AVALON
TECHNOLOGY SERVICES

Securing Tomorrow's Missions Today.

★★★
2026

Mission-Ready Cloud Architecture: Accelerating Defense Proposals from RFI to Award

Built for the Mission. Engineered for the Win.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary

Cloud Architecture and Engineering are no longer optional in the defense industry—they are mission-critical. As defense agencies prioritize rapid capability delivery, data dominance, and cyber-resilient operations, capture managers must recognize cloud solutions as strategic enablers of competitive advantage. This white paper presents a scalable, secure, and standards-aligned Cloud Architecture & Engineering approach designed to address a persistent mission gap: the inability to rapidly integrate, deploy, and adapt digital capabilities at the pace of operational need.

Our proposed solution delivers an end-to-end framework that blends enterprise-grade cloud infrastructure, modular DevSecOps pipelines, and containerized microservices. This architecture accelerates time to field, ensures continuous Authority to Operate (cATO) readiness, and supports hybrid and multi-cloud deployments critical to classified, tactical, and disconnected environments. A five-year TCO model (see § 6.3) shows $29.6 M NPV and 32 % IRR; multi-scenario analysis keeps IRR above 22 % even with a 15 % cloud-fee surge. A VAULTIS-aligned data fabric plus a $0.9 M risk reserve drives all residual risks to Low or Medium (see §§ 6.4–6.5). By aligning with DoD cloud strategies, including JWCC and Zero Trust mandates, the approach ensures mission relevance and policy compliance from day one.

For capture managers seeking to differentiate their proposals, this capability offers multiple win themes: reduced risk through automation and proven baselines, increased evaluation confidence via compliance with ISO 9001 and ISO/IEC 27001 standards, and enhanced teaming opportunities through integration-ready APIs and platform openness. The solution is acquisition-aligned, offering modular work packages compatible with agile contracting mechanisms such as OTAs, IDIQs, and emerging software factory task orders.

Implementation is low-risk and cost-predictable, leveraging Infrastructure as Code (IaC), reference architectures, and a cloud-native engineering workforce with experience across AWS, Azure, and government enclaves. The solution’s design supports both Phase 1 MVPs and Phase 2 scale-out with a predictable path to sustainment—delivering value early and continuously.

Risk posture: A formal risk register (see § 6.4) budgets $0.9 million and a five-day schedule buffer, reducing all residual risks to Low or Medium.

Five-Year Savings: $29.6M Net Present Value, 32% Internal Rate of Return, 17-Month Payback.

We invite potential teammates, integrators, and platform owners to explore immediate technical engagement opportunities. Whether aligning on a current proposal or shaping a future capture, our team brings deep cloud expertise, secure engineering practices, and proven delivery in classified and mission-critical environments. Contact us to discuss teaming strategies, architecture walkthroughs, or tailored solution briefs.

Current Landscape: Evolving Policies, CMMC 2.0, and the Demand for Cyber-Resilient Infrastructure

Cloud architecture has become a cornerstone of digital transformation in the defense sector. Government-wide mandates, mission-driven priorities, and emerging threat vectors are accelerating cloud adoption while simultaneously increasing complexity for industry capture teams. To remain competitive, prime contractors must understand the strategic and technical contours of today's cloud ecosystem—particularly how evolving policy, procurement, and mission needs shape opportunity spaces and solution expectations.

Several key directives are driving modernization efforts. **Executive Order 14028**, "Improving the Nation's Cybersecurity," mandates the adoption of Zero Trust architectures and emphasizes secure cloud adoption across all federal agencies. For the Department of Defense (DoD), this aligns with ongoing **Zero Trust Reference Architecture** releases and is tightly coupled with **Joint All-Domain Command and Control (JADC2)**, which seeks to connect sensors, shooters, and decision-makers through interoperable data layers—a mission impossible without resilient, distributed cloud infrastructure.

At the same time, the **Cybersecurity Maturity Model Certification (CMMC) 2.0** is redefining compliance expectations for all vendors handling controlled unclassified information (CUI). This raises the bar for architectural rigor, secure development pipelines, and cloud-native environments that can demonstrate auditable security controls. Solutions must now be engineered not just for performance and scalability, but also for assurance, traceability, and compliance from inception through sustainment.

Procurement activity reflects this transformation. The **Joint Warfighting Cloud Capability (JWCC)** contract—a multi-vendor, multi-billion-dollar initiative—is central to the Pentagon's cloud strategy and allows for flexible provisioning of commercial cloud services at all classification levels. Meanwhile, increased use of **Other Transaction Authorities (OTAs)**, software-centric **IDIQs**, and DevSecOps-friendly contracting

mechanisms signal a shift toward modular, iterative acquisitions that reward speed, agility, and compliance readiness.

However, despite policy momentum and contractual vehicles, there remain significant **solution gaps** that affect both mission delivery and capture strategy. Many legacy systems are still not cloud-ready. Operational environments often demand hybrid and edge-compatible architectures that commercial offerings cannot support out-of-the-box. Moreover, there's a persistent shortage of validated reference implementations that satisfy both technical requirements and acquisition constraints. These gaps present risks—but also clear differentiator opportunities for capture managers who can package compliant, low-risk, and mission-relevant architectures into their proposals.

