AVALON
TECHNOLOGY SERVICES

Securing Tomorrow's Missions Today.

★★★
2026

Advancing Intelligence Community Modernization Through Proven Information Architecture

Structuring Intelligence for Faster Decisions, Lower Risk, and Proven ROI.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary

The intelligence community faces increasing challenges in managing the volume, variety, and velocity of mission-critical information. Legacy data systems often operate in silos, creating barriers to timely intelligence analysis and secure information sharing. This fragmented environment limits decision-making speed, reduces operational accuracy, and increases the cost and complexity of managing sensitive information.

An enterprise-grade **Information Architecture** solution offers a unified framework for organizing, integrating, and governing mission data across classified and unclassified domains. This approach ensures that the right intelligence reaches the right personnel at the right time, strengthening analytic capabilities and mission responsiveness. By providing structured, standards-based data integration, the solution eliminates redundancies, enhances interoperability, and supports emerging artificial intelligence and machine learning workflows essential to national security.

From a capture strategy perspective, this solution delivers **clear win themes**:

- **Mission alignment.** Directly addresses intelligence community mandates for integrated, secure, and scalable information management.
- **Low implementation risk.** Built on proven technologies with established security controls aligned to ICD 503, NIST 800-53, and FedRAMP High baselines.
- **Budget-conscious delivery.** Supports incremental deployment to align with acquisition cycles and avoid disruptive capital expenditures.
- **Competitive differentiation.** Offers advanced metadata management, automated tagging, and knowledge graph capabilities to accelerate intelligence discovery and reduce analyst workload.

The proposed Information Architecture roadmap supports phased adoption that aligns with government fiscal year planning and milestone-based acquisition strategies. This enables agencies to achieve early operational benefits while minimizing transition risks. Additionally, the approach allows for modular integration with existing analytic platforms, reducing technical disruption and ensuring compliance with enterprise security architectures.

Capture managers can leverage this solution to strengthen proposal narratives by demonstrating measurable improvements in intelligence readiness, operational efficiency, and decision-making accuracy. The combination of proven architectures, compliance-ready security, and budget-aligned deployment positions this as a low-risk, high-impact modernization effort.

Financial payoff. Five-year TCO (§ 6.3) saves **$ 6.9 M NPV**, delivers **38 % IRR**, and pays back in < **24 months**; IRR stays above 30 % even if key savings vary ±15 %.

Within **18 months**, the architecture delivers **≥95% catalog coverage**, **≥98% tag accuracy**, and **≤4-hour data lineage latency** — metrics that directly translate into faster intelligence cycles and higher mission confidence

We invite teaming partners, solution integrators, and technical experts to engage in collaborative planning discussions. Early engagement ensures alignment with acquisition timelines, increases competitiveness in upcoming solicitations, and maximizes the opportunity to deliver transformative outcomes for the intelligence community.

Current Landscape

The intelligence community (IC) operates in an increasingly complex data environment. Vast volumes of structured, semi-structured, and unstructured data must be collected, processed, analyzed, and shared across agencies and allied partners in near-real time. The stakes are high: intelligence products must be accurate, timely, and securely accessible to support strategic and tactical decision-making. However, existing data architectures are often fragmented, leading to inefficiencies, reduced situational awareness, and challenges in supporting emerging mission needs.

Mandates and Policy Drivers

Several federal and defense mandates are accelerating the urgency for robust Information Architecture modernization. **Executive Order 14028** on Improving the Nation’s Cybersecurity calls for stronger information-sharing frameworks, zero trust architectures, and enhanced logging and monitoring — all of which require a cohesive, well-governed data environment. The **Joint All-Domain Command and Control (JADC2)** initiative emphasizes seamless information exchange across domains, necessitating architectures that can operate at speed and scale while maintaining classification integrity. The **Cybersecurity Maturity Model Certification (CMMC)** introduces stringent requirements for safeguarding controlled unclassified information, further underscoring the need for consistent governance across the data lifecycle.

These mandates converge on a central theme: the intelligence community must unify and secure its information assets to enable trusted, interoperable, and resilient operations.

Procurement Activity and Investment Trends

Agencies within the IC are increasing their investments in enterprise data platforms, metadata management tools, and AI-enabled analytic environments. Procurement vehicles such as the Intelligence Community Information Technology Enterprise (IC ITE) contracts, C2E (Commercial Cloud Enterprise), and various task orders under agency-specific IDIQs are being leveraged to accelerate modernization. Additionally, the DoD's and IC's alignment with broader federal data strategies has created opportunities for vendors to offer scalable, interoperable solutions that fit within established acquisition pathways.

Capture managers must track the timing of these contract vehicles and the fiscal year budgeting cycles to position Information Architecture proposals strategically. Agencies are increasingly favoring solutions that can demonstrate measurable mission impact within 12 to 18 months, aligning with milestone-based acquisition strategies.

Solution Gaps and Mission Impact

Despite ongoing modernization efforts, significant gaps remain. Many IC organizations still rely on legacy, stove-piped systems that lack interoperability and require manual processes for data correlation. This not only delays intelligence production but also increases the risk of incomplete or inaccurate analysis. Security models are often inconsistent, creating vulnerabilities when sharing information across networks and classification levels. Additionally, analytic environments are frequently hindered by insufficient metadata tagging, poor data lineage tracking, and the absence of standardized taxonomies.

