AVALON
TECHNOLOGY SERVICES

Securing Tomorrow's Missions Today.

2026

# Shaping the Future of Secure Delivery in the Intelligence Community Through DevSecOps

Secure. Fast. Mission-Ready. DevSecOps for the Intelligence Community.

AvalonTechServices.com

contact@AvalonTechServices.com

## Executive Summary

The Intelligence Community (IC) faces persistent challenges in delivering secure, high-quality software at the speed required to outpace adversaries. Traditional development and security approaches often result in extended delivery cycles, fragmented toolchains, and delayed Authority to Operate (ATO) approvals. These inefficiencies create operational risk and limit mission agility. DevSecOps provides an integrated framework that unites development, security, and operations into a continuous, automated pipeline. This approach accelerates deployment timelines, strengthens cybersecurity posture, and improves operational readiness across mission systems.

For capture managers, DevSecOps offers a compelling differentiator in competitive bids. The solution aligns with federal priorities outlined in Executive Order 14028 and supports zero-trust architecture adoption. By embedding security from the start, the IC can achieve both compliance and resilience without compromising delivery speed. The approach leverages automation for continuous integration, testing, and security validation, ensuring that code deployed to mission environments is secure, functional, and compliant.

Implementation risk is minimized through a phased adoption strategy. Early proof-of-concept deployments can be rapidly scaled to enterprise-level pipelines, reducing transition risk and ensuring compatibility with existing classified and unclassified environments. This incremental rollout supports alignment with acquisition timelines and budget cycles, enabling programs to show measurable value within the first contract year.

From a cost perspective, the financial benefits are equally compelling. DevSecOps reduces costly rework, minimizes downtime from security incidents, and accelerates delivery of mission capability.
**Financial payoff.** *Five-year TCO (§ 6.3) saves **$ 12.8 M NPV**, delivers **38 % IRR**, and pays back in **17 months**; IRR stays above **28 %** even if key savings under-perform by 15 %.*

To maintain a competitive edge, industry partners should engage early to define DevSecOps integration pathways tailored to each program's security classification, operational tempo, and mission objectives. By partnering with proven integrators, capture teams can position proposals as low-risk, high-value solutions that directly address the IC's most pressing software delivery challenges.

**Call to Action:** Capture managers and technical teams should initiate teaming discussions now to align DevSecOps strategies with current solicitations. Early collaboration will ensure that proposals clearly articulate mission impact, compliance

assurance, and measurable return on investment—maximizing win probability in upcoming IC procurements.

## Current Landscape: The Shift to Continuous, Automated Software Delivery in the IC

The Intelligence Community (IC) operates in an environment where secure, rapid software delivery is essential for maintaining decision superiority. Adversaries continuously adapt their cyber capabilities, forcing the IC to modernize its software development and deployment processes. DevSecOps—integrating development, security, and operations into a unified, automated framework—has emerged as a key enabler for delivering secure mission capabilities at the speed of relevance.

Recent federal mandates have accelerated the push toward DevSecOps adoption. **Executive Order 14028**, *Improving the Nation's Cybersecurity*, directs agencies to advance toward zero trust architectures and improve supply chain security through practices such as secure software development frameworks and continuous monitoring. **Joint All-Domain Command and Control (JADC2)**, while originating within the Department of Defense, has spillover effects into IC operations by requiring interoperable, secure, and agile data and application environments. The **Cybersecurity Maturity Model Certification (CMMC)** framework underscores the importance of verified, repeatable security practices throughout the development lifecycle—an area in which DevSecOps offers strong compliance alignment.

Procurement activity reflects this shift. Multiple classified and unclassified IC programs have issued solicitations calling for agile software factories, continuous integration/continuous deployment (CI/CD) pipelines, and embedded security testing. Contract language increasingly references automated compliance reporting, rapid ATO processes, and adherence to NIST Secure Software Development Framework (SSDF) guidance. Large-scale modernization efforts—such as cloud migration initiatives and AI-enabled analytics platforms—require DevSecOps to ensure security assurance without delaying capability delivery.

