

The Presidential AI doctrine — what we handle for you.

For federal contractors, integrators, and the agencies they serve. Four Presidential documents now define how the Executive Branch expects AI to be bought, run, and proven. The directives below are the ones **NiaShield** and **Gateway discharge by architecture** — so your program doesn't have to. Highlighted rows come from the two anchor documents your agency opens the meeting with.

NSPM · JUN 5 2026 AI in the National Security Enterprise PRESIDENTIAL MEMORANDUM · REPLACES NSM-25	E0 · JUN 2 2026 AI Innovation, Cybersecurity & Critical Infrastructure EXECUTIVE ORDER · FULL TEXT PUBLISHED	E0 · DEC 11 2025 National AI Policy Framework EXECUTIVE ORDER · STATE-LAW PREEMPTION	E0 · JUL 23 2025 American AI Technology Stack Exports EXECUTIVE ORDER · FULL-STACK PACKAGES
CITATION	WHAT IT DIRECTS	HOW NiaShield HANDLES IT	STATUS
NSPM Fact Sheet Jun 5 2026	Rapid onboarding of the most advanced AI models <i>from multiple vendors</i> ; ends the "dangerous single-vendor dependencies" of NSM-25.	One deployment, four U.S. frontier vendors — Anthropic, Google, Azure OpenAI, and Groq — behind a single SDK. Models swap by configuration, not re-architecture. No single-vendor dependency exists to unwind.	★ FED · AGY
NSPM Fact Sheet Jun 5 2026	No entity, commercial or otherwise, can <i>disable, degrade, or modify</i> an AI system warfighters depend on without prior approval.	Single-tenant install in the customer's own Azure subscription. Heaviside AI operates no control plane into the deployment — no remote kill switch, no vendor-side update path, no operational reach. The customer's Managed Identity controls everything.	★ FED · AGY
NSPM Fact Sheet Jun 5 2026	AI will never be used to <i>conduct unlawful surveillance</i> against the American people; civil liberties are non-negotiable.	Zero data plane, zero persistence. Prompts and responses live in volatile memory only and end in SDIP-6 incineration. There is no retained record to surveil with — by architecture, not by policy.	★ FED · AGY
NSPM Fact Sheet Jun 5 2026	Accountability as a central pillar — <i>clear lines of accountability</i> from commanders and agency heads down to every fielded system.	Every session emits a signed Certificate of Incineration — Ed25519, customer-resident key, non-repudiable. Mode C ties the certificate to a credential from the customer's own IdP. Accountability arrives as a document, not a promise.	★ FED · AGY
E0 §2(c)(iii) Jun 2 2026	Facilitate access to AI-enabled tools for Federal agencies, State and local authorities, and critical-infrastructure operators — <i>rural hospitals, community banks, local utilities</i> .	Distributed through Azure Marketplace into the buyer's own tenant — the same governed AI layer for a cabinet agency or a community bank, at the buyer's scale. The operators this section names are exactly who the Contractor and Enterprise tiers were built for.	★ FED · AGY
E0 §1, Policy Jun 2 2026	Protect American ingenuity and intellectual property from <i>exploitation and theft by adversaries</i> .	PII detection rejects the request before the model is ever called — not redacted after. Non-U.S. SDKs are not in the bundle; the dependency tree is SBOM-verifiable. Nothing persists for an adversary to take.	★ FED · AGY
E0 §4 Jun 2 2026	Attorney General prioritizes enforcement (18 U.S.C. 1030 et seq.) against AI-enabled unauthorized access and data theft.	Per-session cryptographic evidence: tamper-evident, non-repudially signed certificates with timestamps. If an incident window opens, the evidentiary record for prosecution support is one query away — without Heaviside AI ever holding the content.	★ FED · AGY
E0 §6 Dec 11 2025	FCC to consider a Federal reporting and disclosure standard for AI models, preempting conflicting State laws.	Certificates are JSON. Open formats, customer-resident, export-ready. Whatever disclosure standard emerges — Federal or State — the evidence is already in a shape a regulator can read.	★ FED · AGY
E0 §7 Dec 11 2025	FTC to preempt State laws that <i>mandate altering the truthful outputs</i> of AI models.	Gateway sits in the transport, never the content. Requests are rejected or passed — never rewritten — and responses render exactly as the model returned them. There is no alteration layer for any law to fight over.	★ FED · AGY
E0 §3(b)(1)(D) Jul 23 2025	Full-stack American AI export packages must include <i>measures ensuring the security and cybersecurity</i> of AI models and systems.	Gateway is the governance layer of an American full stack: American models, customer-held keys, bounded sessions, evidence on every call. The security measure the export package needs, already productized.	★ FED · AGY

★ **Highlighted rows** = anchor-document directives. FED = **NiaShield** Federal 5.3.5 · AGY = Gateway Agency 3.0. NSPM rows cite the published Fact Sheet; the Memorandum text is not public, and we only cite what we can hand you.

And here's what your program still owns.

The doctrine puts real obligations on agencies, commanders, and the contractors who serve them — obligations no AI vendor can discharge for you. **NiaShield** supports each one with evidence and tooling, **but the action is yours.**

Why this page matters. Your compliance and mission-assurance teams will write procedures for the items below no matter which AI vendor you pick. Hand this page to your CISO and your contracts attorney before the kickoff meeting — it shows exactly where **NiaShield** evidence plugs into your response. The legal and command conclusions are theirs to make; we supply the product facts and the evidence.