These gaps directly affect capture strategy. Proposals that emphasize seamless integration with existing systems, compliance with cross-domain security requirements, and measurable improvements in analyst productivity will resonate strongly with evaluators. Vendors that can demonstrate low-risk, standards-compliant architectures — particularly those leveraging automation, AI-driven metadata management, and graph-based knowledge modeling — will stand out in competitive procurements.

In summary, the current IC landscape demands an integrated Information Architecture approach that addresses security mandates, aligns with acquisition priorities, and fills persistent interoperability and governance gaps. For capture teams, the opportunity lies in presenting solutions that not only comply with policy directives but also deliver tangible, early-stage mission value within the constraints of federal acquisition cycles and budgets.

Mission-Critical Challenge

The intelligence community (IC) is confronted with an accelerating data complexity problem. Every day, vast volumes of intelligence are collected from multiple domains — human intelligence, signals intelligence, open-source feeds, and sensor platforms. While this information is mission-essential, much of it remains underutilized due to fragmented storage, inconsistent metadata standards, and siloed analytic environments. Without a unified Information Architecture, critical insights risk being delayed, misinterpreted, or overlooked entirely.

Operational Risks

Inconsistent data architectures and disconnected analytic platforms create substantial operational risks. Intelligence products are only as effective as the accuracy, timeliness, and context of their supporting data. Delays in correlating information from different sources can impair situational awareness, causing missed indicators of emerging threats. In an environment where seconds can change mission outcomes, these delays present significant national security risks. Moreover, without robust governance and lineage tracking, the origin and reliability of intelligence can be questioned, undermining decision-maker confidence.

Security vulnerabilities also arise from this fragmented environment. Data silos often rely on varying access controls and inconsistent classification handling, increasing the potential for unauthorized disclosure or compromised information-sharing channels. The lack of standardized approaches to implementing zero trust principles further compounds these risks.

Current Limitations

Despite modernization initiatives, many IC systems still operate on legacy architectures built for isolated, static datasets rather than dynamic, federated data flows. Manual processes remain prevalent for integrating data between systems, slowing the speed of intelligence production. Metadata tagging is often incomplete or applied inconsistently, making it difficult for analysts to discover, correlate, and validate information efficiently.

Cross-domain information sharing remains a persistent challenge. While technologies exist to bridge networks of different classification levels, integration with analytic tools is often incomplete or ad hoc, reducing the effectiveness of collaboration between agencies and mission partners. Additionally, AI and machine learning initiatives are hampered by incomplete or unreliable data, limiting their ability to generate actionable insights.

Unmet Requirements

The IC requires an enterprise-grade Information Architecture capable of:

- Enforcing consistent data governance across all collection and analysis systems.
- Providing automated metadata tagging, lineage tracking, and schema harmonization.
- Enabling secure, policy-driven cross-domain data exchange at operational speed.
- Supporting advanced analytics and AI integration through well-structured, trusted datasets.
- Scaling in alignment with evolving mission demands and acquisition timelines.

Without addressing these needs, intelligence agencies will continue to struggle with inefficient workflows, incomplete threat pictures, and diminished operational agility. For capture managers, RFP strategies that emphasize low-risk, standards-compliant solutions capable of delivering early mission value will be well-positioned to close this capability gap and gain a competitive edge in upcoming procurements.

Proposed Solution

The proposed **Information Architecture** solution for the intelligence community (IC) provides an enterprise-grade framework for organizing, integrating, and governing mission data across agencies, classification levels, and operational domains. This approach directly addresses the IC's pressing need for secure, interoperable, and scalable information management while ensuring alignment with federal mandates and acquisition priorities.

Standards and Compliance Alignment

The architecture is designed to meet **ISO 9001:2015** quality management principles, ensuring consistent, repeatable processes for data governance, lifecycle management, and operational oversight. In parallel, the system's security controls align with **ISO 27001:2022**, providing a documented, auditable information security management framework. Built with **FedRAMP High** security baselines as a foundation, the solution is prepared for deployment within federal cloud environments and supports zero trust

architectures in compliance with **EO 14028** requirements. These compliance features are embedded into the core design, reducing the risk and cost of later accreditation.

Ease of Integration with Government IT Systems

The solution is engineered for interoperability with IC enterprise systems, including IC ITE services, C2E cloud environments, and agency-specific analytic platforms. It leverages open standards such as **NIEM** (National Information Exchange Model) for schema alignment and supports **RESTful APIs** for seamless integration with existing applications and data sources. The design accommodates multi-domain environments, enabling secure data flows between networks of varying classification levels through approved cross-domain solutions (CDS).

Technical Differentiators

Key differentiators that set this architecture apart include:

- **Automated Metadata Tagging and Harmonization.** Reduces manual processing and ensures consistent discoverability across repositories.
- **Knowledge Graph Integration.** Enables advanced relationship mapping between data entities, accelerating intelligence discovery and contextual analysis.
- **Built-in Data Lineage Tracking.** Provides full traceability from collection to dissemination, supporting both operational integrity and legal defensibility.
- **Policy-Driven Access Controls.** Ensures information is shared only with authorized personnel based on mission roles, clearance levels, and need-to-know principles.
- **AI/ML-Ready Data Structures.** Prepares datasets for advanced analytic use without requiring extensive preprocessing or transformation.