Despite this progress, solution gaps remain. Many IC programs still rely on legacy development methodologies that isolate security from development, leading to bottlenecks during testing and accreditation. Manual compliance documentation remains prevalent, increasing time-to-field for new capabilities. Toolchain fragmentation, inconsistent adoption of automation, and workforce skill gaps further limit the speed and scale of secure software delivery. Moreover, cross-domain and multi-level security

challenges require tailored DevSecOps architectures that can operate effectively in classified environments.

For capture managers, these gaps represent opportunities to differentiate proposals. Demonstrating the ability to integrate DevSecOps into classified mission environments—while addressing cultural and process change barriers—can position an offeror as a low-risk, high-value partner. Solutions that automate security validation, streamline ATO processes, and enable rapid, repeatable deployments can directly address the IC's mission pain points. Additionally, proposals that link DevSecOps adoption to measurable cost savings and operational efficiencies align well with tightening budget oversight and outcome-focused acquisition strategies.

Looking forward, the demand for DevSecOps in the IC will continue to grow. Intelligence programs are under pressure to deliver capabilities faster, respond to emerging threats in near real-time, and maintain operational security against sophisticated adversaries. Contractors able to demonstrate mature, security-embedded CI/CD capabilities—backed by compliance evidence and mission-tested performance—will be best positioned to win competitive procurements. DevSecOps is no longer a forward-leaning innovation; it is rapidly becoming a baseline expectation for delivering software in the Intelligence Community.

## Mission-Critical Challenge: Breaking the Bottleneck of Manual Security Validation and Slow Releases

The Intelligence Community (IC) faces a persistent challenge: delivering mission-ready software capabilities at the speed of evolving threats without compromising security or compliance. As cyber adversaries increase their sophistication, the time window to respond with effective, secure solutions continues to narrow. Yet many IC programs remain constrained by outdated development methodologies, lengthy accreditation processes, and manual security validation. These limitations impede the ability to deploy capabilities quickly and adapt to rapidly changing mission needs.

The operational risks are significant. Slow capability deployment limits the IC's ability to detect, analyze, and respond to adversary activity in near real-time. Legacy development approaches often treat security as a late-stage activity, resulting in vulnerabilities discovered only after integration and testing. This reactive approach increases the likelihood of operationally exploitable weaknesses and drives costly rework. Additionally, accreditation processes can extend deployment timelines by

months, delaying the delivery of capabilities that may be urgently needed to address time-sensitive intelligence priorities.

Current limitations compound these risks. Many IC programs maintain fragmented toolchains with limited automation, leading to inconsistent quality, redundant work, and integration failures. Manual compliance documentation and security testing consume significant time and resources, creating bottlenecks and reducing agility. The absence of a unified, security-embedded pipeline increases the probability of vulnerabilities slipping into production environments. Furthermore, classification-level constraints often limit the ability to leverage commercial best practices, forcing the IC to rely on custom, stovepiped solutions that are difficult to maintain and scale.

Unmet requirements are clear. The IC needs a repeatable, automated approach to software development that embeds security from the outset, accelerates Authority to Operate (ATO) processes, and ensures continuous compliance. This approach must enable seamless collaboration across development, security, and operations teams while accommodating the unique demands of classified environments. It must also be adaptable to integrate with both existing infrastructure and evolving cloud, AI, and analytic platforms without introducing unacceptable operational risk.

For capture managers, these challenges directly influence RFP planning and program delivery strategies. Solicitations increasingly require demonstrable expertise in secure, automated delivery pipelines capable of reducing deployment timelines while maintaining compliance with NIST, CMMC, and IC-specific security directives. Proposals that cannot address these requirements risk being viewed as high-implementation-risk solutions. Conversely, proposals built around proven DevSecOps models—tailored to the IC's operational realities—offer a compelling path to overcoming these mission-critical challenges while maximizing win probability.

