GRMG LLC · GLOBAL RESOURCES MANAGEMENT GROUP

AION PROTOCOL

What Strengthens AION

Strategic Capability Factors for DoD Contractors and Vendors Across All Tiers

Standalone Reference Document

Prepared by GRMG LLC — Office of the AION Architect

Scottsdale, Arizona · Subsidiary: VNClagoon (Zug, Switzerland)

Version 1.0 · Reference Document · Commercial-in-Confidence

Important Notice

This document has been prepared by GRMG LLC as a standalone strategic reference for any defense contractor — at any tier of the DoD supply chain — evaluating the AION Protocol as a security and intelligent-agent foundation in its products and programs.

It is not an offer, contract, or commitment. It identifies the architectural and procurement-enablement capabilities that, in GRMG's assessment, would strengthen AION's position across the broader DoD contractor and vendor base. Items presented as roadmap or research-track are clearly labelled as such.

Capability statements in this document are deliberately scoped to what GRMG can either demonstrate today or assert as architecturally tractable on the AION codebase. Where the analysis touches publicly-researched but not-yet-productised capability lines, that is stated explicitly. Where competitor capabilities are compared, the ratings reflect publicly-documented product literature; vendors may offer additional capability under NDA that is not captured here.

This document deliberately makes no financial, revenue, or accreditation-status claims. AION's maturity, FIPS 140-3 validation status, and ATO status are addressed in the parent TES Partnership Proposal and remain accreditation-track items here.

Contents

1. Purpose and Scope

The parent TES Partnership Proposal documents the case for Tucson Embedded Systems to act as authorized channel agent for the AION Protocol. That document is rightly bilateral: it speaks to TES's specific business, customers, and corporate structure.

This document is a different artifact. It is a standalone reference that any DoD contractor — prime, integrator, specialty vendor, or subcontractor — can read to understand what AION offers structurally, where it stands relative to publicly-documented industry alternatives, and what additional capability vectors, when developed, would make AION sought after across the broader defense contracting base rather than at any single partner.

It is intentionally written so the TES partnership conclusions remain intact while the capability narrative travels to any contractor reading it independently.

2. Document Discipline

The same claim-integrity discipline applied in the parent TES proposal applies here. Three working rules:

- Capability claims are scoped to what GRMG can either show in a running system or assert as architecturally tractable on the existing AION codebase. Items requiring new engineering are flagged as near-term roadmap. Items still in public academic or pre-commercial research are flagged as research-track.
- Comparisons against other vendors reflect publicly-documented product capability. Vendors may offer additional capability under NDA; absence in this document means absence in their public literature, not absence in their product.
- Where this document uses qualitative ratings (the comparison charts), the scoring criteria are defined alongside the chart and apply uniformly across columns. Ratings are architectural fit, not formal certification status.

This discipline matters because the audience is procurement-aware. Overclaiming once is enough to compromise the rest of the document.

3. Summary — Six Strategic Strengthening Vectors

Across the DoD contractor base, six vectors emerge consistently from current strategic mandates (Zero Trust, CNSA 2.0, CMMC 2.0, JADC2/MPE, NIST AI RMF, EO 14028) and from the structural weaknesses of the secure-communications and defense-AI vendor field. Each is achievable from the existing AION foundation, with different effort profiles.

Vector	What it is	Effort / horizon
1. Alignment artifacts	Pre-built mappings of AION → DoD ZT pillars, CMMC L2 controls, NIST AI RMF, CNSA 2.0 timeline	Document work; weeks
2. Concrete PQC	ML-KEM (Kyber) in the hybrid handshake — not 'PQC-ready,' but PQC in production	Engineering; weeks
3. TEE-attested execution	AION runs inside Intel TDX / AMD SEV-SNP / ARM CCA with remote attestation	Integration; months
4. Hardware root of trust	Device identity bound to TPM 2.0 PCR / DICE-derived identity, not software fingerprint	Engineering; months
5. Sovereign + Responsible AI	David Prime architecture with classification-aware inference, capability tokens, MITRE ATT&CK / D3FEND audit mapping	Mixed; document work + research-track engineering

Vector	What it is	Effort / horizon
6. Federated trust fabric	Inter-vendor mesh: any cleared contractor joins a shared AION-secured substrate with cross-org k-of-n custody and tamper-evident audit	Architectural; largest engineering scope, largest network effect

Figure 1. Six strengthening vectors. The full body sections cover each one with its publicly-referenceable standard and concrete next step.

