AVALON
TECHNOLOGY SERVICES

Securing Tomorrow's Missions Today.

★★★
2026

From Pilot to Production: Field-Tested SaaS-IaaS Strategies for IC Proposal Advantage

Accelerating Trusted Cloud Solutions for High-Stakes Intelligence Operations

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary

Enabling Mission Agility Through Secure SaaS-IaaS Implementation in the Intelligence Community

As intelligence missions evolve in complexity and pace, the demand for scalable, secure, and mission-ready digital infrastructure has become critical. This white paper presents a low-risk, high-impact approach to SaaS-IaaS implementation that directly addresses a high-priority gap in government modernization efforts: the ability to rapidly deploy and sustain cloud-native services that align with security mandates, cost ceilings, and evolving intelligence priorities.

The solution framework integrates commercially proven SaaS platforms with tailored IaaS environments that are fully compliant with ICD 503, NIST 800-53, and DoD RMF baselines. By abstracting infrastructure complexity while maintaining control over security zones and data flows, this approach empowers mission owners to accelerate capability delivery, reduce sustainment overhead, and maintain operational advantage in contested domains. It is optimized for secure enclaves, air-gapped environments, and hybrid deployments—common conditions across intelligence programs.

For capture managers, this architecture supports key proposal differentiators: rapid ATO acceleration, reusable DevSecOps pipelines, zero-trust enforcement, and budget-aligned deployment models. The implementation roadmap anticipates government acquisition cycles and leverages pre-cleared cloud enclaves and FedRAMP High/SRG IL5 providers to compress timelines and reduce onboarding risks. Demonstrated compatibility with enterprise authorization frameworks ensures alignment with enterprise IT and avoids stovepiped solutions. **Financial payoff.** *Five-year TCO (§ 6.3) saves $ 27.6 M NPV, yields 28 % IRR, and pays back inside 20 months; IRR holds above 21 % even if key savings under-perform by 15 %.* ***Pilot payoff.*** *FY 2024 cross-agency deployment cut O&M 33 % (-9 FTE) and delivered $ 5.9 M NPV with 34 % IRR in 18 months.*

Risk posture. *Our formal risk register (§ 6.5) budgets $ 0.9 M and a 25-day buffer, reducing all residual risks to Low or Medium.*

This white paper underscores win themes critical to competitive pursuits: mission-first delivery, compliance by design, and integrated sustainment planning. The solution is primed for task order execution under IDIQ vehicles such as C2E, ICITE, or cloud BPA call orders, and is backed by a proven record of secure onboarding, containerized service delivery, and mission-need fulfillment.

Capture managers and technical leads are invited to engage in early teaming discussions and technical solutioning workshops to assess alignment with upcoming proposal requirements. Whether your firm leads the bid or contributes as a strategic partner, this SaaS-IaaS approach offers a powerful, low-risk enabler to meet and exceed intelligence customer expectations.

Current Landscape: The Relentless Drive Toward Scalable, Cloud-Native Intelligence Operations

The intelligence community (IC) is undergoing a rapid digital transformation driven by mission urgency, evolving threat vectors, and executive-level mandates that emphasize cloud-native capabilities, cybersecurity, and interoperability. Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) implementations are at the center of this shift—offering scalable, secure, and modular platforms capable of supporting data-intensive and time-sensitive intelligence missions. However, implementation remains uneven due to structural, acquisition, and policy-related constraints.

Several top-down mandates are catalyzing modernization. Executive Order 14028 (“Improving the Nation’s Cybersecurity”) underscores the federal imperative to adopt zero-trust architectures, accelerate cloud migration, and modernize legacy IT. For the IC, this aligns closely with initiatives like the Joint All-Domain Command and Control (JADC2), which demands seamless data sharing and real-time decision support across service lines and classification levels. Similarly, Cybersecurity Maturity Model Certification (CMMC) mandates heightened accountability and security from contractors, further increasing scrutiny on software and infrastructure procurement.

Procurement activity reflects this urgency. Vehicles such as C2E (Commercial Cloud Enterprise), IC ITE (Intelligence Community Information Technology Enterprise), and various cloud-focused BPAs (Blanket Purchase Agreements) are actively shaping the competitive landscape. These contracts emphasize multi-cloud capabilities, enclave compatibility, and mission-readiness at classified levels. Yet many offerings still face bottlenecks in Authorization to Operate (ATO) processes, interoperability testing, or compliance with cross-domain data sharing protocols.

One major implementation gap is the limited availability of SaaS solutions that are pre-authorized for secure enclaves or air-gapped networks. While IaaS has matured—with offerings at FedRAMP High and IL5/IL6—many SaaS platforms require costly customization or recertification. This slows down deployment and undermines the “plug-and-play” agility that SaaS is meant to deliver. Moreover, many mission-critical

workloads still rely on legacy infrastructure, making hybrid models and containerized delivery essential but operationally complex.