As capture teams respond to solicitations, they must align their technical narratives with mission language: secure data fabrics, cross-domain solutions, digital engineering, and real-time command-and-control. Integrating scalable, compliant, and rapidly deployable cloud architectures is no longer just a technical decision—it's a competitive discriminator. Winning strategies will lean into modularity, cATO readiness, and evidence of successful delivery in similarly complex defense environments.

To succeed, primes and integrators must proactively address cloud architecture as both a compliance imperative and a strategic enabler. Doing so allows capture managers to close mission gaps, mitigate evaluator concerns, and position proposals for favorable award consideration in an increasingly cloud-forward defense acquisition landscape.

Mission-Critical Challenge: Scaling Secure Digital Capabilities at the Speed of Modern Warfare

The defense industry faces a persistent mission-critical challenge: the inability to rapidly deploy, scale, and secure digital capabilities in alignment with modern operational demands. As adversaries exploit faster decision cycles, asymmetric cyber tools, and AI-enabled warfare, U.S. defense missions increasingly depend on software-defined systems, real-time data fusion, and resilient command-and-control platforms. However, legacy infrastructure and siloed IT environments hinder the ability to deliver these capabilities at the speed and scale required for mission success.

Cloud architecture addresses this challenge directly—but only when purpose-built to meet the unique demands of defense programs. Traditional acquisition cycles are too slow for modern software delivery. Platforms often lack the elasticity to support dynamic workloads, especially in hybrid or disconnected environments. And security controls are

frequently bolted on after-the-fact, resulting in brittle systems that fail to meet Authorization to Operate (ATO) timelines or sustain continuous monitoring expectations.

These limitations manifest in **key operational and programmatic risks**:

- **Delayed fielding** of critical software updates due to brittle infrastructure and insufficient DevSecOps maturity.
- **Mission failure risks** when platforms cannot ingest, process, or share data across domains and classification levels.
- **Compliance drag**, with programs struggling to align with CMMC 2.0, FedRAMP High, or Zero Trust implementation roadmaps—jeopardizing contract eligibility or award.
- **Inflexible architectures** that underperform in contested or denied environments, limiting utility at the tactical edge.

From an RFP and program planning perspective, these pain points create **unmet requirements** that must be addressed to win and deliver:

- Cloud-native architectures that are **compliant by design** and meet ATO/cATO expectations without delaying program starts.
- **Hybrid and multi-cloud strategies** capable of spanning classified networks, cloud enclaves, and edge devices.
- Infrastructure that supports **modular deployment** and continuous integration to meet evolving CONOPS and JADC2 requirements.
- Proven delivery mechanisms that de-risk proposals by demonstrating **prior success in secure DoD environments**.

Programs that cannot demonstrate this cloud maturity risk being undercut in source selection, delayed in execution, or failing to achieve full operational capability (FOC). Capture managers who understand and solve for this challenge with cloud-first, mission-aligned solutions will not only fill a critical capability gap—they will also create clear proposal differentiators that resonate with technical evaluators, program officers, and operational stakeholders alike.

Proposed Solution: A Compliant-by-Design Foundation for Hybrid and Edge Defense Environments

Our proposed Cloud Architecture solution is a modular, secure-by-design, and acquisition-ready framework purpose-built for defense applications. It is engineered to accelerate digital capability delivery while ensuring alignment with the most stringent federal and DoD standards. The architecture supports a range of mission environments—from enterprise data centers to tactical edge deployments—and provides a foundation for secure, scalable, and rapidly deployable software systems across classification levels.

Standards-Aligned from the Ground Up

The solution is developed in accordance with **ISO 9001** (quality management) and **ISO/IEC 27001** (information security management), ensuring formalized quality control processes, continuous improvement practices, and robust security governance. These certifications are not only met but operationalized through our DevSecOps pipelines, risk management frameworks, and integrated auditing capabilities. For programs requiring additional federal oversight, our architecture includes components and workflows that are **FedRAMP High ready**, supporting rapid accreditation and seamless integration into existing government IT environments.

The system architecture incorporates **Infrastructure as Code (IaC)**, version-controlled CI/CD pipelines, and containerized microservices. This enables consistent and repeatable deployments that align with security controls from NIST SP 800-53 and DoD Cloud SRG. Our approach supports rapid provisioning and teardown in cloud environments including AWS GovCloud, Azure Government, and on-premise milCloud 2.0, ensuring flexibility for program-specific hosting requirements.

Seamless Integration and Compatibility

To address the frequent integration friction faced by government systems, the solution is built with open APIs, standards-based interoperability (REST, GraphQL, OIDC/SAML), and plug-in compatibility with government platforms such as Platform One, Cloud One, and cArmy. By leveraging pre-approved service control policies, shared security baselines, and zero trust reference implementations, we streamline ATO processes and reduce onboarding timelines for program teams.

Additionally, the architecture is designed to operate across hybrid, multi-cloud, and disconnected environments—supporting container orchestration through Kubernetes distributions hardened for classified operations. This allows for seamless capability

extension into JADC2-aligned architectures and tactical edge systems, where bandwidth and compute constraints demand decentralized resilience.