4. Vector 1 — Procurement-Enabling Alignment Artifacts

DoD contractors at every tier are currently being asked the same set of questions by their primes, by procurement officers, and by their own compliance teams: how does this product align with the DoD Zero Trust Strategy? Where does it sit against CMMC 2.0 Level 2? How does it satisfy CNSA 2.0 cryptographic timelines? Does it have a documented NIST AI RMF posture? What is the SBOM and supply-chain evidence pack?

These are not engineering questions. They are document questions, and the contractors asking them are not currently getting clean answers from the secure-communications or defense-AI vendor field. A vendor that ships pre-built mapping artifacts — Zero Trust pillar by pillar, CMMC control by control, AI RMF profile by profile — gives every contractor downstream of it a procurement-time advantage.

Specific artifact set

- DoD Zero Trust Pillar Mapping — AION capability → each of the seven ZT pillars (User, Device, Application/Workload, Data, Network, Visibility/Analytics, Automation/ Orchestration).
- CMMC 2.0 Level 2 Control Evidence Pack — AION-produced artifacts mapped to applicable NIST 800-171 controls.
- NIST AI RMF Profile — Govern / Map / Measure / Manage functions documented against David Prime architecture.
- CNSA 2.0 Compliance Statement — current symmetric posture, PQC transition plan with target dates.
- Signed SBOM and reproducible-build attestation — EO 14028 supply-chain evidence.

Highest leverage per hour invested on this list. The technical work is already done; the gap is the document artifacts that translate the work into the language procurement reviewers read.

5. Vector 2 — Concrete Post-Quantum Cryptography

NIST finalised the first post-quantum standards in August 2024: ML-KEM (Kyber) for key encapsulation, ML-DSA (Dilithium) for digital signatures, and SLH-DSA (SPHINCS+) for stateless hash-based signatures. NSA's CNSA 2.0 sets transition timelines for National Security Systems — symmetric AES-256 remains compliant, but key-exchange mechanisms must migrate.

The parent proposal positions AION as 'PQC-ready.' Across the broader contractor base, 'ready' is a weaker claim than 'integrated.' The strengthening move is to integrate ML-KEM-768 or ML-KEM-1024 into the AION hybrid handshake today, so the procurement statement becomes: 'ML-KEM in the hybrid handshake; CNSA 2.0 transition aligned.'

Implementations exist in liboqs (Open Quantum Safe), in NSS, in BoringSSL forks, and increasingly in mainline OpenSSL. Integration cost is bounded; the procurement upside is a checkbox no other secure-comms vendor in the OEM space currently claims with a concrete algorithm reference.

6. Vector 3 — Hardware-Attested Trusted Execution

Intel TDX (Trust Domain Extensions), AMD SEV-SNP (Secure Encrypted Virtualization — Secure Nested Paging), and ARM CCA (Confidential Compute Architecture) provide hardware-

enforced execution environments where workload memory is encrypted and the execution state can be remotely attested. The procurement framing is direct: with TEE-attested execution, the customer can cryptographically verify that the AION runtime is the bit-exact image GRMG signed, and that no operator — including GRMG itself — has visibility into the data being processed.

This is the strongest available answer to the sovereign-data and zero-operator-trust requirements increasingly written into DoD acquisition language. Microsoft Azure Confidential Computing and Google Confidential VMs offer comparable primitives, but neither is OEM-licensable into a contractor terminal.

GRMG's existing VNClagoon partnership with Intel is a credible foundation for the TDX integration path specifically.

7. Vector 4 — Hardware Root of Trust for Device Identity

AION's current portal performs device fingerprint locking — registered devices are recognised by a software-derived fingerprint and bound to user accounts. This is operationally useful but software-only fingerprints can be replayed, virtualised, or extracted by an attacker with admin access to a stolen endpoint.