CITATION	WHAT YOU'RE ON THE HOOK FOR	WHAT NiaShield GIVES YOU TO MAKE IT EASIER
NSPM Fact Sheet Jun 5 2026	Commanders, directors, and agency heads remain accountable for responsible AI use at every level of the chain of command.	The per-session evidence record your accountability review runs on: who, when, what model family, cryptographically signed — without retaining a word of content.
NSPM Fact Sheet Jun 5 2026	Updated Department of War directive on autonomy in weapon systems; annual review of AI guidance.	Out of product scope, and we say so plainly. NiaShield governs knowledge work and enterprise AI traffic — it is not a weapons-autonomy control, and we will never market it as one.
NSPM Fact Sheet Jun 5 2026	Build the talent pipeline, including the AI National Security Strategic Reserve of outside experts.	A staffing mandate — no product surface. What we contribute: a system simple enough that your existing Azure team runs it without a vendor priesthood.
EO §2(a-b) Jun 2 2026	CNSS and the Department of War prioritize cyber defense of National Security Systems and DoW information systems.	Single-tenant posture means the deployment inherits your hardening baseline automatically — your policies, your network rules, your monitoring. There is no vendor cloud to exempt.
EO §2(d) Jun 2 2026	Voluntary participation in the AI cybersecurity clearinghouse for vulnerability coordination.	Your call to join. If you do: the source-available remediation record, smoke test, and SBOM drop straight into a vulnerability-coordination workflow.
EO §3(b) Jun 2 2026	Voluntary framework for covered frontier models — early Federal access, classified benchmarking, trusted partners.	Sits with the model developers, not the governance layer. AI Choice means you ride whichever American vendors engage with the framework — and swap among them without re-architecture.
EO Fact Sheet Jul 2025	Federal government may not use AI models that embed ideological bias or social agendas; outputs must be truthful and nonpartisan.	A model-behavior mandate — it sits with the chosen U.S. frontier model and your system prompts. NiaShield provides per-session audit evidence for any bias-incident defense, without retaining content, and never alters an output.
EO §§3-5 Dec 11 2025	AI Litigation Task Force, Commerce evaluation of State AI laws, funding conditions — the Federal-State framework fight.	Government action; nothing for you to file. Whichever framework wins, the posture doesn't change: evidence in open formats, ready to prove under Federal doctrine or State law alike.

ON THE HORIZON — WHAT THE DOCTRINE TELLS YOU IS COMING

MAR 2026 — IN CONGRESS National AI legislative framework The framework fight moves from Executive Orders to statute. Whatever passes, the questions stay the same — custody, retention, proof — and the posture doesn't change: ready to prove.	MAY 2026 — UNDERWAY Frontier AI on classified networks The Department of War has agreements with eight AI companies on classified networks. The models are arriving; the governance-layer question — who proves what happened to the data — comes next.	AUG 2 2026 — 52 DAYS OUT EU AI Act enforcement begins Different flag, same questions. For programs with European exposure, the second pillar is already built — one architecture answering both Washington and Brussels.
--	--	---

The bottom line.

10 directly handled + 8 supported = 18 presidential directives

COMPETITORS, WITHOUT ARCHITECTURAL CHANGES THEY HAVE NOT YET MADE: 0

Across the June 5 Memorandum and the three Executive Orders behind it, the doctrine asks the same questions over and over: **Is it American? Who controls it? What does it retain? Can you prove it?**

NiaShield answers all four in the architecture — American-only routing, customer-tenant custody, zero persistence, and a signed **Certificate of Incineration** on every session.

IS IT AMERICAN? Locked at the binary. Four U.S.-headquartered providers — Anthropic, Google, Azure OpenAI, Groq. Non-U.S. SDKs aren't in the bundle.	WHO CONTROLS IT? You do. Your tenant, your subscription, your Managed Identity, your keys. No vendor control plane exists.	WHAT DOES IT RETAIN? Nothing. Volatile memory only. Every session ends in SDIP-6 incineration.	CAN YOU PROVE IT? Every session. A signed, non-repudiable Certificate of Incineration — verified with one command.
---	---	--	--

The architecture existed before the doctrine. NiaShield was not built to chase the June 5 Memorandum. It was built on a conviction about data privacy — before GSAR 552.239-7001 was discovered, and before this doctrine was signed. The Memorandum and the orders before it describe, almost line by line, an architecture Heaviside AI had already shipped: American models only, customer custody, zero persistence, evidence on every session. The mandate is vindication, not motivation. When the next directive lands, we expect to be early again — for the same reason.	Ready to prove. Never "compliant." We do not certify anyone's compliance, and we don't cite documents we can't hand you — the NSPM rows on page 1 cite the published Fact Sheet because the Memorandum text is not public. We hand you the architecture and the evidence; the legal conclusions belong to your counsel and your Contracting Officer. That restraint is the credibility.
--	--

Steve McKim

CEO & Founder, Heaviside AI

602-502-6899

steve@heavisideai.com

niashield.com · heavisideai.com

CDW-G — Channel Partner of Record · Azure-native via Multiparty Private Offer · Azure Marketplace. | **NiaShield, SDIP-6, Certificate of Incineration**™ Heaviside AI, LLC · U.S. Prov. App. 64/042,610 (Apr 17 2026) · 64/068,643 (May 18 2026) · Inventor of record: Steve McKim. | Source documents: NSPM Fact Sheet (Jun 5 2026); Executive Orders of Jun 2 2026, Dec 11 2025, Jul 23 2025, as published by the White House.