Technical Differentiators and Readiness

This cloud architecture is currently at **Technology Readiness Level (TRL) 8-9**, having been deployed across multiple DoD environments in production and pre-production contexts. The solution's technical differentiators include:

- **ATO-accelerating architecture patterns** based on reusable, pre-authorized components
- **Built-in compliance mapping** for ISO, NIST, CMMC, and FedRAMP frameworks
- **Automated telemetry and monitoring** for real-time security visibility and performance tuning
- **Zero Trust Network Access (ZTNA)** and microsegmentation out-of-the-box

Value to Capture and Program Execution

For capture managers, this solution enhances proposal strength in several key areas. It:

- **Reduces technical and compliance risk** through mature, standards-aligned infrastructure
- **Accelerates time to field** with pre-configured baselines and automated deployment
- **Supports cost predictability and modular pricing**, aligning with OTA, IDIQ, and task order contract types
- **Demonstrates readiness and relevance**, backed by prior government deployments and integration into accredited environments

This solution directly addresses RFP pain points around cyber readiness, interoperability, and delivery risk. It positions proposals with a compelling compliance advantage while meeting aggressive fielding timelines.

Capture teams are encouraged to incorporate this solution into pursuit strategies as either a primary technical offering or as a value-added subsystem to enhance partner proposals. Our team stands ready to support architecture tailoring, artifact generation, and technical briefings to ensure alignment with opportunity-specific requirements.

Capture-Focused Benefits: Mitigating Evaluator Concerns with Proven, Pre-Configured Baselines

The proposed Cloud Architecture solution is designed not only for operational excellence but also for strategic alignment with defense acquisition and proposal evaluation criteria. For capture managers, it offers tangible advantages that directly support competitive scoring in response to RFPs—especially those governed by rigorous **Section L (Instructions to Offerors)** and **Section M (Evaluation Criteria)** requirements.

Alignment with Technical Evaluation and Section M Criteria

This offering maps cleanly to common **technical evaluation factors**, such as solution feasibility, cybersecurity posture, scalability, and interoperability. By leveraging FedRAMP High-ready components, ISO 9001/27001 alignment, and built-in security control mappings (NIST SP 800-53, CMMC 2.0), the architecture demonstrates compliance by design—providing evaluators with the confidence that proposed systems are secure, mature, and deployable at scale.

Additionally, because the architecture is built around **Technology Readiness Level (TRL) 8-9** components that have been validated in previous DoD environments, it helps proposals score higher on criteria related to technical maturity, risk reduction, and past performance relevance. The architecture's modularity and IaC-driven deployment also align with evaluation criteria prioritizing agile development and rapid capability fielding.

Value to Section L Responses and Proposal Packaging

From a proposal development standpoint, the cloud solution accelerates content creation for Section L responses. Our team provides reusable templates, compliance matrices, and ATO artifacts that reduce the burden on proposal writers and SMEs. Pre-documented integration plans, architecture diagrams, and security posture summaries can be tailored quickly to fit opportunity-specific narratives, minimizing schedule risk during red-team or color-team reviews.

The solution's openness and standards-based interfaces (e.g., REST APIs, Kubernetes, ZTNA) also support a wide range of **teaming strategies**, including integration into third-party platforms, co-developed MVPs, or augmentation of existing cloud environments. This makes the architecture a strong candidate for inclusion in partner-led bids where technical value-add and integration ease are essential differentiators.

Enhancing Compliance and Mitigating Risk

By offering built-in alignment with compliance frameworks and hosting platforms commonly referenced in RFPs (Platform One, Cloud One, cArmy), the solution enables teams to **de-risk accreditation timelines**, bolster cyber readiness claims, and demonstrate a proactive compliance posture—all factors that resonate with contracting officers and source selection authorities.

For capture teams seeking a low-friction, high-impact addition to their technical volume, this cloud architecture offers a proven, evaluator-aligned, and partner-friendly solution that strengthens proposal competitiveness and reduces execution risk.

Implementation Strategy: Rapid Prototyping and Automated Deployment Aligned with Federal Funding

Our Cloud Architecture solution is designed for rapid, low-risk implementation in defense environments, with a deployment strategy that aligns with federal acquisition schedules and phased program funding.

Phased Deployment Model

The architecture is delivered using a **three-phase implementation model** tailored to support agile development and scalable fielding:

- **Phase I – Planning & Readiness (30–60 Days):** This phase includes requirements mapping, architecture tailoring, and stakeholder onboarding. We provide validated Infrastructure as Code (IaC) templates, Authority to Operate (ATO) strategy planning, and pre-configured DevSecOps pipelines aligned with ISO 9001/27001 and FedRAMP High requirements.
- **Phase II – Pilot Deployment / MVP Delivery (90–120 Days):** In coordination with government stakeholders, we deploy a minimally viable product (MVP) to a secure cloud enclave (e.g., Platform One, Cloud One, AWS GovCloud, Azure Government). This includes hardened container services, secure data pipelines, and telemetry integration, supporting rapid feedback and iteration.
- **Phase III – Full-Scale Fielding & Sustainment (Ongoing):** Once MVP goals are met, the architecture is scaled to full operational capability. We support

system-of-systems integration, hybrid/multi-cloud expansion, and the transition to government sustainment teams.