The strengthening move is to bind device identity to a hardware root of trust. Specifically:

- TPM 2.0 PCR-bound device identity — the device's cryptographic identity derives from Platform Configuration Register measurements that cannot leave the silicon. A cloned or virtualised device produces a different identity.
- DICE-derived identity (TCG Device Identifier Composition Engine) — for embedded targets without a discrete TPM, DICE provides a comparable cryptographic device-identity primitive.

Both are publicly-specified open standards (TCG TPM 2.0 specification, TCG DICE specification). Engineering cost is bounded. The procurement value: device identity becomes tamper-evident and survives physical endpoint compromise.

8. Vector 5 — Sovereign and Responsible AI Architecture

The David Prime intelligent-agent layer is, structurally, the most differentiated component AION carries — no comparable OEM-licensable secure-communications product in the defense market ships with an embedded, locally-running, policy-bound intelligent assistant. To make it sought-after rather than novel, four architectural primitives need to be both implemented and documented.

8.1 Capability tokens for tool invocation

Every agent action carries a cryptographically signed token from the planner: 'this action is authorized in service of goal X, with budget Y, expires at Z.' The executor verifies before invoking. This is the structural fix for prompt-injection attacks and ties directly to AION's existing audit-chain primitive. Defense procurement increasingly expects this; cloud-based AI agents structurally cannot provide it the same way.

8.2 Runtime policy validation against a mission constitution

Before any consequential or irreversible action, the agent self-validates the proposed action against a configurable mission-policy file. The validation event itself is written to the audit chain. The procurement framing: 'the agent has an auditable, configurable, policy-bound constraint engine that runs before every external action.'

8.3 Classification-label-aware inference

This is the research-track item. The UK AI Safety Institute, NIST AI Safety Institute, and several academic laboratories have active public research on language models that respect data-sensitivity labels at inference time and refuse cross-label leakage. A model-level solution is not yet available. A system-level enforcement layer — input tagging, label-routed processing paths, cross-label refusal, and audit-logged label transitions — is buildable today and would put the

David Prime architecture ahead of every cloud LLM vendor for classified or controlled data work.

8.4 MITRE ATT&CK and D3FEND agent-action mapping

Every tool invocation the agent makes is categorised against the MITRE D3FEND defender taxonomy and, where applicable, MITRE ATT&CK technique IDs. Blue-team operators see agent activity in language they already use. No competing AI assistant in the defense market produces this artifact today.

8.5 Documented air-gap deployment pattern

Local LLM execution (via Ollama or comparable runtimes) already makes air-gap deployment technically possible. Formalising the offline install path, offline model-update sync, and offline policy-update mechanism turns possibility into a procurement-ready capability. Cloud-based AI vendors cannot match this; it is the structural reason David Prime exists as a separate product line.

9. Vector 6 — Federated AION Trust Fabric

The single highest-leverage architectural move available to AION is to evolve from a per-deal security overlay into a federated trust fabric across the DoD vendor ecosystem. The mechanism: any cleared contractor — at any tier — can join a shared AION-secured substrate using its own AION key, with cross-organisation k-of-n custody and tamper-evident audit across the entire consortium.

This maps directly to what JADC2 (Joint All-Domain Command and Control) and Mission Partner Environment are asking for at a doctrinal level: secure data sharing across services, agencies, and coalition partners without a central operator with visibility into all traffic. Existing cross-domain solution vendors — Forcepoint, Owl Cyber Defense, and the Raytheon/Arcfield CDS line — solve adjacent problems but do not offer a contractor-licensable inter-vendor fabric of this kind.