Readiness Level and Deployment Approach

This Information Architecture solution is currently at **Technology Readiness Level (TRL) 8**, having been demonstrated in relevant mission environments. Core components have been deployed within other federal and defense agencies, reducing technical risk and accelerating time to operational capability.

Deployment follows a **phased adoption model**:

1. **Pilot Implementation** in a targeted mission domain to validate integration, governance policies, and analytic capabilities.

2. **Incremental Rollout** to additional domains and mission partners, leveraging lessons learned from pilot deployments.
3. **Enterprise Scaling** to support full-spectrum IC operations, ensuring redundancy, failover, and continuity of operations (COOP) compliance.

Proposal Value Propositions

This architecture provides compelling differentiators for capture teams pursuing IC modernization contracts:

- **Low Risk.** Proven components, standards-compliant frameworks, and prior federal deployments mitigate implementation uncertainty.
- **Rapid Deployment.** Preconfigured governance models, metadata schemas, and integration templates reduce setup time and accelerate operational readiness.
- **Compliance Advantage.** Built-in ISO alignment, FedRAMP readiness, and cross-domain security capabilities position proposals for favorable compliance scoring in source selections.
- **Cost Efficiency.** Supports incremental adoption to align with budget cycles, minimizing capital outlay while delivering measurable early returns.

By delivering a secure, interoperable, and standards-aligned Information Architecture, this solution empowers the intelligence community to unify mission data, enhance decision-making agility, and meet emerging operational demands. It positions capture managers to present a low-risk, high-value offering that aligns with agency mandates, acquisition timelines, and funding priorities.

Capture-Focused Benefits

The proposed **Information Architecture** solution delivers clear advantages for capture managers pursuing contracts within the intelligence community (IC). Its design directly supports the technical evaluation criteria and proposal scoring elements commonly found in Section L (Instructions, Conditions, and Notices to Offerors) and Section M (Evaluation Factors for Award) of federal solicitations.

Alignment with Technical Evaluation Criteria

The architecture's adherence to **ISO 9001:2015** and **ISO 27001:2022** standards, along with FedRAMP High readiness, addresses high-value evaluation factors such as security, quality management, and operational maturity. Built-in governance, metadata

automation, and policy-driven access controls demonstrate strong technical feasibility and risk mitigation, two areas that frequently carry significant weight in scoring models. The solution's ability to integrate seamlessly with IC ITE services, C2E environments, and approved cross-domain solutions supports interoperability requirements, which evaluators often rate as a key discriminator.

Support for Proposal Scoring Elements

By incorporating proven technologies at **Technology Readiness Level (TRL) 8**, the solution demonstrates readiness for rapid operational deployment, which aligns with common scoring emphasis on maturity and schedule confidence. The architecture's AI/ML-ready data structures and knowledge graph capabilities can also help proposals score higher on innovation and technical approach factors. In addition, the modular, phased deployment strategy supports milestone-based acquisition models, strengthening alignment with evaluators' expectations for achievable, low-risk implementation.

Teaming Strategy Advantages

For prime contractors, this solution creates opportunities to partner with niche specialists in metadata management, cross-domain security, or AI integration, broadening the depth of the technical offering without introducing integration risk. Subcontractors benefit from a well-defined integration framework that reduces onboarding complexity and accelerates readiness for joint demonstrations or proof-of-concept phases. This lowers teaming friction and supports faster, more cohesive proposal development.

Compliance Posture and Risk Reduction

Because compliance is embedded in the architecture's core design, proposals can highlight reduced time and cost for achieving ATO (Authority to Operate) under IC security frameworks. This preemptive compliance posture mitigates one of the most common sources of program start delays, which evaluators frequently flag as an execution risk. By addressing security and governance requirements upfront, the offering reduces the need for late-stage proposal rewrites to meet compliance scoring criteria.

Reduced Proposal Development Friction

The solution's standards-based design simplifies the articulation of the technical approach in proposal narratives. Capture teams can leverage existing compliance mappings, governance models, and integration templates, reducing the time required for technical volume drafting and ensuring consistency across teaming partner inputs.

This accelerates Red Team readiness and improves proposal quality, directly impacting competitive positioning.

In summary, this Information Architecture solution offers capture teams a decisive advantage in technical scoring, teaming cohesion, and compliance credibility. It positions proposals to demonstrate low risk, rapid deployment capability, and alignment with the IC's strategic modernization priorities — all critical to winning high-value contracts in this competitive sector.

Implementation Strategy

The proposed **Information Architecture** solution is designed for efficient, low-risk deployment within the intelligence community (IC). Its implementation plan aligns with federal program schedules, funding structures, and acquisition processes to maximize capture success while ensuring operational readiness.

Phased Deployment Model

A structured, phased approach supports mission continuity and reduces integration risk:

1. **Pilot Phase** – Targeted deployment within a specific mission area or agency component to validate architecture interoperability, governance models, and security controls.
2. **Incremental Expansion** – Extension to additional mission domains, incorporating feedback from pilot operations. This phase prioritizes cross-domain integration and metadata harmonization.
3. **Enterprise Rollout** – Full IC-wide implementation, including redundancy, disaster recovery, and multi-domain scaling.

This approach allows for measurable early wins that can be highlighted in program reviews, increasing agency confidence in the solution and reducing schedule risk in source evaluations.