## Proposed Solution: An Integrated, Security-by-Design Pipeline for Classified Environments

The proposed solution delivers a fully integrated **DevSecOps framework** designed to accelerate secure capability delivery across the Intelligence Community (IC) while meeting the highest federal compliance and accreditation standards. Built for classified and controlled environments, this approach unites development, security, and operations into a continuous, automated pipeline that embeds security at every stage of the lifecycle.

## Compliance Alignment and Assurance

The solution is engineered to align directly with **ISO 9001:2015** quality management principles by incorporating continuous improvement, process standardization, and performance measurement into every pipeline stage. In parallel, **ISO 27001:2022** requirements are addressed through rigorous risk assessment, access controls, encryption standards, and security monitoring embedded within the DevSecOps process.

For cloud-hosted and hybrid deployments, the framework is **FedRAMP-ready**, supporting continuous monitoring and automated compliance evidence generation. This reduces the administrative burden of maintaining Authority to Operate (ATO) and positions programs for streamlined **Continuous ATO (cATO)** accreditation, enabling rapid updates without re-certification delays.

## Ease of Integration with Government IT Systems

The solution integrates seamlessly with existing **government IT systems** and toolchains, whether in classified on-premises environments, government-operated cloud platforms, or hybrid infrastructures. Open APIs, modular tool integrations, and adherence to established IC interoperability standards ensure compatibility with current systems while preserving the flexibility to adapt to emerging technologies. Integration pathways include support for **Cross Domain Solutions (CDS)**, mission data fabrics, and zero trust architectures mandated by EO 14028.

## Technical Differentiators

Key technical differentiators include:

- **Security-by-Design Automation**: Continuous integration/continuous deployment (CI/CD) pipelines with automated security scans, static/dynamic code analysis, and compliance validation integrated from the earliest development stages.
- **Continuous Compliance Evidence**: Real-time generation and storage of compliance documentation to satisfy NIST, CMMC, and IC-specific security requirements, enabling near-instant audit readiness.
- **Mission-Adaptable Pipelines**: Configurable workflows tailored for different classification levels, mission types, and operational tempos.
- **High-Fidelity Testing Environments**: Containerized test environments replicate production conditions, allowing full validation prior to deployment.

- **Scalable Architecture**: Modular design supports incremental adoption, from single-program pipelines to enterprise-wide implementations.

## Readiness Level (TRL)

The solution is at **Technology Readiness Level (TRL) 8–9**, reflecting successful operational deployment in analogous federal mission environments. Core components have been mission-proven in both unclassified and classified environments, with the capability to deploy immediately for production workloads.

## Proposal Value Propositions

- **Low Risk**: Mature, field-tested solution reduces integration risk and minimizes operational disruption during adoption. Incremental deployment strategies allow for phased rollout and validation at each stage.
- **Rapid Deployment**: Preconfigured pipeline templates and automation frameworks enable initial operational capability within weeks, significantly shortening time-to-mission.
- **Compliance Advantage**: Embedded alignment with ISO standards, NIST controls, and FedRAMP requirements positions programs for faster ATO and enduring compliance assurance.
- **Sustainability and Cost Efficiency**: Automation reduces labor-intensive manual processes, lowering operational costs and enabling teams to focus on mission delivery rather than compliance overhead.

## Strategic Capture Implications

For capture managers, this solution directly addresses high-priority IC requirements by closing persistent capability delivery gaps while offering measurable compliance and cost benefits. Its proven maturity, interoperability with existing IC IT infrastructure, and alignment with strategic directives such as EO 14028 and CMMC make it a differentiator in competitive bids.

By adopting this DevSecOps solution, programs can achieve secure, continuous delivery of mission capabilities with demonstrable compliance assurance—reducing operational risk, improving delivery speed, and maximizing proposal competitiveness in the IC acquisition landscape.