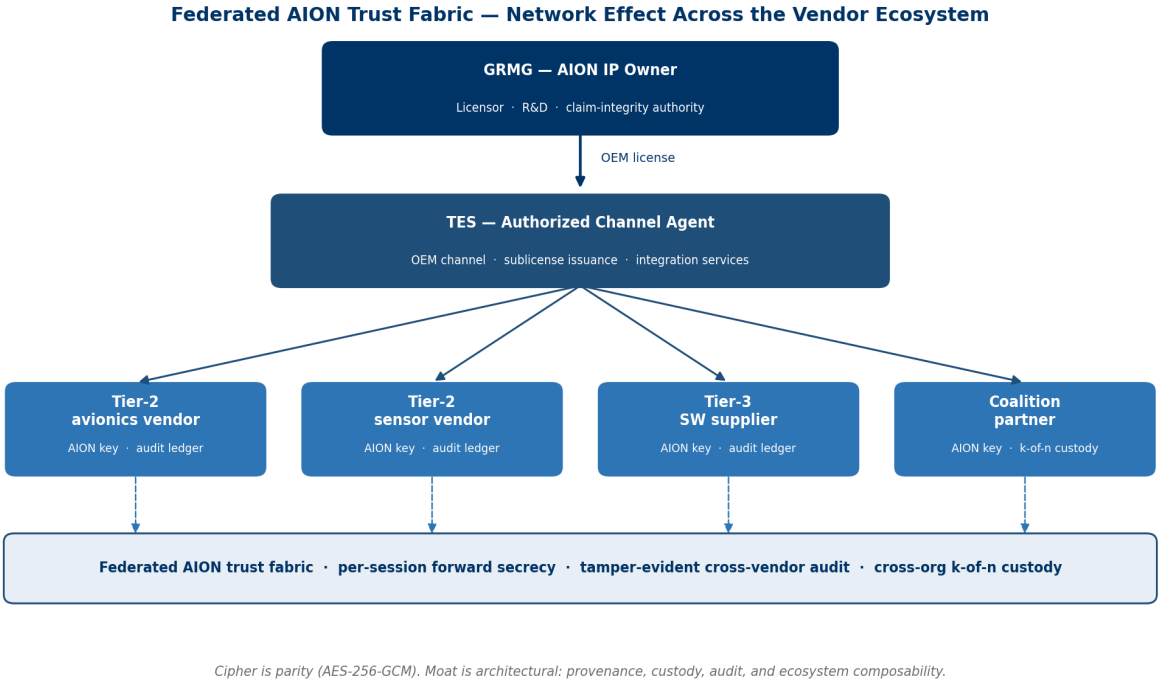

Figure 2. The federated trust fabric pattern. GRMG retains AION IP ownership; TES (or any authorized channel agent) issues sublicenses; vendors and coalition partners participate in a shared, audited, k-of-n custodial substrate. The cipher (AES-256-GCM) is industry parity; the architecture around it is the moat.

Network-effect economics. The value of a federated fabric grows with the number of cleared participants joining it. Each new contractor onboarded by TES or another channel agent makes the fabric more useful to every existing participant. This is structurally absent from per-deal secure-communications products.

10. Defense-in-Depth Through Key Custody (Not Cipher Stacking)

A common request from defense buyers is 'redundant encryption' — typically meaning wrapping AES-256 inside a second cipher such as ChaCha20-Poly1305. GRMG's position, stated openly: cipher stacking is largely cargo-cult crypto. AES-256-GCM is not the weak link in modern defense cryptography, and adding a second cipher introduces performance overhead, key-management complexity, and debugging surface without raising real-world security.

The defensible interpretation of 'defense in depth' on the cryptographic side is redundancy of key custody and provenance, not redundancy of cipher. AION already has the components for what GRMG terms four-factor key custody:

Factor	What it is	Why it strengthens
Physical-entropy derivation	Keys derived from a physical entropy source produce maximum-entropy AES-256 material	Resists weaknesses in software RNGs and seed-state attacks
Per-session forward secrecy	Keys rotate per session; compromise of one key does not retroactively expose history	Limits blast radius of any single-key compromise
Cross-org k-of-n custody	Key material is threshold-split across organisational boundaries	No single party — including GRMG — can unilaterally recover a key
Hardware-rooted device binding	Device identity bound to TPM 2.0 PCR or DICE-derived identity	Survives endpoint physical compromise; cannot be replayed from a clone

Figure 3. Four-factor key custody. Each factor is independently sourced and independently auditable. Compromise of any one factor does not, on its own, defeat the others.

This is the marketing line the broader contractor base will respond to: not 'we encrypt twice,' but 'four independent layers of key custody, each separately auditable.'