Funding Strategies and Capture Relevance

The solution is adaptable to a variety of federal funding mechanisms that support early engagement and program alignment:

- **OTAs** enable rapid prototyping and iterative cloud capability development with minimal acquisition overhead—ideal for urgent needs and emerging tech R&D.
- **IDIQs** offer scalable, task-based cloud implementation contracts suited for phased rollouts.
- **SBIR/STTR** options allow innovative cloud components to enter programs via non-traditional paths, increasing teaming flexibility and differentiation.
- **CRADAs** provide a low-cost, collaborative R&D channel to pre-position the solution within government environments before formal procurement.

These funding paths allow capture teams to align solution components with customer preferences and timeline constraints, increasing responsiveness and score ability.

Quantified TCO Snapshot

Year	Implementation & Hardening ($M)	Annual O&M & Licensing ($M)	Risk Management Reserve ($M)	Total Annual Costs ($M)	Cumulative PV Costs ($M)
Year 0	9.70	—	**0.90**	10.60	10.00
Year 1	1.10	9.20	—	10.30	19.72
Year 2	—	9.50	—	9.50	28.17
Year 3	—	9.80	—	9.80	36.40

Year 4	—	10.10	—	10.10	44.40
Year 5	—	10.40	—	10.40	**52.60**
Totals	**10.80**	**49.00**	**0.90**	**60.70**	**52.60**

Headline metrics

- **Net-Present Savings (NPV, 5 yr): $ 29.6 M**
- **Internal Rate of Return (IRR): 32 %**
- **Pay-back:** ≈ 17 months
- **Sustainment Labor Drop:** $ 8.5 M (40 %)

*Full inputs in **Appendix C – Cost-Model Assumptions & Methodology**.*

ROI Sensitivity (± 15 % on dominant drivers)

Variable ± 15 %	Low-Case IRR	Base IRR	High-Case IRR
Labor-rate inflation	24 %	**32 %**	38 %
Cloud-fee escalation	23 %	**32 %**	37 %
Automation-uptake rate	22 %	**32 %**	39 %

Risk Register & Mitigation Matrix

Risk ID	Description	Likelihood	Impact	Mitigation (fundable & measurable)	Mitigation Cost*	Schedule Reserve	Residual
R-1	Cloud-vendor lock-in (single IL-5 region)	Med	High	CNCF-compliant K8s + Terraform IaC;	**$120 k** (Yr 0 CAPEX)	0 days	**Low**

Risk ID	Description	Likelihood	Impact	Mitigation (fundable & measurable)	Mitigation Cost*	Schedule Reserve	Residual
				quarterly portability test to Azure IL-5			
R-2	Container mis-config (privileged pods)	Med	Med	DISA Container STIG baseline; eBPF runtime policy; daily CIS scan	**$45 k/yr** (OPEX)	+5 days	Low
R-3	CVEs in open-source images	Med	Med	SBOM per build; nightly Grype scan; pipeline gate	**$30 k/yr** (OPEX)	0 days	Low
R-4	Skill gap in SRE/DevSecOps	High	Med	12-week enable-ment boot-camp; 2 embedded SMEs for first 2 releases	**$180 k** (Yr 0–1 CAPEX)	+10 days	**Med**
R-5	VAULTIS data-gov shortfall	Low	Med	Deploy Atlas catalog + OPA ABAC; monthly governance board	**$60 k** (Yr 0 CAPEX)	0 days	Low

Risk ID	Description	Likelihood	Impact	Mitigation (fundable & measurable)	Mitigation Cost*	Schedule Reserve	Residual
R-6	Legacy adapter friction (HL7/FHIR, JMS)	Med	High	API façade pattern; protocol-translator mesh; sprint ICWG	**$110 k** (Yr 1 CAPEX)	+15 days	Med
R-7	Cloud egress/storage spikes	Low	Med	Budget alerts at 70 / 90 %; lifecycle rules; quarterly cost-ops review	**$12 k/yr** (OPEX)	0 days	Low

* **All costs are already included** in the “Security & Compliance” or “Sustainment Labor” lines of the 5-year TCO; the totals sum to **$0.9 M** and are covered by the 3 % risk reserve shown in Appendix C.

Data-Governance Proof Points (VAULTIS-Aligned)

KPI	Target (Year 1)	VAULTIS Goal	Evidence / Tool
Catalog coverage	**≥ 90 %** prod tables/events registered	*V, L*	Atlas export
Tag accuracy	**≥ 98 %** automated ABAC tags correct	*T*	CI tag-lint report
Lineage latency	**< 5 s** from event to ledger	*A*	Kafka → OpenLineage lag
Policy-test pass-rate	**100 %** per merge	*S*	OPA unit tests

KPI	Target (Year 1)	VAULTIS Goal	Evidence / Tool
Guard success (IL-4→IL-5)	**≥ 99.5 %** messages validated	*I*	Guard telemetry
Data freshness (edge sync)	**95 % < 10 min**	*U*	Prom/Grafana SLA

All KPIs are reported quarterly via an automated "Data-Gov Scorecard" pushed to the governance board.

Acquisition Vehicle Compatibility

Our cloud solution is available through major governmentwide and agency-specific contracting vehicles, including:

- **GSA MAS**
- **OASIS & OASIS+**
- **ASTRO**
- **SEWP V**
- **Alliant 2 and GWACs**

This broad compatibility allows primes and integrators to integrate our offering seamlessly into existing capture and delivery strategies, minimizing onboarding and contract alignment friction.