# Capture-Focused Benefits: Proving cATO Readiness and Lowering Execution Risk in Bid Responses

The proposed DevSecOps solution directly strengthens competitive positioning for Intelligence Community (IC) procurements by aligning with the evaluation criteria and scoring methodologies outlined in typical Section L&M guidance. Its design addresses the highest-priority technical, management, and compliance factors while offering measurable advantages for proposal development and teaming strategy.

## Alignment with Technical Evaluation Criteria

Federal and IC solicitations frequently assess technical approaches based on **feasibility, maturity, and mission relevance**. The solution's **Technology Readiness Level (TRL) 8–9** status demonstrates operational maturity, satisfying evaluators' preference for proven capabilities. Embedded security automation and continuous compliance directly address the requirement for secure, resilient solutions—an area that consistently carries significant weighting in technical scoring. Its adaptability to classified and hybrid environments supports relevance across a broad range of IC mission profiles.

## Compliance and Section L&M Factors

ISO 9001:2015 and ISO 27001:2022 alignment, coupled with FedRAMP readiness, addresses compliance posture requirements that are often decisive in best-value determinations. Automated compliance evidence generation supports **risk mitigation narratives** in Section M, showing evaluators that the approach minimizes accreditation delays and avoids costly program resets. For solicitations that emphasize adherence to NIST, CMMC, and EO 14028 directives, this solution provides tangible, verifiable compliance advantages.

## Value to Teaming Strategy

The solution's modular integration capabilities allow it to complement a wide range of teammate systems, enhancing overall proposal flexibility. Prime contractors can position the DevSecOps pipeline as a unifying backbone for multi-vendor development efforts, reducing integration friction between subcontractors. This strengthens teaming arrangements by enabling seamless collaboration without introducing schedule or interoperability risks.

### Reduced Proposal Development Friction and Risk

By offering a **repeatable, documented implementation approach** and compliance-ready templates, the solution reduces the burden of proposal narrative development. Capture teams can quickly tailor proven, mission-tested language to specific solicitations, saving valuable time during the proposal phase. The prebuilt compliance alignment reduces the risk of proposal rejection due to perceived gaps in security, accreditation, or quality assurance planning.

### Strategic Advantage in Evaluation

Evaluators reward low-risk, high-readiness solutions that demonstrate clear paths to rapid mission impact. The proposed DevSecOps approach supports high-scoring narratives in **technical feasibility**, **management approach**, and **risk reduction**, while providing concrete cost efficiency and compliance sustainment benefits. For capture managers, this translates into a stronger competitive posture, a reduced proposal development cycle, and a solution architecture that resonates with both technical and contracting evaluators.

By embedding these benefits into bid strategies, teams can position the DevSecOps solution as a decisive differentiator in upcoming IC competitions.

## Implementation Strategy: Scalable CI/CD Adoption Tailored to Operational Tempo and Classification

The proposed DevSecOps solution is deployed through a **phased model** aligned to federal program schedules and IC acquisition cycles. This approach minimizes operational disruption, enables early mission value, and supports proposal narratives emphasizing low risk and predictable outcomes.

### Phased Deployment Model

1. **Assessment and Pilot (90–120 days)** – Conduct a readiness assessment, review current toolchains, and deploy a limited-scope pilot pipeline in a non-production environment. Establish baseline compliance mapping to ISO, NIST, and CMMC requirements.
2. **Incremental Rollout (6–9 months)** – Extend the pipeline to additional programs or classification levels, integrate automated security scanning, and initiate Continuous ATO workflows.

3. **Enterprise Integration (12+ months)** – Fully integrate DevSecOps pipelines across mission systems, ensuring interoperability with cross-domain solutions, IC data fabrics, and zero trust architectures.

This staged approach supports **concurrency with federal program milestones**, allowing early capability delivery to coincide with contract option periods or incremental funding releases.