11. Comparative Positioning vs Industry Leaders

The chart below compares AION × TES — both in its current operational form and with the strengthening vectors in this document applied — against publicly-documented capabilities of the principal secure-communications and defense-AI platforms a contractor would consider as alternatives. Ratings reflect publicly-documented product literature; competitor offerings under NDA may differ.

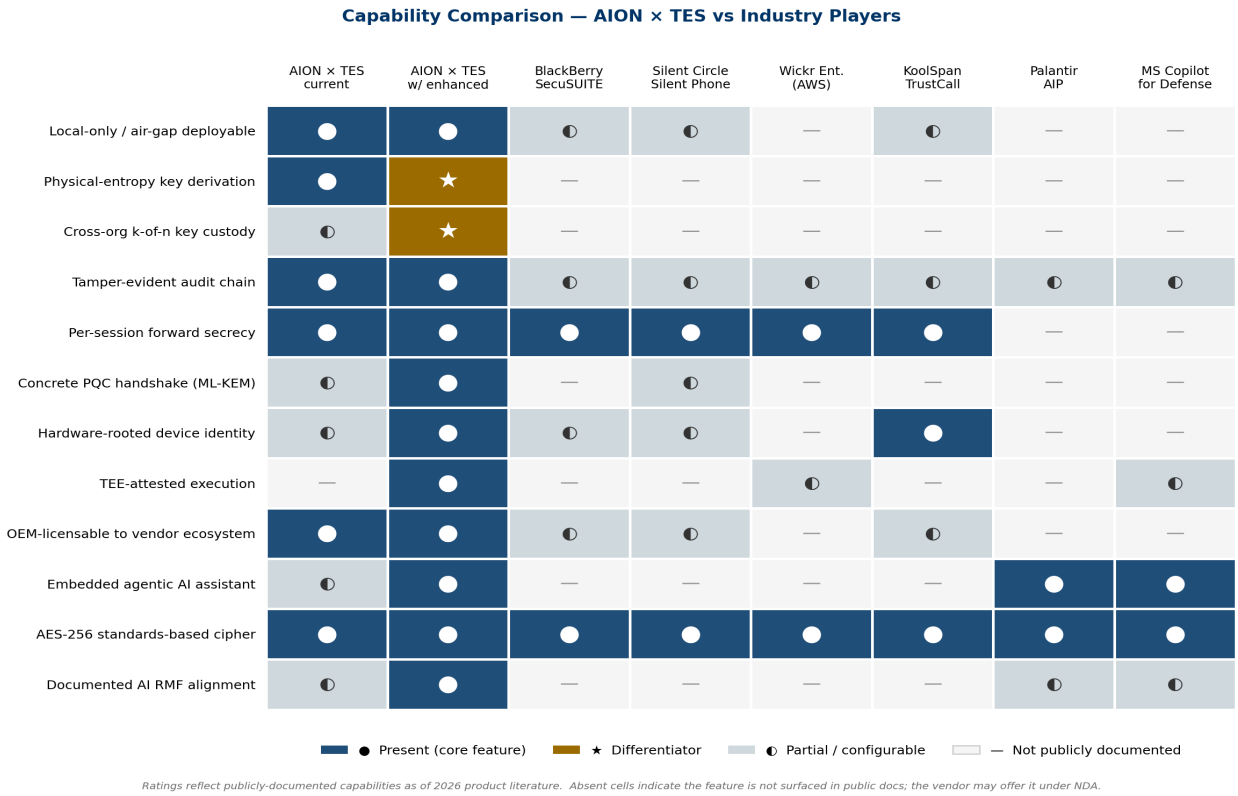

Figure 4. Capability comparison. The two AION columns show current state and the post-strengthening state described in Sections 4–9. Differentiator (★) marks capabilities where, at the public-literature level, no competitor in the comparison set offers an equivalent feature.

Reading the chart: the cipher itself (AES-256) is industry parity, as the parent TES proposal already states. The architectural advantages cluster in key origin and custody, OEM-licensable delivery, embedded agentic AI, and the AI-RMF / Responsible-AI alignment posture. These are the columns where AION × TES separates from the field.