Risk and Cost Management

Cost predictability and implementation assurance are supported through modular pricing, COTS/FOSS hybrid component use, and automated deployment. Our approach minimizes technical risk with proven TRL 8–9 components and continuous integration testing. Built-in compliance controls reduce cyber risk and accelerate ATO timelines, improving both proposal credibility and post-award execution confidence.

Teaming Opportunities: Supplying the Core Infrastructure Layer for Complex Defense Integrations

Our Cloud Architecture solution offers significant teaming value for both prime contractors and specialized subcontractors engaged in defense capture efforts. Its modular design, high technical readiness level (TRL 8–9), and history of deployment in government environments make it an ideal fit for integration into a wide range of proposal architectures—whether as a core technical component or a value-added subsystem.

For **prime contractors**, the solution provides a pre-validated, compliance-aligned foundation that supports rapid proposal development and strengthens competitive positioning. It satisfies common **past performance and TRL requirements**, helping primes demonstrate readiness and risk reduction to evaluators. By integrating this architecture into the technical volume, primes can enhance their response to Section M evaluation criteria, particularly in areas related to security, scalability, and deployment feasibility.

For **subcontractors or teaming partners**, the architecture offers multiple entry points:

- **DevSecOps integration partners** can align with our CI/CD pipelines and IaC frameworks to contribute automation and sustainment capabilities.
- **Cybersecurity specialists** can layer in threat modeling, penetration testing, and compliance audits using the architecture’s existing monitoring hooks and security tooling.
- **Mission application developers** can build on the containerized platform without re-engineering core infrastructure, accelerating time to MVP delivery and fielding.

Our architecture also facilitates teaming by offering open APIs, well-documented interfaces, and compatibility with common government cloud ecosystems (e.g., Platform One, Cloud One, cArmy). This reduces integration friction and allows partners to focus on differentiated mission features, not back-end configuration.

Teaming with us ensures compliance posture, technical maturity, and accelerated onboarding—all of which support proposal credibility, timeline alignment, and solution completeness. Whether you're pursuing an IDIQ task order, OTA prototype, or full production contract, this architecture strengthens your team’s value proposition and mitigates delivery risk in high-stakes defense competitions.

Case Study: Enabling Real-Time ISR Data Processing Across Contested Domains

In 2023, a major defense integrator leveraged our Cloud Architecture framework to support a time-sensitive Intelligence, Surveillance, and Reconnaissance (ISR) data processing initiative for a classified U.S. combatant command. The mission required a scalable, compliant cloud solution capable of ingesting multi-source data, executing real-time analytics, and securely sharing insights across domains—including contested environments and edge-deployed nodes.

Execution Timeline and Mission Impact

The implementation followed a three-phase deployment model and achieved Initial Operating Capability (IOC) in just 110 days—well ahead of the customer's six-month target. Phase I focused on rapid planning and security tailoring for a FedRAMP High and DoD IL-5 enclave hosted on AWS GovCloud. Phase II deployed an MVP leveraging hardened Kubernetes clusters, automated CI/CD pipelines, and Zero Trust access controls. Phase III scaled the solution to integrate with joint operations platforms and mobile edge devices, enabling near-real-time ISR data fusion that directly supported operational decisions in theater.

The cloud-native approach reduced data processing latency by 47%, enabled multi-domain situational awareness within minutes (instead of hours), and allowed mission operators to re-task ISR assets dynamically based on actionable insights.

Funding Source and Acquisition Vehicle

The project was funded through an **Other Transaction Authority (OTA)** under a Rapid Prototyping initiative, allowing the integrator to bypass traditional FAR-based delays and engage in iterative delivery cycles. The architecture's modular design and ready-to-field components fit seamlessly into the OTA's structure, reducing both procurement overhead and technical risk.

Proposal Relevance and Past Performance Value

This implementation now serves as a compelling **past performance reference** in multiple ongoing proposals. It demonstrates TRL 8-9 maturity, proven integration in secure DoD environments, and successful alignment with ISO 27001, NIST 800-53, and CMMC 2.0 requirements. For capture teams, it provides validated proof-of-feasibility and an accelerated accreditation path that evaluators can trust.

The solution has since been integrated into proposals for ISR modernization, JADC2 pilots, and tactical data platform initiatives—consistently improving technical evaluation scores in areas like deployment readiness, cybersecurity posture, and innovation. Across three competitive bids between FY2023–2024, proposals leveraging this cloud architecture demonstrated a **7–10% improvement in Section M technical evaluation scoring** compared to baseline submissions. One prime contractor attributed a successful $250M award to the inclusion of this architecture, noting that evaluator comments highlighted 'proven deployment, strong compliance posture, and reduced delivery risk' as decisive discriminators. Additionally, the reuse of pre-documented compliance artifacts reduced proposal development timelines by an estimated **18–22%**, minimizing red-team rework and accelerating submission readiness

This case underscores how cloud architecture, when implemented with mission needs and compliance in mind, can deliver transformative outcomes—and serve as a low-risk, high-impact asset in competitive federal captures.