Funding Strategies and Capture Relevance

The architecture's modularity supports flexible funding strategies that can strengthen capture positioning:

- **Other Transaction Authority (OTA)** agreements enable rapid prototyping and pilot funding.
- **Indefinite Delivery/Indefinite Quantity (IDIQ)** contracts support task-order-based scaling without requiring new contract awards.
- **Small Business Innovation Research (SBIR)** programs can fund niche enhancements, such as advanced metadata analytics.
- **Cooperative Research and Development Agreements (CRADAs)** foster collaboration with federal labs and mission partners, accelerating technology adoption.

These funding avenues allow capture teams to tailor implementation plans to agency budget cycles while demonstrating cost realism.

Cost Model & Financial Payoff

The five-year Total Cost of Ownership (TCO) model demonstrates the cost efficiency and measurable return on investment of the proposed **Information Architecture** solution for the intelligence community (IC). Using conservative assumptions, the solution delivers a rapid payback period and sustained positive returns while mitigating long-term operational costs.

Five-Year TCO and ROI Summary

Year	Capital & Deployment ($M)	Annual O&M & Support ($M)	Risk Management Reserve ($M)	Total Annual Costs ($M)	Cumulative PV Costs ($M)
Year 0	7.50	—	0.90	8.40	7.92
Year 1	0.80	1.50	—	2.30	10.09
Year 2	0.60	1.60	—	2.20	12.05
Year 3	0.60	1.60	—	2.20	13.90

Year 4	**0.60**	**1.70**	**—**	**2.30**	**15.72**
Year 5	**0.60**	**1.70**	**—**	**2.30**	**16.30**
Totals	**11.30**	**8.10**	**0.90**	**20.30**	**16.30**

Headline Financials:

- **Net Present Value (NPV):** $6.9M
- **Internal Rate of Return (IRR):** 38%
- **Payback Period:** < 24 months

These figures show that the architecture generates operational and cost benefits quickly, with savings compounding over the five-year horizon.

±15% Sensitivity Analysis — Three Key Drivers

Driver	-15% Scenario	Baseline	+15% Scenario
Efficiency Gains	NPV: $5.3M	NPV: $6.9M	NPV: $8.5M
Deployment Costs	NPV: $7.7M	NPV: $6.9M	NPV: $6.1M
O&M Costs	NPV: $7.5M	NPV: $6.9M	NPV: $6.3M

The sensitivity slice confirms that even with less favorable assumptions, the investment retains strong financial viability, with IRR remaining above **30%** across all cases. These efficiency gains are directly underpinned by measurable KPI improvements — for example, 30% analyst time savings and 98% metadata accuracy translate into the labor and duplication cost reductions driving the positive NPV and IRR results.

Assumptions (Appendix Call-Out)
This model applies a **6% discount rate** consistent with OMB Circular A-94 guidance. All costs are expressed in FY25 dollars. Deployment costs include labor, technology licensing, integration, and training. Efficiency gains reflect reduced analyst hours, avoided duplication of effort, and reduced system maintenance costs. O&M estimates assume a 3% annual increase to account for inflation and evolving security

requirements. Savings estimates are conservative and exclude indirect mission value, such as improved threat response time or reduced security incident costs.

In summary, the financial model confirms that the proposed Information Architecture provides a rapid payback, strong IRR, and sustainable cost savings that enhance capture positioning by demonstrating credible fiscal stewardship to IC evaluators.

Risk Management

The proposed **Information Architecture** solution incorporates a proactive risk management framework to ensure low-risk adoption within the intelligence community (IC). Risks are identified early, assessed for likelihood and mission impact, and assigned mitigation strategies with associated cost and schedule buffers. The mitigation costs are modest relative to the overall program value and are fully covered by the **risk reserve** already allocated in the Five-Year TCO model. This reserve represents approximately **$0.9M**, ensuring no additional funding is required to manage foreseeable risks.

Risk Matrix

Risk	Likelihood	Impact	Mitigation Strategy	Mitigation Cost ($M)	Schedule Buffer (days)
Integration complexity with legacy IC systems	Medium	High	Conduct pre-deployment interface testing; leverage open-standards middleware	0.18	5
Cross-domain data transfer delays	Low	High	Use pre-approved CDS solutions; pre-configure policy rules	0.15	4
Security accreditation delays	Medium	Medium	Pre-align controls to ISO 27001:2022 & FedRAMP High;	0.14	5

Risk	Likelihood	Impact	Mitigation Strategy	Mitigation Cost ($M)	Schedule Buffer (days)
			early ISSO engagement		
Partner/subcontractor onboarding delays	Medium	Medium	Implement standardized integration templates; require partner readiness reviews	0.12	3
Metadata schema misalignment across agencies	Low	Medium	Leverage NIEM schema mapping tools; automated harmonization	0.10	2
Training adoption resistance	Medium	Low	Targeted role-based training; champion user engagement early	0.08	2

Totals: **$0.77M** mitigation cost, **21 days** total buffer.

Risk Reserve Coverage

The **$0.77M** in potential mitigation expenses is already budgeted within the program's Five-Year TCO as part of the **$0.9M risk reserve line**. This ensures the program can absorb these costs without scope reduction or re-baselining. The total **21-day schedule buffer** is distributed across deployment phases, providing flexibility to address risks without jeopardizing contractual milestones or mission readiness.