From a capture strategy standpoint, these conditions present both challenges and differentiators. Vendors that offer SaaS-IaaS solutions pre-aligned with NIST 800-53, support automated compliance tooling, and demonstrate compatibility with zero-trust and DevSecOps frameworks will hold an edge. Capture managers must also anticipate long procurement lead times and budget cycles, tailoring proposals to reflect phased implementation models, secure data zones, and modular scalability.

The landscape is also shaped by increasing pressure to avoid vendor lock-in and ensure interoperability across agencies and mission sets. Solutions that support containerized delivery, portable workloads, and common orchestration frameworks (e.g., Kubernetes, Terraform, OpenShift) are better positioned to meet evolving requirements.

In this context, the need for low-risk, policy-aligned, and rapidly deployable SaaS-IaaS solutions is more urgent than ever. Proposals that emphasize compliance-by-design, fast ATO paths, and flexible deployment models aligned with IC acquisition goals will have a distinct advantage in the next generation of mission contracts.

Mission-Critical Challenge: Fielding Modern Apps at Mission Speed While Navigating ATO Latency

The intelligence community (IC) faces a mission-critical challenge: delivering secure, scalable, and continuously updated digital capabilities at the speed of mission demands. Traditional IT delivery models—often reliant on custom-built, on-premises infrastructure—are increasingly misaligned with modern intelligence operations that require elastic compute, real-time analytics, and rapid software iteration. SaaS-IaaS implementation addresses this disconnect by enabling agile, modular deployment of infrastructure and mission applications across secure environments. However, several operational risks and limitations still constrain adoption and performance.

One of the most pressing risks is the delayed delivery of capabilities due to prolonged Authorization to Operate (ATO) timelines. Programs often wait months for infrastructure or applications to be certified for use in classified or controlled environments. This bottleneck limits the IC's ability to deploy cutting-edge tools like AI/ML, data fusion platforms, or analytic dashboards in time-sensitive contexts. It also introduces scheduling risk into program execution and reduces the government's return on investment for software procurement.

Additionally, mission owners are constrained by infrastructure silos and inconsistent security baselines. While some enclaves have adopted IaaS platforms at IL5 or IL6, many SaaS tools require reengineering or rehosting to meet security boundary requirements. This creates duplication of effort, complicates sustainment, and inhibits the reuse of software across agencies or mission sets—directly conflicting with JADC2 and multi-INT integration goals.

Another challenge is the inability to scale rapidly in response to emerging needs. Current models require physical provisioning or lengthy service onboarding for surge operations, such as during geopolitical crises, major cyber events, or rapid tasking. SaaS-IaaS architectures theoretically enable “on-demand” expansion, but in practice, many mission systems are locked into static provisioning or outdated deployment processes.

Unmet requirements also persist in the realm of telemetry, observability, and automated compliance. Many legacy systems lack the instrumentation to meet EO 14028 mandates around continuous monitoring or zero-trust enforcement. Without integrated security tooling and audit-ready logging, program managers are exposed to risk during operational test events, audits, or cyber inspections.

From an RFP planning perspective, these pain points introduce cost volatility, schedule uncertainty, and performance gaps that can sink bids or erode program credibility. Capture strategies must now account for how a solution reduces ATO latency, supports hybrid and classified deployment, and delivers measurable compliance and scalability from day one.

SaaS-IaaS implementation offers a strategic path forward—but only if designed with these challenges in mind.

Proposed Solution: A Portable, Containerized Cloud Stack with Pre-Packaged Security Artifacts

The proposed solution is a modular, compliance-forward SaaS-IaaS architecture purpose-built for secure deployment within the intelligence community (IC). It enables mission programs to provision, operate, and scale digital capabilities in classified and hybrid environments with high assurance, low risk, and alignment to key government compliance frameworks. This solution bridges the gap between traditional on-premise systems and modern cloud-native demands by integrating mission-ready SaaS applications with secure IaaS foundations pre-aligned to ISO, NIST, and FedRAMP standards.

At its core, the architecture combines containerized SaaS workloads with infrastructure deployed in government-authorized commercial cloud environments at IL5 and IL6 security levels. The IaaS layer is provisioned through FedRAMP High and DoD SRG-compliant service providers, ensuring the underlying infrastructure meets rigorous security and audit requirements. SaaS components are hosted within secure VPCs or air-gapped enclaves as needed, using Infrastructure-as-Code (IaC) to support reproducibility, auditability, and automation.

ISO and FedRAMP Alignment

The solution was designed from inception to align with ISO 9001:2015 (quality management systems) and ISO 27001:2022 (information security management systems), ensuring traceability of operational procedures, configuration management, and continuous improvement. Security controls are mapped to NIST 800-53 and CMMC 2.0, enabling streamlined ATO documentation and audit readiness.

In terms of FedRAMP readiness, the platform leverages pre-cleared service providers and implements standard boundary controls such as enclave isolation, data encryption in transit and at rest (FIPS 140-2), multifactor authentication, continuous monitoring (SOC/NOC integration), and automated patching. These elements ensure that SaaS workloads can achieve rapid FedRAMP Moderate or High authorization where required or operate within existing enclave ATO boundaries to minimize delay.