12. DoD Strategic Mandate Alignment

The strengthening vectors in this document are not arbitrary engineering wishlist items. Each maps to a current DoD strategic mandate or executive-order requirement that contractors of every tier are now being asked to demonstrate against.

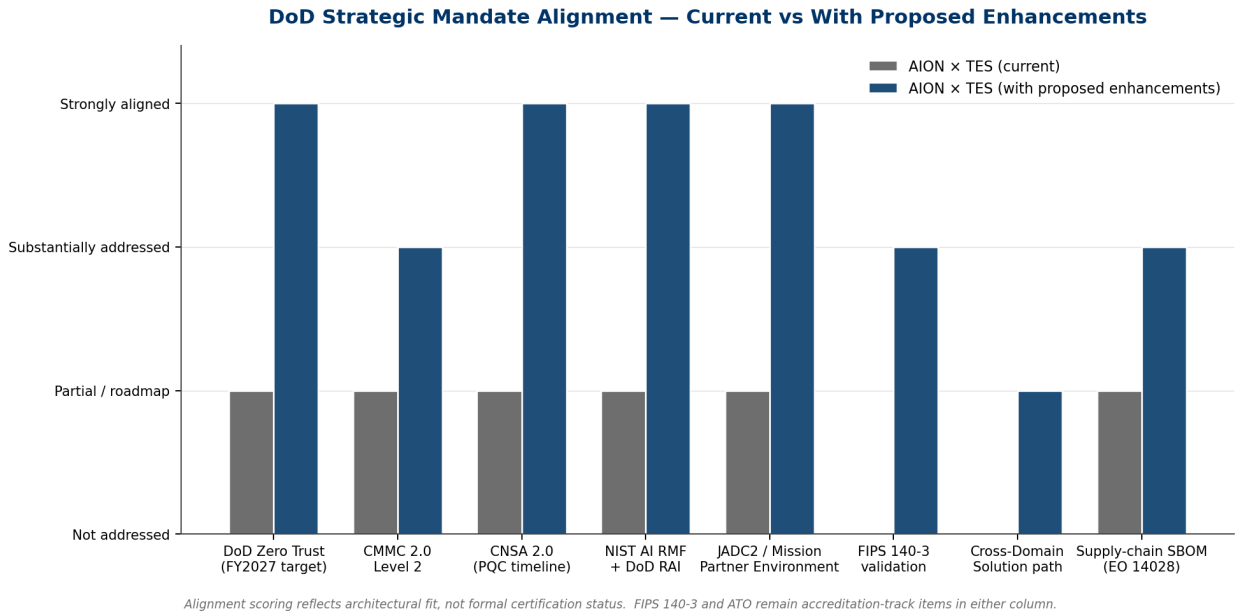

Figure 5. Mandate-by-mandate alignment. Grey bars: AION current state. Navy bars: AION with the strengthening vectors applied. Alignment is architectural fit; formal certification status (FIPS, ATO) remains a separate accreditation track in either column.

The mandates carry their own enforcement timelines. The DoD Zero Trust target year is FY2027. CMMC 2.0 Level 2 is being enforced against contracting actions through 2025–2026. CNSA 2.0 PQC transition is on a published NSA timeline. NIST AI RMF, while voluntary, is rapidly entering procurement language. EO 14028 supply-chain requirements are already binding on federal software acquisitions.

A contractor that adopts AION × TES with the strengthening vectors applied receives a near-finished compliance posture against this entire mandate set rather than having to build each alignment story per-program.

13. Tier-by-Tier Relevance Map

Different positions in the DoD supply chain value different aspects of AION. The chart below summarises which value drivers act as a primary procurement driver, a material consideration, a modest contribution, or are not relevant for each tier.