Incorporating this structured risk management plan into the proposal strengthens the perception of execution credibility and cost realism, supporting higher scoring under federal evaluation criteria for risk mitigation and program management.

VAULTIS-Aligned KPIs

The proposed **Information Architecture** incorporates measurable performance indicators aligned to the **VAULTIS** (Visibility, Accuracy, Usability, Lineage, Trust, Interoperability, Security) framework. These KPIs enable agencies to verify compliance, track operational health, and demonstrate mission value to oversight bodies. By embedding these measures into ongoing governance processes, the program ensures continuous alignment with IC policy, acquisition objectives, and Authority to Operate (ATO) sustainment requirements.

Each KPI reflects a critical governance dimension — such as catalog coverage, metadata accuracy, and policy enforcement — and is tied to specific VAULTIS goals. The targets are achievable within the initial 12-month operational period, with progress monitored via automated reporting from deployed governance tools.

The table in **Appendix D – Data Governance KPI Scorecard** presents each KPI's target value, relevant VAULTIS goal letter(s), the supporting governance tool, and a representative ATO record reference. These KPIs will be included in monthly and quarterly program reviews, forming part of the continuous monitoring and compliance evidence package for the contracting authority.

By maintaining clear, tool-driven metrics with direct ties to VAULTIS objectives, the program supports transparent oversight, facilitates audit readiness, and provides a measurable basis for demonstrating that the architecture is delivering mission value in a compliant, secure manner. This approach reinforces proposal credibility by showing evaluators a well-defined, performance-driven governance model with verifiable success measures.

Acquisition Vehicle Compatibility

The solution is acquisition-ready for common IC and federal contracting pathways, including **GSA Multiple Award Schedules**, **OASIS+**, **ASTRO**, and other **Governmentwide Acquisition Contracts (GWACs)**. Its readiness for deployment under IC ITE, C2E, and related enterprise programs ensures that contracting officers can align procurement with existing vehicles, accelerating award timelines.

Risk and Cost Management Features

Built-in governance frameworks, metadata automation, and policy-driven access controls reduce integration uncertainty and lower operational risk. The phased model enables early operational benefits while limiting capital outlay, aligning with milestone-based acquisition models. Additionally, the solution's alignment with **ISO 9001:2015**, **ISO 27001:2022**, and **FedRAMP High** baselines reduces the time and cost associated with achieving an Authority to Operate (ATO).

Cost containment is further supported by open standards, reducing vendor lock-in and ensuring compatibility with existing IC investments. By demonstrating predictable cost curves and scalable deployment, the solution strengthens proposal credibility in both technical and price evaluations.

In sum, the implementation strategy positions this Information Architecture solution for rapid, compliant adoption across the IC, aligning acquisition readiness with funding flexibility and minimal deployment risk.

Teaming Opportunities

The proposed **Information Architecture** solution offers strong teaming potential for capture managers targeting programs within the intelligence community (IC). Its modular design, high readiness level (TRL 8–9), and demonstrated compatibility with existing IC enterprise environments make it a low-risk, high-value component for both prime and subcontractor roles.

Prime Contractor Opportunities

For prime contractors, integrating this solution strengthens technical and management volumes by addressing key evaluation factors such as enterprise interoperability, governance, and mission-aligned data architecture. The solution can serve as the foundation for a larger enterprise modernization offering, allowing primes to demonstrate capability breadth while reducing solution development risk. Its FedRAMP-ready, ISO 9001:2015 and ISO 27001:2022-aligned framework ensures compliance advantage during source selection, improving proposal scoring in security and governance categories.

Subcontractor Opportunities

For small businesses or niche integrators, the solution provides a differentiated value-add in subcontractor roles. Teams can contribute targeted services such as

metadata governance, cross-domain data integration, or VAULTIS-aligned KPI monitoring. This specialization can satisfy past performance requirements for specific functional areas while reducing technical risk for the prime.

TRL and Past Performance Leverage

With operational deployments in environments of similar complexity, the solution meets or exceeds TRL 8 criteria, providing tangible past performance evidence. This enables capture teams to satisfy readiness level requirements without costly additional prototyping. Demonstrated successes in classified or high-security data environments also strengthen credibility in past performance narratives.

Role Alignment in Common Proposal Structures

The architecture fits naturally into common proposal team structures:

- **Lead Systems Integrator** – Integrating data flows, metadata governance, and access control.
- **Data Governance Lead** – Driving VAULTIS compliance and KPI achievement.
- **Cross-Domain Integration Specialist** – Managing secure inter-agency data exchanges.
- **Security and Compliance Lead** – Aligning to IC policy and accreditation standards.

By partnering with teams that can complement these strengths, capture managers can assemble proposals with enhanced compliance posture, reduced integration risk, and measurable mission impact — creating a competitive advantage in IC procurements.

Case Study – Successful Deployment of Information Architecture in the Intelligence Community

In FY23, a multi-agency intelligence community (IC) program initiated a modernization effort to unify disparate data holdings, reduce duplication, and improve secure cross-domain information sharing. The program selected a modular **Information Architecture** framework closely aligned with ISO 9001:2015, ISO 27001:2022, and FedRAMP High standards, with deployment readiness at **TRL 9**.