Integration and Interoperability

To support seamless integration with government IT environments, the architecture includes preconfigured APIs, data ingest pipelines, and security telemetry agents compatible with common IC platforms such as IC GovCloud, JWICS/NSANet, and enterprise IT systems. Interoperability is further enhanced via container orchestration (Kubernetes/OpenShift), IaC templates (Terraform/CloudFormation), and CI/CD toolchains that conform to DevSecOps and zero-trust reference architectures.

Technical Differentiators and Readiness

Key differentiators include:

- **ATO-Accelerated Deployment**: Pre-packaged security artifacts and compliance-as-code support rapid ATO reuse and documentation.

- **Portable SaaS Containers**: Mission applications are containerized and certified for deployment across multiple environments—on-premise, cloud, or disconnected.
- **Observability and Compliance**: Integrated dashboards and audit logging support real-time risk monitoring and automated compliance scoring.
- **Modular Scalability**: Services can be deployed incrementally or in full stack, supporting low-cost pilots or full production rollouts.

The solution is currently at **Technology Readiness Level (TRL) 8–9**, with multiple mission demonstrations completed in classified environments and production deployments under ICITE and DoD cloud modernization efforts. Reference architectures and implementation playbooks are available to support proposal integration.

Proposal Value and Capture Advantage

This solution enables low-risk, high-confidence program execution. It reduces schedule uncertainty through ATO reusability, supports rapid deployment within budget-constrained environments, and positions teams to meet EO 14028, JADC2, and ISO/NIST compliance requirements out of the box. Its modular design supports phased implementation aligned with acquisition milestones, enabling early value delivery and scalability without rework.

For capture managers, this translates to a differentiated, field-proven offering that aligns with IC mission priorities, reduces proposal execution risk, and demonstrates technical maturity.

Capture-Focused Benefits: Demonstrating a 60% Cut in ATO Timelines and Clear TCO Reductions

The proposed SaaS-IaaS implementation offers a suite of capture-focused benefits that directly align with the technical evaluation criteria and scoring elements commonly found in intelligence community (IC) solicitations. Designed for integration into high-stakes proposals under vehicles like C2E, ICITE, and various cloud BPAs, this solution strengthens competitive positioning across multiple Section L and M factors—including technical merit, risk mitigation, compliance alignment, and past performance relevance.

Alignment with Section L&M Criteria

Under Section M evaluation models, the solution scores strongly on **Technical Approach**, **Risk**, and **Compliance**. It supports measurable low-risk implementation through the use of FedRAMP High and IL5/IL6 authorized IaaS environments, pre-certified SaaS components, and a proven DevSecOps pipeline that accelerates ATO issuance. By delivering compliance artifacts and security boundary controls as code, the approach reduces time-to-field and demonstrates technical maturity—key differentiators in best-value tradeoff procurements.

The modularity and portability of the SaaS workloads also support high marks in **Innovation** and **Scalability**, enabling phased deployment strategies that match program funding profiles or transition plans. The use of containerization and open orchestration tools (e.g., Kubernetes) ensures flexibility, vendor neutrality, and alignment with zero-trust mandates under EO 14028.

Teaming Strategy Enablement

For capture managers building prime-sub teaming strategies, this offering provides clear integration points for specialized small businesses, cybersecurity providers, or mission software vendors. The open architecture and API-first design reduce integration barriers and simplify workshare segmentation. Teams can easily map roles and responsibilities across deployment, sustainment, and compliance functions—improving teaming clarity and proposal structure.

Compliance Posture and Proposal Friction Reduction

From a compliance standpoint, the solution comes pre-aligned with ISO 9001:2015, ISO 27001:2022, and NIST 800-53 controls, allowing capture teams to incorporate verifiable evidence into Volume II/III submissions. By providing ATO-ready documentation, test data, and operational KPIs, the solution reduces proposal development friction—especially during Red/Gold Team reviews when compliance proof points often create schedule pressure.

Capture Value Summary

In summary, this offering improves proposal win probability by aligning with high-weight evaluation criteria, streamlining compliance documentation, and enabling flexible, team-friendly integration models. It presents a technical solution that is not only field-proven but also primed for rapid delivery—providing a compelling narrative for risk reduction, mission impact, and readiness to execute.

Implementation Strategy: Iterative Delivery from Enclave Hardening to Full Mission Deployment

The implementation of the proposed SaaS-IaaS solution is structured around a phased deployment model that aligns with federal acquisition lifecycles and intelligence community (IC) program schedules. This model supports modular rollout across three stages: Phase 1: Technical Pilot & Environment Hardening, Phase 2: Initial Operating Capability (IOC), and Phase 3: Full Mission Deployment (FMD). Phase 1 enables early mission sponsor engagement and ATO preparation through low-risk, containerized deployment in controlled test environments. Phase 2 introduces scalable SaaS functionality and data ingest pipelines, validated through mission-specific use cases. Phase 3 completes integration with IC networks and sustainment operations, with full metrics and security telemetry reporting.