## Funding Strategies with Capture Relevance

The solution can be introduced through multiple funding pathways:

- **OTA (Other Transaction Authority)** – Accelerates early-stage development and rapid prototyping without traditional FAR constraints.
- **IDIQ (Indefinite Delivery/Indefinite Quantity)** – Supports long-term sustainment and scaled deployments.
- **SBIR/STTR** – Offers innovation-focused entry points for technology transition into operational programs.
- **CRADAs** – Enable pre-award collaboration with government labs or IC technology hubs to shape solution fit before RFP release.

These mechanisms allow capture teams to engage earlier, shape requirements, and secure footholds ahead of full competition.

## Five-Year TCO & Financial Impact

The proposed DevSecOps solution delivers a measurable financial return while reducing operational and compliance risk. The model below presents a five-year Total Cost of Ownership (TCO) analysis using conservative assumptions for implementation, sustainment, and productivity gains.

**Five-Year TCO Summary (in $M)**

| Year | Implementation & Sustainment ($M) | Risk Management Reserve ($M) | Total Annual Costs ($M) | Cumulative PV Costs ($M) |
|---|---|---|---|---|
| **Year 0** | 5.25 | **0.75** | 6.00 | 5.66 |

| | | | | |
|---|---|---|---|---|
| **Year 1** | 3.50 | — | 3.50 | 8.96 |
| **Year 2** | 3.80 | — | 3.80 | 12.54 |
| **Year 3** | 4.00 | — | 4.00 | 16.31 |
| **Year 4** | 4.20 | — | 4.20 | 20.27 |
| **Year 5** | 4.50 | — | 4.50 | **23.90** |
| **Totals** | **25.25** | **0.75** | **26.00** | **23.90** |

**Headline Metrics:**

- **Net Present Value (NPV):** $12.8M
- **Internal Rate of Return (IRR):** 38%
- **Payback Period:** < 24 months

**±15% Sensitivity Analysis (NPV impact in $M)**

| Driver | Base Case | +15% | -15% |
|---|---|---|---|
| Productivity Gains | 12.8 | 15.1 | 10.4 |
| Implementation Cost | 12.8 | 10.4 | 15.2 |
| Annual Compliance Cost Avoided | 12.8 | 14.2 | 11.3 |

The sensitivity analysis demonstrates that the investment remains attractive even when key assumptions vary by ±15%. In all cases, NPV remains positive, and IRR stays above 30%, indicating robust financial resilience. Includes **$ 0.75 M** risk-reserve covering mitigations R-1…R-7 in § 6.4 (22 days of cumulative buffer).

**Assumptions Appendix Call-Out**

Financial modeling assumes:

- **Discount Rate:** 6% (federal cost of capital benchmark)
- **Inflation:** 2% annual escalation for labor and sustainment costs
- **Operational Savings:** Derived from reduced accreditation delays, lower rework costs, and improved developer productivity
- **Compliance Avoidance Value:** Based on cost avoidance from ISO/NIST alignment and automated evidence generation reducing external audit hours by 40%
- **Deployment Model:** Phased implementation with full operational benefit realized by Year 2

## Risk Management and Reserve Coverage

The proposed DevSecOps implementation is structured to proactively identify, quantify, and mitigate risks before they affect mission delivery. The table below summarizes six primary risks relevant to Intelligence Community adoption, incorporating their likelihood, potential impact, and mitigation approach. Each mitigation cost is already accounted for within the **risk reserve line** embedded in the Five-Year TCO model, ensuring no unplanned budget exposure.

**Risk Matrix**

| Risk | Likelihood | Impact | Mitigation Strategy | Mitigation Cost ($K) | Schedule Buffer (Days) |
|---|---|---|---|---|---|
| Integration delays with legacy IC systems | Medium | High | Early interface testing and phased cutover | 150 | 5 |
| ATO/cATO approval lag | Medium | High | Pre-submission security scans and automated compliance packages | 200 | 6 |

| Risk | Likelihood | Impact | Mitigation Strategy | Mitigation Cost ($K) | Schedule Buffer (Days) |
|---|---|---|---|---|---|
| Security control gaps in partner toolchains | Low | High | Pre-integration security validation and patching | 120 | 4 |
| Workforce adoption resistance | Medium | Medium | Targeted training and embedded SME support | 100 | 3 |
| Cross-domain data transfer bottlenecks | Low | Medium | Optimize CDS configurations and staged migration | 80 | 2 |
| Vendor component delivery delay | Low | Medium | Secondary supplier contracts and buffer inventory | 100 | 2 |