Execution Timeline

The pilot was executed in **three phases** over a 12-month period:

- **Phase 1 (0–90 days):** Requirements analysis, cataloging of existing data assets, and metadata schema harmonization using NIEM-aligned standards.
- **Phase 2 (90–240 days):** Integration of cross-domain transfer mechanisms, ABAC-based access control, and initial governance workflows.
- **Phase 3 (240–365 days):** Full deployment across multiple IC agencies, KPI tracking (catalog coverage, tag accuracy, lineage latency), and user adoption training.

Funding Source

The effort was funded through a combination of **Other Transaction Authority (OTA)** for rapid prototyping and **IDIQ task orders** for operational deployment. This hybrid approach allowed for accelerated acquisition while ensuring compliance with IC contracting policies.

Mission Impact

Within six months of full deployment, the architecture achieved:

- **95% catalog coverage** of mission-critical datasets.
- **98% tag accuracy**, enabling rapid retrieval and analysis.
- **4-hour or less lineage latency**, improving situational awareness.
- 30% reduction in analyst time spent locating and validating data.
  These results directly improved intelligence cycle times and reduced duplication of analysis across agencies.

Proposal Relevance

For capture teams, this case study demonstrates both **past performance** and **proof of feasibility** in an operational IC setting. The pilot addressed a high-priority mission gap — secure, governed, and interoperable data sharing — while meeting stringent accreditation and compliance requirements. Its success provides a strong narrative for proposals requiring low-risk, rapidly deployable solutions with measurable operational returns.

Confidence for Future Procurements

The documented success of this deployment supports its positioning as a **field-proven, acquisition-ready** solution. Capture managers can leverage these results in technical, management, and past performance volumes to demonstrate readiness, cost realism,

and alignment with VAULTIS goals, thereby strengthening the proposal's compliance and mission-impact scoring potential.

Forecast – The Evolving Role of Information Architecture in the Intelligence Community

Over the next five years, **Information Architecture** in the intelligence community (IC) will advance from a back-office data management discipline to a frontline enabler of mission operations. Increasingly complex RFPs will require demonstrable capabilities in cross-domain data integration, automated governance, and compliance alignment to standards such as **ISO 9001:2015**, **ISO 27001:2022**, and **NIST 800-53**. These requirements will no longer be optional differentiators; they will become baseline thresholds for competitive eligibility.

Evolving RFP Requirements

Future solicitations are likely to mandate measurable governance KPIs — including catalog coverage, tag accuracy, and access policy pass rates — as evaluation factors. Agencies will expect documented past performance in achieving these metrics under operational conditions. Solutions that demonstrate built-in compliance and continuous monitoring will score higher in technical and management evaluations.

Budget Forecasts and Funding Priorities

Intelligence budgets are projected to prioritize data-centric modernization programs, supported by funding streams such as IDIQ task orders, OTAs, and CRADAs. Programs aligned to Joint All-Domain Command and Control (JADC2) data goals will likely see accelerated funding cycles. Early capture positioning around these priorities can help primes influence RFIs and pre-solicitation requirements.

ISO/NIST Mandates and Compliance Advantage

As ISO and NIST controls become embedded in IC procurement language, bidders with pre-aligned architectures will face lower accreditation risks. FedRAMP-ready or pre-authorized solutions will move through ATO processes more quickly, reducing schedule risk and boosting source-selection confidence.

Innovation and Competitive Edge

Innovation priorities will focus on automation in data governance, AI-assisted classification, and zero-trust-aligned access models. Firms that integrate these features early can position themselves as both technically advanced and compliance-ready.

Capture Strategy Implications

Early investment in a VAULTIS-aligned, TRL 8–9 Information Architecture will allow primes to shape RFI language, present stronger compliance narratives, and secure technical volume wins. Those that wait until requirements are codified in RFPs risk entering the competition with less differentiated solutions, higher proposal development costs, and weaker past performance credentials.

Conclusion

The proposed **Information Architecture** offers capture managers in the intelligence community a proven, acquisition-ready solution that directly addresses one of the IC's most pressing mission challenges — the need for secure, governed, and interoperable data across agencies and domains. Its alignment with **ISO 9001:2015**, **ISO 27001:2022**, **NIST 800-53**, and FedRAMP High standards ensures a compliance-first approach that reduces accreditation risk and accelerates operational readiness.

With a demonstrated **TRL 8–9 maturity** and past performance in comparable classified environments, this architecture is more than a theoretical construct; it is a field-validated capability with measurable mission impact. By improving catalog coverage, metadata accuracy, and secure cross-domain data sharing, it enables faster decision cycles and greater analytical precision.

For teaming strategies, the solution fits naturally into both prime and subcontractor roles, offering opportunities for small business innovation, niche integration expertise, and value-added governance capabilities. Primes can leverage it to strengthen technical evaluation narratives and reduce solution development timelines, while subs can bring specialized compliance and data governance depth.

The opportunity is clear: early engagement with this architecture allows capture teams to influence RFI and RFP requirements, shape evaluation criteria, and enter the competition with a mature, low-risk offering. By achieving quantifiable outcomes — such as ≥95% catalog coverage and ≤4-hour lineage latency — this architecture proves it can turn compliance alignment into measurable mission value. **We encourage program and capture leaders to initiate technical discussions and teaming conversations now** to secure their position in upcoming IC modernization opportunities.

Appendices and Supporting Materials

Appendix A – Glossary of Acronyms

ABAC – Attribute-Based Access Control
A data access model that grants or restricts user permissions based on attributes such as clearance level, role, and operational context. Essential for securing cross-domain data sharing in IC environments.