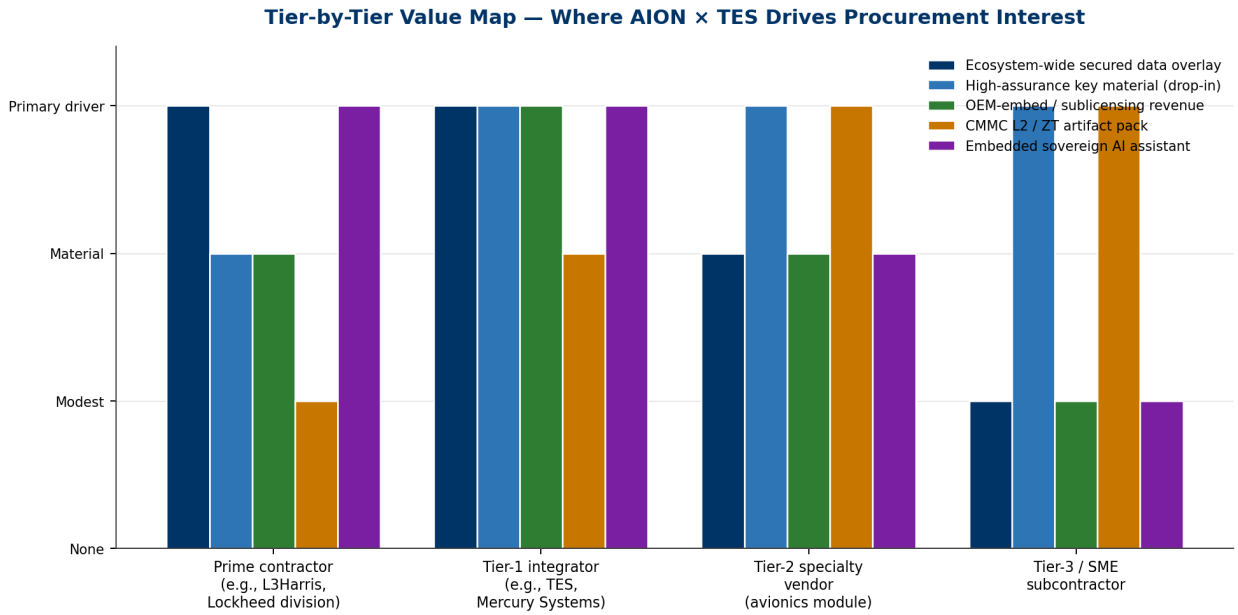

Figure 6. Tier-by-tier value distribution. Primes and Tier-1 integrators value the ecosystem-wide secured data overlay and the embedded sovereign AI assistant. Tier-2 and Tier-3 vendors value drop-in high-assurance key material and turnkey CMMC L2 / ZT artifact packs that lower their own compliance burden.

Reading the chart by tier

- Prime contractors care about ecosystem-wide overlay and embedded sovereign AI: AION is a platform play that strengthens their integration story and gives them a defense-AI capability not available from commercial cloud vendors.
- Tier-1 integrators (TES, Mercury Systems, and comparable) see every value driver — they are the natural channel agent layer where OEM-embed revenue concentrates.
- Tier-2 specialty vendors care most about high-assurance key material and CMMC artifacts: AION lowers their security-engineering burden and gives them compliance evidence they would otherwise have to produce themselves.
- Tier-3 and SME subcontractors care principally about compliance artifacts and drop-in key material: AION is, for them, the fastest path to meeting cybersecurity requirements that would otherwise price them out of contracts.

14. What This Document Does Not Claim

In keeping with the claim-integrity discipline of the parent TES proposal, the following are stated openly:

- AION does not currently hold FIPS 140-3 cryptographic module validation. FIPS validation is on the accreditation roadmap, not in the present state.
- AION does not currently hold any government Authorization to Operate (ATO). ATO support packaging is part of the proposed partnership scope, not a present claim.
- AION is not currently on the NCDSMO accredited Cross-Domain Solution list. Pursuing Raise-the-Bar accreditation is a multi-year process and is mentioned only as a long-horizon option, not a near-term capability.
- Competitor ratings in this document reflect publicly-documented capabilities as of 2026 product literature. Competitors may offer additional capability under NDA that is not captured in their public documentation.
- The 'with proposed enhancements' column in Figure 4 represents architectural fit and tractable engineering scope on the existing AION codebase. It is not a representation that those enhancements are already implemented.