Flexible Funding Strategies Aligned to Capture

To match the diverse funding landscape of the IC, the solution supports flexible funding strategies that align with capture and proposal development goals. For rapid prototyping or early experimentation, Other Transaction Agreements (OTAs) and SBIR/STTR pathways offer agile entry points. For more formalized programs of record, the solution is positioned to support IDIQ-based call orders under enterprise contracts such as C2E or cloud BPAs. CRADAs and tech insertion programs allow dual-use innovation partners to de-risk integration without requiring full procurement. Each funding route supports early technical validation, stakeholder engagement, and transition to production with reduced obligation upfront—enhancing proposal flexibility.

Acquisition Vehicle Compatibility

The solution is also acquisition-ready across multiple federal contracting vehicles, including GSA MAS (Multiple Award Schedule), OASIS, ASTRO, and various GWACs (e.g., SEWP, Alliant 2). These channels support both unclassified and classified service acquisition, enabling streamlined contracting and competitive teaming under full-and-open or small business set-asides. The architecture's modularity allows it to be scoped as either a managed service, software license, or infrastructure support package depending on the acquisition strategy—enhancing alignment with Section L technical format and pricing structures.

Five-Year TCO / ROI Snapshot

To quantify the operational and financial benefits of the proposed solution, we modeled a five-year comparison of siloed legacy systems versus a shared SaaS-IaaS platform. This snapshot highlights reductions in infrastructure spend, licensing sprawl, and sustainment labor—delivering a compelling return on investment even under conservative assumptions.

Year	Implementation & Migration ($M)	Annual O&M & Sustainment ($M)	Risk Management Reserve ($M)	Total Annual Costs ($M)	Cumulative PV Costs ($M)
Year 0	9.80	—	**0.90**	10.70	10.09
Year 1	1.10	8.80	—	9.90	19.43
Year 2	—	9.20	—	9.20	27.61
Year 3	—	9.50	—	9.50	35.59
Year 4	—	9.80	—	9.80	43.82
Year 5	—	10.10	—	10.10	**52.90**

Totals	**10.90**	**47.40**	**0.90**	**59.20**	**52.90**

Headline metrics

- **NPV savings (5 yrs): $ 27.6 M**
- **Internal Rate of Return (IRR): 28 %**
- **Pay-back: ≈ 20 months**
- **Sustainment labor delta: –9 FTE (≈ 35 %)**

These cost savings are not hypothetical—they reflect patterns observed in pilot deployments and validated IC usage profiles. The 28% IRR and sub-20-month payback window demonstrate the financial sustainability of the model, particularly when paired with compliance and risk advantages discussed in the following section.

ROI Sensitivity (± 15 % on dominant drivers)

To test the resilience of this model, we ran sensitivity scenarios on key financial drivers. Even with 15% underperformance in license consolidation, labor costs, or infrastructure utilization, the solution maintains IRRs above federal hurdle rates.

Driver ± 15 %	Low-Case IRR	Base IRR	High-Case IRR
Licence-consolidation pace	21 %	**28 %**	34 %
Labor-rate escalation	22 %	**28 %**	32 %
IaaS utilisation (shared-node gain)	23 %	**28 %**	35 %

This resilience underscores the defensibility of the business case—critical when responding to Red Team challenges or price realism scoring in proposal evaluations.

Risk Register & Mitigation Matrix

While SaaS-IaaS adoption offers clear performance and cost benefits, intelligent risk planning remains essential. The following matrix highlights anticipated challenges and funded mitigations, each traceable to measurable cost reserves and time buffers.

Risk ID	Description	Likelihood	Impact	Fundable, Measurable Mitigation	Mitigation Cost*	Schedule Buffer	Residual
R-1	Cross-agency identity-federation failure (SAML/OIDC drift)	Med	High	Dual-stack IdP; weekly schema-diff; hot-patch scripts	**$150 k** (Yr 0 CAPEX)	+ 5 d	**Low**
R-2	SaaS licence tiering underestimates surge users	Med	Med	Auto-tier alert at 80 %; prepaid buffer SKUs	**$80 k / yr** (OPEX)	+ 3 d	Low
R-3	IAM mis-scope exposes management APIs	Med	Med	Open Agent Policy/Rego ABAC; daily OpenSCAP & eBPF runtime guard	**$60 k / yr** (OPEX)	+ 3 d	Low
R-4	FedRAMP-High / IL-6 ATO delay for shared SaaS stack	Med	High	ATO-as-code pipeline; control inheritance; pre-audit	**$200 k** (Yr 0 CAPEX)	+ 6 d	**Med**
R-5	Skill gap—agency ops to SRE/DevSecOps roles	High	Med	8-week FinOps/SRE boot-camp; 2 embedded SMEs	**$240 k** (Yr 0-1 CAPEX)	+ 5 d	Med
R-6	Cloud egress / storage spike	Low	Med	Cost-ops alerts at 75	**$60 k / yr** (OPEX)	0 d	Low

Risk ID	Description	Likelihood	Impact	Fundable, Measurable Mitigation	Mitigation Cost*	Schedule Buffer	Residual
	from unexpected analytics			% / 90 %; lifecycle rules			
R-7	Vendor lock-in to single IL-5 region	Low	High	Multi-cloud IaC (Terraform); quarterly fail-over drill	**$110 k** (Yr 0 CAPEX)	+ 3 d	Low

* **Total mitigation cost ≈ $ 900 k**, funded by the **$ 0.9 M risk-reserve** already embedded in the 5-year TCO (see Appendix C).
The cumulative **25-day schedule buffer** is likewise built into the phased-deployment timeline.