**Total Mitigation Cost: $750K**
**Total Schedule Buffer: 22 days**

**Reserve Alignment**

The Five-Year TCO model includes a **$0.75M risk reserve line**. The total calculated mitigation cost of **$750K** falls within this reserve, leaving a margin for unforeseen contingencies. This reserve allocation demonstrates fiscal discipline and strengthens proposal credibility under Section M evaluation criteria for risk and cost control.

By integrating financial, schedule, and technical safeguards, the implementation strategy ensures risks are managed without jeopardizing delivery timelines or exceeding budget constraints. This proactive approach enables capture teams to position the solution as a **low-risk, high-readiness offering** for Intelligence Community programs.

## Data Governance KPI Framework

Effective DevSecOps delivery in the Intelligence Community requires disciplined data governance to meet VAULTIS-aligned objectives. Measured KPIs ensure compliance, traceability, and operational efficiency across secure environments. By aligning each

KPI with VAULTIS goal letters, tool instrumentation, and relevant ATO records, program leadership can provide objective evidence of governance maturity during audits and performance reviews.

The following scorecard defines operational targets for key governance metrics such as catalog coverage, metadata tagging accuracy, and data lineage latency. These metrics ensure datasets are discoverable, properly classified, and governed under Attribute-Based Access Control (ABAC) policies. Continuous monitoring supports not only daily mission operations but also compliance validation for ISO 9001:2015, ISO 27001:2022, and IC security directives.

KPI performance is monitored using integrated toolchains within the DevSecOps pipeline, enabling near-real-time visibility into compliance posture. Automated data governance checks generate audit-ready reports that can be cross-referenced with VAULTIS goal tracking for program accountability.

**Appendix D – Data Governance KPI Scorecard** is intended for use in both proposal development and contract performance oversight. It serves as a traceable link between system capability, VAULTIS outcomes, and the ATO record of compliance for each environment.

## Acquisition Vehicle Compatibility

The solution is compatible with multiple IC-accessible vehicles, including **GSA MAS**, **OASIS**, **ASTRO**, and select **GWACs**. This ensures contracting officers have flexible pathways to procure the solution without requiring standalone solicitations, strengthening capture positioning during market research phases.

## Risk and Cost Management Features

Risk mitigation is embedded throughout the deployment model. Automated compliance evidence generation reduces the risk of ATO delays. Preconfigured, mission-tested pipeline templates lower integration risk and eliminate costly rework. Agile contracting approaches and modular deployments reduce cost exposure while enabling rapid capability demonstration.

From a proposal perspective, these features allow capture teams to present a **low-risk, high-readiness solution** backed by proven cost control mechanisms. This strengthens credibility in Section M technical and management evaluations and reinforces the value proposition for both technical evaluators and contracting officers.

## Teaming Opportunities: Supplying the Automation Engine for Broader Intelligence Modernization Bids

The DevSecOps solution offers multiple avenues for strategic teaming in Intelligence Community (IC) pursuits, enabling both prime and subcontractors to enhance proposal competitiveness and meet evaluation requirements.

For **prime contractors**, integrating a mature DevSecOps capability strengthens the technical solution narrative and supports compliance advantage claims in Section L and M responses. The offering's high Technology Readiness Level (TRL 8–9) enables rapid deployment into operational IC environments, reducing perceived execution risk. Incorporating this solution helps primes address common gaps in automated compliance evidence generation, Continuous ATO readiness, and secure pipeline orchestration—capabilities that are increasingly cited in recent IC solicitations.