- Classification-label-aware inference (Section 8.3) is identified explicitly as an active public-research line. Operationalising it at the system level is engineering work that builds on but does not require an unsolved model-level research result.
- No financial, revenue, or market-size claims are made in this document. The TES Partnership Proposal contains separately-scoped illustrative financial scenarios; nothing in this reference document should be read as a forecast.

15. Recommended Order of Pursuit

The strengthening vectors do not all carry the same effort-to-leverage ratio. For a contractor or partner evaluating where to focus, GRMG recommends pursuing them in the following order:

Order	Vector	Why first / why later
1	ZT pillar mapping + CMMC L2 + AI RMF artifact pack (Vector 1)	Highest leverage per hour invested. Document work, not engineering. Unlocks procurement conversations across every contractor tier immediately.
2	Concrete ML-KEM integration (Vector 2)	Bounded engineering effort (weeks). Converts 'PQC-ready' into a concrete CNSA 2.0 checkbox. Immediate procurement value.
3	David Prime capability tokens + policy validation + ATT&CK mapping (Vector 5, parts 8.1, 8.2, 8.4)	Locks the AI architecture story before the AI-RMF questions become procurement-blocking. Manageable engineering scope.
4	Hardware root of trust for device identity (Vector 4)	Months of engineering. Closes the most credible attack against the current device-fingerprint mechanism.
5	TEE-attested execution (Vector 3)	Months to quarters. Requires Intel TDX / AMD SEV-SNP integration depth. Highest sovereign-data value once delivered.
6	Federated trust fabric (Vector 6)	Largest architectural scope. Pursued last because the network-effect value compounds only once a non-trivial number of participants are onboarded; building it before there are channel agents to feed it is premature.
—	Classification-label-aware inference (Section 8.3)	Pursued opportunistically in parallel with research community progress. Not on the procurement-critical path.
—	NCDSMO Raise-the-Bar CDS accreditation	Long-horizon. Worth scoping eventually; not a near-term wow.

Figure 7. Recommended pursuit order. The ordering optimises for procurement-time leverage in the near term and architectural compounding in the long term.

16. Glossary

Term	Meaning in this document
AION	GRMG's operational protocol: working DSL + configurable multi-level encoding + physical-entropy AES-256 key derivation

Term	Meaning in this document
David Prime	GRMG's intelligent-agent architecture: locally-deployable, policy-bound, OEM-embeddable AI assistant designed for sovereign-data environments
ZT / Zero Trust	DoD Zero Trust Strategy framework; seven pillars governing modern defense architecture
CMMC 2.0	Cybersecurity Maturity Model Certification; Level 2 corresponds to NIST 800-171 control set
CNSA 2.0	NSA Commercial National Security Algorithm Suite version 2.0; defines PQC transition timeline for National Security Systems
NIST AI RMF	NIST AI Risk Management Framework (NIST AI 100-1) — Govern, Map, Measure, Manage functions
DoD RAI	Department of Defense Responsible AI principles, as articulated by the DoD CDAO
JADC2 / MPE	Joint All-Domain Command and Control / Mission Partner Environment — secure cross-domain data-sharing requirements
ML-KEM	Module-Lattice-based Key Encapsulation Mechanism (Kyber); NIST FIPS 203 finalised August 2024
ML-DSA / SLH-DSA	Module-Lattice / Stateless Hash-Based Digital Signature Algorithms; NIST FIPS 204 and 205
TEE	Trusted Execution Environment — Intel TDX, AMD SEV-SNP, ARM CCA; hardware-attested execution with memory encryption
TPM 2.0 / DICE	Trusted Platform Module v2.0; Device Identifier Composition Engine — hardware roots of trust for device identity
SBOM	Software Bill of Materials; supply-chain transparency artifact mandated by EO 14028
MITRE ATT&CK / D3FEND	Adversarial tactics taxonomy / defensive countermeasures taxonomy maintained by MITRE
k-of-n custody	Threshold cryptographic custody where any k of n parties can reconstruct a secret
NCDSMO	National Cross Domain Strategy Management Office; accredits Cross-Domain Solutions for DoD use

End of document — GRMG LLC · AION Protocol · Strengthening Reference · v1.0 · Commercial-in-Confidence