All risks are reduced to Low or Medium residual levels through embedded controls and pre-funded actions. This risk posture is fully captured in the $0.9M reserve and 25-day buffer embedded in the cost model, further strengthening proposal defensibility.

Risk and Cost Management Features

Built-in risk and cost management features further strengthen proposal credibility. These include cost-optimized resource provisioning, automated compliance reporting to reduce audit costs, and predefined playbooks for environment stand-up that eliminate rework. Version-controlled templates ensure configuration consistency and traceability, while usage-based scaling controls limit budget overrun exposure. Importantly, the ATO-acceleration framework reduces schedule risk by months—addressing one of the most persistent pitfalls in IC program execution.

Together, this implementation strategy presents a low-risk, flexible, and funding-aligned path to mission impact—backed by acquisition readiness and technical maturity that enhances proposal scoring across cost, technical, and risk criteria.

Teaming Opportunities: Anchoring Modular Workshares with a Compliant, API-First Platform

The proposed SaaS-IaaS solution offers a versatile foundation for teaming strategies in intelligence community (IC) pursuits, supporting both **prime-led proposals** and **subcontractor contributions** across large-scale acquisition vehicles such as C2E, ICITE, and GWACs like Alliant 2 and SEWP. Its modular, standards-based design allows integrators, cybersecurity providers, analytics firms, and infrastructure partners to align their offerings around a common, mission-ready platform that accelerates proposal readiness and strengthens overall solution credibility.

For **prime contractors**, the solution serves as a low-risk, high-readiness technology stack that satisfies technical evaluation criteria tied to zero-trust, cloud enablement, and secure DevSecOps pipelines. It enhances the proposal's **Technology Readiness Level (TRL)** profile—demonstrated at TRL 8–9 through multiple deployments in classified and controlled environments—and brings validated **past performance** to bolster Volume III narratives. This makes the offering highly attractive for competitive bids where evaluators prioritize field-tested, low-friction implementations.

For **subcontractors**, the architecture offers multiple entry points to contribute value. Small businesses and niche vendors can integrate mission-specific SaaS applications, data visualization tools, or AI/ML modules within the solution's containerized framework. Cybersecurity firms can embed continuous monitoring, SIEM, or threat analytics components, while infrastructure providers support enclave provisioning and cross-domain deployment. These roles align well with common **proposal workshare structures** such as software engineering, security operations, integration support, and sustainment.

The solution also supports teaming narratives around innovation, compliance, and technical interoperability—key win themes in IC proposals. Its API-first architecture and compliance-by-design foundation make it easy to define clean interfaces, handoffs, and integration points between team members. This minimizes risk and enhances proposal defensibility during Red Team reviews and oral presentations.

In sum, this SaaS-IaaS implementation is a force multiplier for teaming strategies—providing a credible, adaptable, and field-proven platform around which primes and subs can coalesce to deliver mission-aligned, technically mature solutions.

Case Study: Rapidly Integrating Threat Intelligence Fusion Across Cross-Agency Clouds

Mission Requirement

In late FY23, a joint mission team within the intelligence community (IC) faced an urgent requirement: rapidly integrate disparate threat intelligence streams across multiple classified networks to support time-sensitive operations. Traditional infrastructure provisioning and software onboarding would have taken 6–9 months—time the mission didn't have.

Execution Timeline and Technical Approach

Instead, program leadership piloted a modular SaaS-IaaS implementation designed specifically for secure, containerized deployment within IL5 and IL6 cloud environments. The solution leveraged a pre-cleared IaaS provider authorized under FedRAMP High and DoD SRG IL6, paired with containerized SaaS analytics and data fusion applications. These workloads were deployed using pre-configured Infrastructure-as-Code (IaC) templates and compliance-as-code packages, enabling a hardened enclave and development pipeline to be operational in under 30 days. The pilot was executed in three phases:

- ***Week 1–2**: Environment stand-up*
- ***Week 3–5**: SaaS container deployment and integration*
- ***Week 6–8**: Operational validation using live data*

Funding and Acquisition Path

Funding was secured through an OTA pilot agreement, allowing the agency to bypass lengthy procurement cycles and validate capability performance before committing to a multi-year contract. The success of the pilot directly influenced downstream program planning and was cited in the justification for a sole-source follow-on under a task order on the agency's existing IDIQ.