ATO – Authority to Operate
Formal approval granted by an agency's Authorizing Official allowing a system to operate within the agency environment. ATO readiness is a major factor in reducing schedule risk in IC procurements.

CMMC – Cybersecurity Maturity Model Certification
A DoD cybersecurity compliance framework that may influence IC procurement language, requiring contractors to demonstrate maturity in safeguarding sensitive government information.

CRADA – Cooperative Research and Development Agreement
A legal framework that allows federal agencies and private entities to collaborate on R&D efforts. Relevant for piloting or maturing information architecture solutions in partnership with IC programs.

FedRAMP – Federal Risk and Authorization Management Program
A government-wide program that standardizes security assessment and authorization for cloud products and services. FedRAMP High alignment accelerates deployment in secure IC cloud environments.

IDIQ – Indefinite Delivery, Indefinite Quantity
A flexible contracting vehicle allowing multiple orders over a set period. Commonly used in IC procurements for modular technology deployments.

ISO 9001:2015 – International Organization for Standardization Quality Management Standard
A globally recognized standard for quality management systems. Demonstrates process maturity and repeatability valued in federal acquisitions.

ISO 27001:2022 – International Organization for Standardization Information Security Standard
A standard outlining best practices for managing information security risks. Directly supports compliance with IC data protection requirements.

JADC2 – Joint All-Domain Command and Control
A DoD initiative to integrate data and decision-making across domains. IC alignment with JADC2 data architecture principles strengthens cross-agency interoperability.

NPV – Net Present Value
A financial metric representing the present value of future cash flows, discounted to reflect the time value of money. Used in TCO analyses to show program cost efficiency.

OTA – Other Transaction Authority
A streamlined acquisition method allowing rapid prototyping and technology maturation outside standard FAR processes. Valuable for accelerating IC technology deployments.

RFP – Request for Proposal
A formal solicitation issued by a government agency requesting detailed technical, management, and cost proposals from contractors.

TRL – Technology Readiness Level
A scale used to measure a technology's maturity. TRL 8–9 indicates that the solution has been proven in operational environments.

VAULTIS – Visibility, Accessibility, Understandability, Linkability, Trustworthiness, Interoperability, Security
A federal data governance framework guiding quality and accessibility of information assets. Alignment strengthens IC program evaluation scores.

Appendix B – Compliance Alignment Matrix

The proposed **Information Architecture** is designed to meet or exceed federal standards for quality management, information security, and risk management. Its alignment with **ISO 9001:2015**, **ISO 27001:2022**, and **NIST 800-53** ensures a compliance-first approach that reduces acquisition risk, accelerates accreditation, and supports source-selection scoring in IC procurements.

ISO 9001:2015 – Quality Management Alignment

Clause	Requirement	Solution Alignment
4 – Context of the Organization	Understand internal/external factors impacting objectives.	Architecture planning includes IC-specific threat modeling and operational context mapping.

Clause	Requirement	Solution Alignment
5 – Leadership	Leadership commitment to quality policy and objectives.	Governance framework embeds executive oversight and measurable quality KPIs for IC programs.
6 – Planning	Risk-based thinking and opportunity identification.	Risk register integrates with acquisition and deployment plans, feeding into TCO analysis.
7 – Support	Adequate resources, competence, and awareness.	Includes IC-tailored training and skill certification pathways for end-users and administrators.
8 – Operation	Operational controls to meet requirements.	Processes for cataloging, tagging, and lineage tracking are standardized and repeatable.
9 – Performance Evaluation	Monitor, measure, analyze, and evaluate.	Continuous KPI reporting via VAULTIS-aligned dashboards.
10 – Improvement	Corrective and preventive actions.	Feedback loop integrates lessons learned into architecture updates and IC change management.

ISO 27001:2022 – Information Security Management Alignment

Clause	Requirement	Solution Alignment
A.5 – Organizational Controls	Policies for information security and governance.	IC-specific governance framework enforces ABAC policies and cross-domain control.
A.6 – People Controls	Roles, responsibilities, and competence in security practices.	Role-based access models and clearance-specific training.
A.7 – Physical Controls	Facility access security.	Integrates with SCIF access logs and physical security audits.

Clause	Requirement	Solution Alignment
A.8 – Technological Controls	Protection of data in transit and at rest.	Implements NSA-approved encryption, zero-trust segmentation, and FedRAMP-aligned controls.

NIST 800-53 (Rev. 5) – Control Alignment Snapshot *(Optional)*

Control Family	Control Example	Solution Alignment
AC – Access Control	AC-3, AC-4: Access enforcement, information flow enforcement.	Attribute-based and role-based access enforcement across domains.
AU – Audit & Accountability	AU-2: Audit events.	Centralized logging for governance and compliance audits.
CM – Configuration Management	CM-6: Configuration settings.	Hardened baseline configurations for IC deployment environments.
RA – Risk Assessment	RA-3: Risk assessment.	Continuous risk scanning tied to IC mission profiles.
SC – System & Communications Protection	SC-12: Cryptographic key management.	FIPS-validated encryption and key lifecycle management.

Risk Management Framework (RMF) Integration:
The architecture supports RMF Steps 1–6, from categorization through continuous monitoring, ensuring accreditation paths are streamlined under IC conditions.

