENT · GTW ✓
(f)	Detect, prevent, and reject PII entering the AI system.	Built-in PII detection on every prompt and uploaded file, and on every Gateway request body. The request is rejected before the model is called — not redacted after.	ENT · GTW ✓
(g)	Open formats (JSON/XML), exportable, no vendor lock-in.	Data lives in standard Azure services (Cosmos DB, Key Vault, Log Analytics). COIs are JSON. The customer keeps and exports on their own.	ENT · GTW ✓
(h)(1)	30-day concurrent access to successor models before retiring the current one.	Deploy a second Gateway instance pointed at the new model; both serve the same SDK with identical COI format.	ENT · GTW ✓
(i)(2)(i–ii)	Government may run automated benchmarks against the deployed system at any time.	Deployment is in the customer's tenant. Inspector access is direct and unmediated. No vendor side to hide from.	ENT · GTW ✓

Highlighted rows = CO-priority clauses. ENT = **NiaShield** Federal 5.3.5 · GTW = **Gateway** Agency 3.0.0.

And here's what your contract still owns.

The clause requirements that fall on the contractor or integrator, not the AI vendor. **NiaShield** supports each one with evidence and tooling — but the action is yours.

Why this page matters. Your compliance team drafts contract language and operational procedures for the items below regardless of which AI vendor you pick. Hand this page to your contracts attorney and your CISO before the kickoff meeting — it shows exactly where **NiaShield** evidence plugs into your contract response. (The legal conclusions are theirs to make; we supply the product facts and the evidence.)

CLAUSE §	WHAT YOU'RE ON THE HOOK FOR	WHAT NiaShield GIVES YOU TO MAKE IT EASIER
(d)(2)	License grant to the Government — irrevocable, royalty-free, for the contract term — written into the contract.	Standard contract language; NiaShield 's zero-retention posture means no carve-outs needed for vendor data rights.
(d)(5)	Dedicate Custom Developments (prompts, RAG corpora, fine-tunes) to the Government's exclusive use; treat as confidential.	Per-deployment isolation means Custom Developments are physically segregated from other customers. Contract language handles the dedication.
(d)(6)	Government owns feedback on the AI system; feedback containing Government Data is not used for improvement.	NiaShield collects no feedback (we collect nothing). Contract language is clean — no vendor exception to write.
(e)(1)	Disclose all AI systems used in performance of the contract to the CO within 30 days of award.	NiaShield ships a short, defensible Bill of Materials and the THIRD-PARTY-LICENSES file. Drop it into your disclosure.
(e)(4)	File the CISA incident report within 72 hours of any confirmed or suspected security incident; daily updates until resolved.	Every session emits a tamper-evident Certificate of Incineration with cryptographic timestamps; Ed25519 signatures are non-repudiable. Pull the COIs for the affected window — your CISA filing is one query away.
(e)(5)	Establish formal channels for the Government to send performance feedback and modification requests.	Process question — set up an email alias and a ticket queue. NiaShield doesn't affect this.
(h)(2)	Notify the Government within 7 days of any material change to AI safety guardrails or output truthfulness.	When we ship a material change to NiaShield , you get release notes in clause-aligned language. Pass it along.
(h)(3–4)	Notify the CO 30 days before adding or materially changing any Service Provider in the supply chain.	NiaShield 's sub-processors are documented and stable. Material changes get the same 30-day-ahead notification from us to you.
(i)(1)	Commercial efforts to ensure the AI system is truthful, neutral, nonpartisan, free of ideological manipulation.	Model-behavior mandate — sits with the chosen U.S. frontier model (Anthropic, Google, Azure OpenAI, Groq) and your system prompts. NiaShield provides per-session audit evidence for any bias-incident defense without retaining content.
(i)(3)	Liable for decommissioning costs if the Government terminates for cause under the Unbiased AI Principles.	Contractual risk allocation — not a product feature. Your contracts attorney handles this in the negotiation.

The bottom line.

The clause has roughly twenty-three distinct line items. **NiaShield** handles thirteen directly and supports the other ten with evidence and tooling. The other AI vendors you are evaluating handle none of them without architectural changes they have not yet made.

13 directly handled + 10 supported = 23 · competitors: 0

Why GPT runs through the Azure door — and never the consumer one.

The no-training mandate in (d)(3)(i) is black and white. The consumer OpenAI platform is built around retention, history, and tracking — B2C by design — so a contractor routing Government Data through it is working against the clause.

NiaShield reaches GPT models only through Azure OpenAI, inside the customer's own tenant: the same models, with the consumer machinery removed, under Microsoft's no-training contractual terms. Right models, right door. Whether a given commercial AI ToS conflicts with the clause is a question for your counsel — we make sure the architecture never puts you there in the first place.

Steve McKim

CEO & Founder, **Heaviside AI**

602-502-6899

steve@heavisideai.com

niashield.com · heavisideai.com