Pilot Financial Outcomes

The pilot's $ 2.4 M up-front investment is recouped in 18 months through annual O&M savings of $ 1.6 M and a nine-person reduction in sustainment head-count. Discounted over five fiscal years at a 6 % real rate, the shared environment produces $ 5.9 M in net-present savings and a 34 % IRR—well above typical IC hurdle rates (E-7). Operationally, ATO lead-time fell 60 % while stand-up duration dropped from 120 days to 30 days, validating the phased rollout model in § 6.2.

Metric	***Legacy Stack***	***Pilot (Shared SaaS-IaaS)***	***Δ / ROI***
One-time CAPEX (tooling, ATO, cut-over)	—	***$ 2.4 M***	—
Annual O&M $	*$ 4.8 M*	*$ 3.2 M*	***–33 % (-$ 1.6 M/yr)***
Sustainment FTE	*24*	*15*	***-9 FTE (-38 %)***
ATO lead-time	*75 days*	*30 days*	***-60 %***
Stand-up duration	*120 days*	*30 days*	***-75 %***
Five-year NPV (6 %)	—	—	***$ 5.9 M saved***
Internal Rate of Return (IRR)	—	—	***34 %***
Pay-back	—	—	***Month 18***

CAPEX covers container refactor, FedRAMP High boundary inherit docs, dual-run window, and ATO-as-code pipeline.

Mission Impact and Proposal Relevance

The mission impact was significant. Analysts previously siloed by classification boundaries were able to access shared dashboards, federated queries, and collaborative tools that surfaced real-time threat indicators and mission context. System logs, audit trails, and compliance dashboards were available from day one, satisfying internal CISO requirements without delaying deployment. The ATO process was

reduced by over 60% thanks to reusable documentation and pre-accredited components.

From a capture and proposal perspective, this pilot now serves as past performance for bids under the C2E and Alliant 2 vehicles. The solution's demonstrated TRL 8–9 maturity, low-risk deployment model, and compliance alignment are key strengths in competitive evaluations. Moreover, teaming partners were able to integrate their analytics, cyber, and support capabilities into the architecture—validating interoperability and strengthening technical narratives in current proposals.

This case study provides a clear, real-world example of SaaS-IaaS feasibility, speed, and mission value—proving that secure innovation at classified levels is not only possible, but repeatable.

Forecast: Enterprise-Standard SaaS/IaaS Architectures Displacing Isolated Cloud Pilots

Over the next 3–5 years, SaaS-IaaS implementation in the intelligence community (IC) will evolve from isolated pilots to enterprise-standard practice. Driven by modernization mandates, zero-trust enforcement, and multi-agency interoperability demands, IC programs will increasingly require solutions that deliver secure, scalable, and rapidly deployable capabilities with minimal infrastructure burden. This shift will directly influence RFP structures, evaluation weightings, and the expectations placed on technical volumes and teaming strategies.

Emerging RFPs will emphasize **compliance-by-design**, mandating pre-alignment with frameworks such as **ISO 9001:2015**, **ISO 27001:2022**, **NIST 800-53 Rev. 5**, and zero-trust architecture models. Solutions that can demonstrate FedRAMP authorization, pre-cleared IL5/IL6 deployments, and automated security controls will gain early evaluator confidence. Budget guidance will favor **modular acquisition strategies**—enabling initial SaaS-based pilots with scalability into full IaaS-backed production environments. This flexibility supports programs constrained by continuing resolutions or incremental funding releases.

Capture managers must anticipate a shift in value scoring. Technical volumes will increasingly be judged on **deployment readiness**, **compliance automation**, and **interoperability proof points**. As agencies seek to avoid vendor lock-in, offerings that support containerized delivery, open standards, and rapid ATO acceleration will score

higher in innovation and risk categories. Primes that wait to build these capabilities post-RFP may find themselves behind the curve.

To stay competitive, **early investment is essential**. Primes and major integrators that engage during the RFI stage—with proof-of-concept architectures, field-tested SaaS-IaaS integrations, or compliance artifacts—will be better positioned to shape requirements, influence evaluation language, and define teaming structures. These early engagements also provide the evidence base needed for strong past performance and TRL assertions, which often carry significant scoring weight under Section M.

In short, SaaS-IaaS is not just an IT trend—it's a capture imperative. Teams that embed this model early in their pipelines will define the technical baseline, reduce proposal risk, and increase their probability of win in an increasingly cloud-first, compliance-driven IC acquisition landscape.

Conclusion: Accelerating Intelligence Delivery and Bid Success with Field-Tested Cloud Solutions

For capture managers operating in the intelligence community (IC), SaaS-IaaS implementation represents more than a technical offering—it is a strategic enabler of mission agility, proposal credibility, and competitive differentiation. As IC agencies accelerate their shift toward zero-trust architectures, cloud-native delivery, and compliance automation, solutions that offer secure, scalable, and rapidly deployable capabilities are no longer optional—they are expected.

This white paper has outlined a proven SaaS-IaaS framework that delivers measurable mission impact through accelerated ATO timelines, containerized portability, and alignment with ISO 9001:2015, ISO 27001:2022, and NIST 800-53 mandates. With a TRL of 8–9 and successful deployments in secure, classified environments, the solution provides a low-risk, high-readiness platform that aligns well with evolving RFP requirements and technical evaluation criteria.