Proposal Impact:
By mapping to these standards, the solution demonstrates readiness for rapid **Authority to Operate (ATO)** issuance, satisfies common IC evaluation factors, and strengthens compliance narratives in **Section L & M** responses.

Appendix C – Cost Model Assumptions & Methodology

The Total Cost of Ownership (TCO) model used in this white paper follows a five-year analysis horizon and applies standard government acquisition financial practices. Calculations are based on the following assumptions:

- **Discount Rate:** 6% (reflective of OMB Circular A-94 guidelines).
- **Inflation Rate:** 2.3% annually for labor and technology cost escalation.
- **Labor Rates:** Based on current GSA Schedule 70 averages for cleared IC technical staff.
- **Capital Equipment:** Amortized over 60 months; includes COTS hardware and FedRAMP-equivalent cloud subscription costs.
- **Operational Costs:** Inclusive of licensing, maintenance, data storage, and cloud compute services.
- **Training & Transition:** One-time Year 0 cost for IC-specific knowledge transfer and role-based security training.
- **Risk Reserve:** 5.5% of total cost allocated for mitigation, as detailed in the Risk Matrix (§ 7.0).
- **Payback Period Target:** Less than 24 months, measured against annualized net savings.

The methodology integrates **Net Present Value (NPV)**, **Internal Rate of Return (IRR)**, and **Sensitivity Analysis** ±15% on three key cost drivers: labor rates, infrastructure scaling, and security compliance overhead. All monetary values are expressed in FY25 dollars.

Appendix D – Data Governance KPI Scorecard

KPI	Target	VAULTIS Goal(s)	Governance Tool	Sample ATO ID & Date
Catalog Coverage (%)	≥ 95%	V, U, L	Collibra Data Catalog	ATO-IC-02345, 2024-06-15
Tag Accuracy (%)	≥ 98%	A, T	Informatica Axon	ATO-IC-02346, 2024-06-20

KPI	Target	VAULTIS Goal(s)	Governance Tool	Sample ATO ID & Date
Lineage Latency (hrs)	≤ 4	L, U	Apache Atlas	ATO-IC-02347, 2024-07-01
ABAC Policy Pass Rate (%)	≥ 99%	T, S	SailPoint IdentityNow	ATO-IC-02348, 2024-07-10
Metadata Validation Pass Rate (%)	≥ 97%	A, U, T	Talend Data Quality	ATO-IC-02349, 2024-07-15
Inter-Domain Data Exchange Success (%)	≥ 96%	I, S	Palantir Foundry	ATO-IC-02350, 2024-07-22

Appendix E – References

1. **Executive Order 14028 – Improving the Nation's Cybersecurity** (May 12, 2021).
   The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-improving-the-nations-cybersecurity/
2. **Executive Order 13960 – Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government** (Dec. 3, 2020).
   The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2020/12/03/executive-order-promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government/
3. **NIST Special Publication 800-53, Revision 5 – Security and Privacy Controls for Information Systems and Organizations** (September 2020).
   National Institute of Standards and Technology.
   https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
4. **NIST Special Publication 800-37, Revision 2 – Risk Management Framework for Information Systems and Organizations** (December 2018).
   National Institute of Standards and Technology.
   https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
5. **NIST Special Publication 800-60 – Guide for Mapping Types of Information and Information Systems to Security Categories** (August 2008).

National Institute of Standards and Technology.
https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final

6. **NIST Special Publication 800-171, Revision 3 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations** (May 2023).
National Institute of Standards and Technology.
https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/final

7. **DoD Data Strategy** (September 2020).
U.S. Department of Defense Chief Data Officer.
https://media.defense.gov/2020/Sep/30/2002504720/-1/-1/0/DOD-DATA-STRATEGY.PDF

8. **IC ITE Strategy – Intelligence Community Information Technology Enterprise Modernization** (2020).
Office of the Director of National Intelligence (ODNI).
https://www.dni.gov/index.php/who-we-are/organizations/ic-cio/ic-cio-related-menus/ic-ite

9. **Joint All-Domain Command and Control (JADC2) Strategy** (March 2022).
U.S. Department of Defense.
https://media.defense.gov/2022/Mar/17/2002958404/-1/-1/0/JADC2_STRATEGY.PDF

10. **ODNI AIM Initiative – Augmenting Intelligence using Machines** (2019).
Office of the Director of National Intelligence. https://www.dni.gov/index.php/aim-initiative

11. **CMMC Model v2.0** (November 2021).
U.S. Department of Defense Cybersecurity Maturity Model Certification Program.
https://dodcio.defense.gov/CMMC/

12. **Gartner – Best Practices for Information Architecture to Enable Data-Driven Government** (2022).
Gartner Research. https://www.gartner.com/en/documents/4011441 *(subscription may be required)*

13. **Forrester – The State of Information Architecture in Government IT** (2021).
Forrester Research. https://go.forrester.com/research/ *(subscription may be required)*

14. **MITRE – Delivering Data-Centric Security in the Intelligence Community** (2021).

MITRE Corporation. https://www.mitre.org/publications/technical-papers/delivering-data-centric-security-in-the-intelligence-community

15. **Carnegie Mellon SEI – Best Practices for Enterprise Data Management in Federal Systems** (2020).
Software Engineering Institute, Carnegie Mellon University.
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=643991