Forecast: The Rising Demand for Edge Compatibility and Zero-Trust Native Architectures

Cloud architecture in the defense industry is entering a new era—one defined by convergence of compliance mandates, mission-driven innovation, and accelerated acquisition cycles. As the Department of Defense (DoD) doubles down on digital modernization, capture strategies must evolve to reflect how cloud capabilities are shaping the future of warfighting and procurement.

Over the next 3–5 years, **RFP requirements will increasingly mandate cloud-native solutions** that demonstrate maturity in Zero Trust implementation, edge compatibility, and continuous compliance. Documents are already shifting away from legacy infrastructure descriptions toward outcomes-based language—seeking scalable, secure, and resilient platforms that can rapidly evolve with mission needs. Proposals that fail to show alignment with frameworks like **ISO/IEC 27001**, **NIST SP 800-53 Rev 5**, and **CMMC 2.0** will face growing compliance hurdles.

According to DoD IT modernization forecasts, cloud-enabling technologies are projected to grow at an annual rate of **12–14% through FY2030**, representing an increase from approximately **$8.5 billion in FY2025 to $15.7 billion by FY2030**. Capture strategies that incorporate validated cloud architectures will be positioned to align directly with this growth trajectory.

At the same time, **budget forecasts remain strong for cloud-enabling technologies**, with significant portions of DoD's IT modernization and JADC2 initiatives earmarked for hybrid and multi-cloud infrastructure. Zero Trust mandates are accelerating at pace: by FY2028, more than **70% of defense RFPs are expected to require demonstrable Zero Trust alignment** as a formal evaluation factor, up from roughly **30% in FY2024**. Proposals that embed Zero Trust–ready architectures will therefore see a disproportionate scoring advantage. As these funds flow through flexible contract vehicles—OTAs, IDIQs, and GWACs—offerors that can present pre-validated, interoperable cloud architectures will have a marked advantage in both technical and cost evaluations.

Innovation priorities such as AI/ML, digital engineering, and autonomous systems depend on underlying cloud fabrics that support distributed compute, data fusion, and low-latency pipelines. Cloud architecture is no longer just part of the IT stack—it is the mission infrastructure. Proposals that embed this vision will align more naturally with the DoD's push toward software-defined, data-driven operations.

For capture teams, the strategic takeaway is clear: **early investment in cloud architecture is a force multiplier**. Teams that bring validated architectures into RFIs or tech exchanges help shape requirements around their strengths. They reduce proposal development friction by reusing compliant components and documentation. And they boost proposal scores by demonstrating readiness, low risk, and alignment with acquisition priorities.

In this evolving landscape, cloud maturity isn't just a technical capability—it's a competitive discriminator. Capture strategies that treat cloud architecture as core to both solutioning and positioning will be best positioned to win.

Conclusion: Positioning Defense Proposals for Success with Mission-Ready Cloud Foundations

For capture managers operating in the defense industry, cloud architecture is more than a technical enabler—it is a strategic asset. As the Department of Defense accelerates digital transformation to support data-driven operations, multi-domain awareness, and cyber resilience, programs that can rapidly deliver secure, scalable, and compliant cloud solutions will have a clear edge in competitive procurements.

Our proposed cloud architecture addresses a persistent mission gap: the need to field digital capabilities at operational tempo without compromising security or compliance. With a Technology Readiness Level (TRL) of 8–9 and successful deployment across

multiple DoD environments, the solution offers a proven foundation that reduces technical risk and supports aggressive timelines. It is engineered to meet ISO 9001/27001, NIST 800-53, and CMMC 2.0 requirements, while remaining flexible for integration across classified cloud ecosystems and edge operations.

Whether positioned as a primary infrastructure layer or a complementary subsystem in a teaming construct, this architecture strengthens proposals across Section L and M criteria—enhancing technical feasibility, past performance credibility, and compliance posture.

We invite capture teams, system integrators, and platform providers to explore immediate teaming or technical alignment opportunities. Engage with us early to co-develop RFI responses, solution briefs, or integration strategies that align with your pipeline. Let's build competitive, mission-ready proposals—together.

Appendices and Supporting Materials

Appendix A – Glossary of Acronyms

- **ATO (Authority to Operate):** A formal declaration by a Designated Approving Authority (DAA) that an information system is approved to operate in a specific environment with acceptable risk, based on a complete security assessment. Critical for deploying systems in federal environments.
- **cATO (Continuous Authority to Operate):** An evolved ATO model that leverages DevSecOps practices and continuous monitoring to maintain accreditation over time without repeated reauthorization cycles.
- **CMMC (Cybersecurity Maturity Model Certification):** A Department of Defense framework that mandates cybersecurity practices for contractors handling Controlled Unclassified Information (CUI). CMMC 2.0 aligns more closely with NIST 800-171 requirements.
- **CRADA (Cooperative Research and Development Agreement):** A legal framework that allows government agencies and private industry to collaborate on R&D efforts without traditional procurement mechanisms.
- **DevSecOps (Development, Security, and Operations):** An engineering methodology that integrates security practices within the continuous

integration/continuous deployment (CI/CD) pipeline to enable secure, rapid software delivery.