The architecture supports flexible teaming strategies, enabling primes and subs alike to integrate seamlessly into modular roles—from infrastructure support to mission software delivery. It also strengthens proposal narratives across Section L and M factors, particularly in areas of technical maturity, compliance alignment, and risk mitigation.

Now is the time for capture teams to act. Whether you're pursuing an IDIQ call order, shaping an RFI response, or defining your technical volume strategy, this SaaS-IaaS approach can give your bid the operational edge and evaluator confidence needed to

win. **Engage early—secure your teaming position, validate your solution set, and shape the next generation of IC cloud modernization.**

Appendices and Supporting Materials

Appendix A – Glossary of Acronyms

This glossary provides definitions of key acronyms relevant to SaaS-IaaS implementation within the intelligence community (IC), specifically in the context of federal procurement, compliance, and technical execution.

ATO – Authorization to Operate
A formal declaration by a Designated Authorizing Official (AO) that an information system is approved to operate in a given environment. Crucial for SaaS/IaaS deployment in classified or sensitive networks.

C2E – Commercial Cloud Enterprise
The enterprise-wide acquisition vehicle used by the IC for commercial cloud services, supporting multi-cloud strategies and enabling access to IaaS, PaaS, and SaaS offerings.

CI/CD – Continuous Integration / Continuous Deployment
An automated DevSecOps approach that ensures frequent, reliable updates of software and infrastructure, supporting rapid delivery in IC environments.

CRADA – Cooperative Research and Development Agreement
A funding and collaboration mechanism between federal agencies and private-sector partners to test or co-develop technologies, often used in early-stage SaaS/IaaS pilots.

FedRAMP – Federal Risk and Authorization Management Program
A government-wide program that standardizes security assessment and authorization for cloud services. FedRAMP High and IL5/IL6 compliance are essential for IC cloud deployments.

GWAC – Government-Wide Acquisition Contract
Multi-agency contracts such as Alliant 2 or SEWP that facilitate federal procurement of IT services and cloud solutions.

ICITE – Intelligence Community Information Technology Enterprise
A shared infrastructure initiative that unifies and modernizes IT across IC agencies, setting key standards for SaaS-IaaS integration and interoperability.

IL5 / IL6 – Impact Level 5 / 6
Department of Defense classification levels for cloud service offerings, indicating the security level required for handling Controlled Unclassified Information (CUI) and classified data, respectively.

ISO – International Organization for Standardization
Refers here to **ISO 9001:2015** (Quality Management) and **ISO 27001:2022** (Information Security Management), which are foundational to SaaS-IaaS credibility and ATO acceleration.

NIST – National Institute of Standards and Technology
NIST 800-53 and related publications define security controls and risk management frameworks for federal systems, used extensively in SaaS-IaaS compliance planning.

OTA – Other Transaction Authority/Agreement
A flexible acquisition vehicle used to rapidly prototype or evaluate non-traditional solutions, often leveraged to test SaaS-IaaS in IC missions prior to full-scale procurement.

SaaS – Software-as-a-Service
A cloud service model where software applications are delivered on demand via secure hosting platforms, minimizing infrastructure and operations overhead.

IaaS – Infrastructure-as-a-Service
A cloud model providing scalable compute, storage, and network infrastructure as a service, supporting containerized workloads, secure enclaves, and mission systems in IC programs.

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

This appendix outlines how the proposed SaaS-IaaS solution aligns with key compliance frameworks—**ISO 9001:2015**, **ISO 27001:2022**, and applicable **NIST 800-53** or **Risk Management Framework (RMF)** controls—tailored for intelligence community (IC) requirements. The approach emphasizes security, quality, and auditability from design through operations, supporting ATO acceleration and mission assurance.

1. ISO 9001:2015 – Quality Management System (QMS) Alignment

Clause	Description	SaaS-IaaS Implementation Alignment
4.4	Process Approach	Defined DevSecOps pipelines with IaC, version control, and CI/CD workflows ensure repeatable, documented outcomes.
5.1	Leadership and Commitment	Solution design includes governance playbooks and designated system owners to meet IC leadership requirements.
6.1	Risk-Based Thinking	Integrated risk registers and automated vulnerability scanning tied to release gates in CI/CD.
7.1	Resource Management	Cloud resources are allocated and monitored using automated policies and dashboard-based observability.
8.5	Production and Service Provision	SaaS components delivered via containerized pipelines, tested and validated prior to deployment in secure enclaves.
9.1	Performance Evaluation	KPIs tracked for system uptime, compliance drift, and mission data throughput.

2. ISO 27001:2022 – Information Security Management System (ISMS) Alignment

Control Area	Description	SaaS-IaaS Implementation Alignment
A.5	Organizational Controls	Role-based access control (RBAC), security policy enforcement across tenant zones.
A.6	People Controls	Support for SCIF-cleared personnel, MFA, and least privilege enforced for IC users.
A.8	Technological Controls	Encryption (FIPS 140-2), secure API gateways, telemetry with SIEM integration.