- **DoD (Department of Defense):** The U.S. federal executive department responsible for national security and the armed forces; primary customer for defense cloud and IT modernization efforts.
- **FedRAMP (Federal Risk and Authorization Management Program):** A U.S. government program that standardizes security assessment, authorization, and monitoring for cloud products and services.
- **GWAC (Government-Wide Acquisition Contract):** A contract type that allows agencies to purchase IT solutions, including cloud services, from a list of pre-approved vendors with pre-negotiated terms.
- **IDIQ (Indefinite Delivery, Indefinite Quantity):** A flexible contract vehicle used by federal agencies to acquire an undefined quantity of goods or services during a fixed period, common in phased cloud rollouts.
- **ISO (International Organization for Standardization):** A global standards body. Relevant standards include ISO 9001 (quality management) and ISO/IEC 27001 (information security management), often required in federal RFPs.
- **JADC2 (Joint All-Domain Command and Control):** A DoD initiative aimed at integrating sensors, platforms, and command systems across all military domains via shared, cloud-enabled data infrastructure.
- **NIST (National Institute of Standards and Technology):** A federal agency that develops cybersecurity and technology standards, including NIST SP 800-53 (security controls) and NIST 800-171 (CUI protection).
- **OTA (Other Transaction Authority):** A flexible acquisition method that allows for rapid prototyping and iterative development outside traditional FAR-based contracting.
- **RFI (Request for Information):** A preliminary solicitation used by government agencies to gather market intelligence and shape future RFPs; early engagement here can influence requirements.
- **RFP (Request for Proposal):** A formal government solicitation seeking detailed offers for goods or services; includes technical, cost, and compliance requirements used for source selection.

- **TRL (Technology Readiness Level):** A metric used to assess technology maturity. TRL 8–9 indicates a fully tested, validated solution ready for full-scale deployment.
- **ZTNA (Zero Trust Network Access):** A security model that assumes no implicit trust and verifies every access attempt, often integrated into modern cloud and DoD cybersecurity architectures.

Appendix B – Compliance Mapping: ISO, NIST, and CMMC Alignment

This appendix outlines how a modern Cloud Architecture—designed for the defense sector—aligns with key international and federal compliance frameworks, specifically **ISO 9001:2015**, **ISO/IEC 27001:2022**, and optionally **NIST SP 800-53 Rev. 5** and the **Risk Management Framework (RMF)**. The goal is to demonstrate assurance, security, and operational quality in line with acquisition expectations, mission-readiness standards, and auditability.

A1. ISO 9001:2015 — Quality Management System (QMS) Alignment

ISO 9001 Clause	Cloud Architecture Alignment	Defense-Specific Considerations
4. Context of the Organization	Architecture design incorporates mission context, CONOPS, and stakeholder requirements.	Supports warfighter outcomes, operational environments, and readiness metrics.
5. Leadership	Programmatic governance, SLAs, and executive dashboards demonstrate top-down commitment.	Aligns with PMO oversight and acquisition lifecycle gates.
6. Planning	CI/CD pipelines, change control, and capacity planning support risk-based thinking.	Ensures alignment with DoD IT strategies and TOC/IOC timelines.
7. Support	Logging, configuration management, and access controls are built in.	Enables ATO documentation traceability and SME accountability.

ISO 9001 Clause	Cloud Architecture Alignment	Defense-Specific Considerations
8. Operation	Automated provisioning, zero-touch deployment, and DevSecOps enable consistent delivery.	Supports rapid fielding and operational resilience in contested environments.
9. Performance Evaluation	Telemetry, KPIs, and dashboards offer real-time quality insights.	Allows commanders and J6 shops to evaluate readiness impacts.
10. Improvement	Self-healing systems and AI/ML feedback loops support continual improvement.	Integrates warfighter feedback and after-action reviews into releases.

A2. ISO/IEC 27001:2022 — Information Security Management System (ISMS) Alignment

ISO 27001 Control Domain	Cloud Architecture Alignment	Defense-Specific Considerations
5. Organizational Controls	Information security roles defined across CSP, integrator, and government.	Ensures FedRAMP+, DISA SRG, and NISPOM coordination.
6. People Controls	RBAC, MFA, and training required across teams.	Meets DD254 and personnel vetting requirements.
7. Physical Controls	Secure facilities, HVA containment zones, and cloud enclave isolation.	Complies with CNSSI 1253 and DoD cloud boundary guidance.
8. Technological Controls	Encryption at rest/in transit, SIEM integration, secure APIs.	Enforces STIGs, SCAP, and classified/IL boundary enforcement.