Control Area	Description	SaaS-IaaS Implementation Alignment
A.12	Operations Security	Immutable logging, container monitoring, patch automation for OS and runtime dependencies.
A.15	Supplier Relationships	Secure integration paths with cleared subcontractors and SaaS vendors; chain-of-custody audits.

3. NIST 800-53 Rev. 5 / RMF Control Alignment

Control Family	Example Control	SaaS-IaaS Implementation Coverage
AC – Access Control	AC-2, AC-6	Federated identity management, MFA, just-in-time access via IAM tools.
AU – Audit and Accountability	AU-2, AU-6	Centralized, immutable log collection with retention policies and real-time alerts.
CM – Configuration Management	CM-2, CM-6	Declarative IaC with drift detection, container image scanning before deployment.
SC – System and Communication Protection	SC-12, SC-28	TLS encryption for all data in transit, volume-level and object-level encryption at rest.
SI – System and Information Integrity	SI-2, SI-4	Continuous vulnerability scanning, threat intelligence feeds, runtime behavior monitoring.

4. Tailoring for the Intelligence Community

- **Impact Level Readiness**: Designed for IL5/IL6 environments using FedRAMP High baselines and enclave-hardened configurations.
- **Cross-Domain Awareness**: Enclave-aware deployment models and secure data movement support for air-gapped or multi-network architectures.

- **ATO Support**: Pre-built System Security Plans (SSPs), Security Control Traceability Matrices (SCTMs), and Plan of Action & Milestones (POA&M) templates accelerate RMF compliance.

This compliance-driven approach reduces program onboarding time, supports mission assurance, and ensures audit readiness—providing a defensible, low-risk path to deployment within the IC's most sensitive operating environments.

Appendix C – Cost-Model Assumptions & Methodology

Category	Assumption	Rationale / Data Source
Analysis window	5-yr NPV (FY 26-30)	Matches IC IDIQ base + 4 options
Discount rate	6 % real	OMB Circular A-94 midpoint
Baseline footprint	52 isolated agency VMs, PUE 1.95, 24 FTE sustainment	Current IC ops logs (Mar 2025)
Shared footprint	34 hyper-converged nodes, PUE 1.38, 15 FTE SRE	2024 cross-agency pilot
IaaS tariff	$ 0.052 / vCPU-hr, IL-5	FY 25 GSA Cloud SIN
Licence escalation	4 % CAGR legacy vs. flat SaaS bundle	Gartner Fed-SW Index '24
Labor rate	$ 174 k loaded GS-13 FTE	FY 25 OPM + 38 % OH
Automation uptake	55 % Yr 1 → 85 % Yr 3	Pilot DevSecOps metrics
One-time compliance	$ 340 k (STIG, SBOM, FedRAMP inherit)	DISA SRG audits
Inflation factors	2.2 % labor, 2 % cloud infra	OSD CAPE 2025-30 guidance

Category	Assumption	Rationale / Data Source
Risk reserve	$ 0.9 M (~3 % PV)	Matches § 6.5 mitigation totals
Schedule buffer	25 calendar days	Embedded in phased timeline
Exclusions (neutral)	WAN backhaul, leasehold rent	Equal across scenarios

Sensitivity derivation: ± 15 % swings on licence-cut pace, labor escalation, and utilisation gain produce an IRR band **21–35 %**.

Appendix D – References

Executive Orders and Federal Memos

1. **Executive Order 14028** – *Improving the Nation's Cybersecurity* (May 2021) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
2. **OMB Memorandum M-22-09** – *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 2022) https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
3. **DoD Cloud Strategy** (December 2018) https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Cloud%20Strategy.pdf

NIST Publications

4. **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
5. **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

6. **NIST SP 800-160 Vol. 1** – *Systems Security Engineering*
https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/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

DoD and Intelligence Community Documents

8. **IC CIO Strategy 2023–2025** – *Transforming Intelligence Through Secure IT Modernization*
https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/item/2306-ic-chief-information-officer-strategy-2023-2025
9. **Joint All-Domain Command and Control (JADC2) Strategy** – DoD (2022)
https://media.defense.gov/2022/Mar/17/2002958402/-1/-1/0/JADC2-STRATEGY.PDF
10. **CISA Cloud Security Technical Reference Architecture (TRA)** (August 2021)
https://www.cisa.gov/resources-tools/resources/cloud-security-technical-reference-architecture

FedRAMP and ISO Standards

11. **FedRAMP Security Assessment Framework (SAF)** – Version 3.0
https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf
12. **ISO/IEC 27001:2022** – *Information Security Management Systems*
https://www.iso.org/standard/27001
13. **ISO 9001:2015** – *Quality Management Systems Requirements*
https://www.iso.org/standard/62085.html

Commercial and Industry White Papers

14. **Microsoft Azure Government – Cloud Adoption Framework for National Security and IC**
https://learn.microsoft.com/en-us/azure/azure-government/documentation-government-overview

15. **AWS – Implementing Zero Trust Architectures in National Security Environments**
https://aws.amazon.com/government-education/national-security/