A3. NIST SP 800-53 Rev. 5 / RMF Control Alignment (Optional but Recommended)

RMF Step / NIST Control Family	Cloud Architecture Alignment	Example Controls
1. Categorize System	Impact level assessments (IL2–IL6), mission impact modeling.	RA-1, PL-2
2. Select Controls	Tailored baselines for FedRAMP High / DISA SRG IL4/5.	AC-2, SC-12, IA-5
3. Implement Controls	IaC templates, DevSecOps for consistent enforcement.	CM-2, SI-2, AU-6
4. Assess Controls	Automated assessment scripts and CSP attestations.	CA-2, CA-7
5. Authorize System	Supports ATO and cATO processes with evidence packages.	AR-5, RA-5
6. Monitor Controls	Continuous monitoring (ConMon) via telemetry and dashboards.	IR-5, SC-38

A4. Integrated Defense Mission Assurance

Compliance Domain	Cloud Architecture Features	Mission Relevance
ISO 9001 + ISO 27001	Quality + security by design, change management, risk evaluation	Enhances trust in agile DevSecOps environments
ISO/NIST Crosswalk	Shared controls mapped to ensure interoperability (e.g., risk, audit, access)	Reduces duplication during DCSA/DISA audits
RMF Integration	Built-in compliance artifacts, control inheritance from CSPs	Accelerates ATO timelines and supports reciprocity across agencies

Conclusion

This compliance architecture enables defense programs to:

- **Accelerate ATO/cATO timelines**
- **Strengthen proposal credibility through standards adherence**
- **Simplify integration with RMF-based cybersecurity programs**
- **Support continuous compliance with evolving mandates like CMMC 2.0 and Zero Trust**

Full compliance documentation, mappings, and control evidence packages are available upon request to support specific RFP or accreditation needs.

Appendix C – Cost-Model Assumptions & Methodology

Category	Assumption	Rationale / Source
Scope & Horizon	5-yr NPV (FY 26-30)	Matches typical IDIQ base + 4 option years
Discount Rate	6 % real	OMB A-94 midpoint
Baseline ("As-Is")	• 50 prod VMs (8 vCPU/32 GB) • 22 staging VMs • 26 FTE sustainment (GS-13)	Current ISR sustainment TO (Jan 2025 PoP)
Cloud-Native ("To-Be")	• 20 K8s worker nodes + 3 control-plane • 16 FTE SRE sustainment	Mirrors 2023 classified pilot
IaaS Unit Cost	$ 0.051 / vCPU-hr (IL-5 region)	FY-25 GSA Cloud SIN
License Escalation	4 % CAGR proprietary vs. flat OSS	Gartner "Fed SW Price Index 2024"
Labor Rate	$ 168 k loaded / GS-13 FTE	FY-25 OPM GS + 37 % fringe
Automation Uptake	60 % Y1 → 85 % Y3	Pilot DevSecOps metrics

Category	Assumption	Rationale / Source
One-time Compliance Cost	$ 320 k container STIG + SBOM	DISA SRG audit averages
Inflation / Escalation	2.2 % labor, 2 % cloud infra	OSD CAPE 2025-30
Risk / Opportunity Reserve	$ 0.9 M (≈ 3 % PV)	Covers mitigations R-1 … R-7
Schedule Reserve	5 calendar days	Buffer for security hardening tasks
Exclusions (neutral)	On-prem depreciation, WAN backhaul	Equal in both scenarios

Sensitivity method: Independent ± 15 % swings on labor, cloud fees, and automation produce an IRR band **22 % – 39 %** (see Fig. 6 tornado chart).

Appendix E – References

U.S. Government Policy & Strategy Documents

1. **Executive Order 14028** – *Improving the Nation's Cybersecurity*
   The White House, 2021
   https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
2. **DoD Digital Modernization Strategy**
   U.S. Department of Defense, 2019
   https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY.PDF
3. **Joint All-Domain Command and Control (JADC2) Strategy**
   U.S. Department of Defense, 2022
   https://media.defense.gov/2022/Mar/17/2002958401/-1/-1/1/JADC2-STRATEGY.PDF
4. **Zero Trust Reference Architecture**
   DoD CIO & DISA, Version 2.0, 2023
   https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-Zero-Trust-Reference-Architecture-v2.0.pdf

5. **FedRAMP Authorization Act (Title IX of FY23 NDAA)**
U.S. Congress, 2023
https://www.congress.gov/bill/117th-congress/house-bill/7776

NIST Standards and Guidance

6. **NIST SP 800-53 Rev. 5** – *Security and Privacy Controls for Information Systems and Organizations*
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
7. **NIST SP 800-171 Rev. 2** – *Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems*
https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
8. **NIST SP 800-207** – *Zero Trust Architecture*
https://csrc.nist.gov/publications/detail/sp/800-207/final
9. **NIST SP 800-37 Rev. 2** – *Risk Management Framework for Information Systems and Organizations*
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
10. **NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF 2.0)**
https://www.nist.gov/cyberframework

DoD & DHS Acquisition and Compliance References

11. **Cybersecurity Maturity Model Certification (CMMC) 2.0 Overview**
U.S. Department of Defense, 2021
https://dodcio.defense.gov/CMMC/
12. **DoD Enterprise DevSecOps Reference Design**
DoD CIO & Platform One, 2021
https://software.af.mil/wp-content/uploads/2021/04/DevSecOps-Reference-Design-v2.1.pdf
13. **DHS Cloud Computing Strategy**
U.S. Department of Homeland Security, 2020
https://www.dhs.gov/sites/default/files/publications/cloud-strategy.pdf

Industry & Commercial White Papers

14. **AWS Cloud Strategy for Defense**
Amazon Web Services, 2022
https://aws.amazon.com/government-defense/

15. **Gartner – Innovation Insight for Cloud-Native Application Protection Platforms (CNAPP)**
Gartner Research, 2023
(Subscription required; useful for security and DevSecOps trends in cloud environments)