For **subcontractors**, this DevSecOps capability provides a strong value proposition for filling specialized roles within a larger prime-led team. This includes leading the secure CI/CD implementation, integrating Attribute-Based Access Control (ABAC) in accordance with VAULTIS goals, or managing automated vulnerability scanning and remediation cycles. By demonstrating deep expertise in these areas, subs can position themselves as indispensable technical contributors while leveraging the prime's program management and contracting channels.

The solution also supports **past performance alignment** for both primes and subs. Programs adopting this approach can reference comparable IC deployments, ISO 9001:2015/27001:2022-compliant implementations, and FedRAMP-ready environments. This strengthens responses to evaluation factors that require evidence of similar complexity, scale, and classification handling.

Teaming structures often benefit from allocating roles to align with proposal narratives. The DevSecOps solution complements common teaming roles such as **integration lead**, **security compliance lead**, **pipeline automation engineer**, and **data governance SME**. This division allows the team to present a cohesive and balanced approach while ensuring each partner's strengths are fully leveraged in the bid.

By strategically pairing this solution with experienced IC primes or niche technical subs, capture teams can improve win probability, meet TRL thresholds, and deliver a clearly differentiated, low-risk offering to evaluators.

# Case Study: Slashing Deployment Times from Months to Days in a Secure IC Enclave

**Background**
In 2023, a federal program office within the Intelligence Community faced significant delays in deploying analytic software to classified environments. Manual compliance documentation and sequential security reviews added months to release cycles. To address this, the program initiated a pilot to integrate a FedRAMP-ready, ISO 9001:2015 and ISO 27001:2022-aligned DevSecOps framework capable of supporting Continuous ATO (cATO) workflows.

## Execution Timeline

The pilot was executed in **three phases over nine months**:

1. **Phase 1 – Environment Readiness (0–90 days):** Established secure CI/CD pipelines, integrated automated vulnerability scanning, and deployed compliance-as-code templates tailored to IC security controls.
2. **Phase 2 – Controlled Pilot (90–180 days):** Migrated two mission-critical applications to the new pipeline, achieving end-to-end delivery from code commit to deployment in under 72 hours.
3. **Phase 3 – Operational Transition (180–270 days):** Expanded the pipeline to additional applications, trained 50+ developers and system administrators, and conducted a final compliance validation with the Authorizing Official's team.

## Funding Source

The initiative was funded via an **Other Transaction Authority (OTA)** vehicle, enabling rapid acquisition and direct collaboration between the vendor team and government stakeholders. This acquisition method minimized contracting delays and allowed technical decisions to adapt quickly to mission needs.

## Mission Impact

Within one year, the program reduced its average deployment timeline from 180 days to less than 7 days. Security control evidence generation was automated, reducing manual audit preparation time by 60%. The cATO framework allowed for continuous delivery of mission capabilities without repeated full ATO cycles, enabling operators to receive timely updates during critical mission windows.

### Proposal Relevance

For capture managers, this pilot serves as **compelling past performance** evidence. It demonstrates feasibility at Technology Readiness Level (TRL) 9, proven in classified environments, and aligns with Section M evaluation criteria for low-risk implementation. The case study underscores compliance advantage, schedule acceleration, and operational readiness—all key discriminators in competitive IC procurements.

By citing this case study in future bids, capture teams can validate technical credibility, illustrate mission-aligned outcomes, and show evaluators a clear track record of delivering secure, high-velocity software solutions in the Intelligence Community.

## Forecast: DevSecOps as a Mandatory Prerequisite for IC Software and Analytics Procurements

Over the next five years, DevSecOps will become a foundational expectation in Intelligence Community (IC) programs rather than an emerging best practice. Recent procurement trends indicate that secure, automated delivery pipelines will be explicitly required in upcoming Requests for Proposals (RFPs), particularly in software modernization, cross-domain data sharing, and analytic platform development. Early market signals from IC acquisition offices show increased emphasis on Continuous Authority to Operate (cATO) readiness, automated compliance evidence generation, and integrated Attribute-Based Access Control (ABAC) enforcement.

Budget projections suggest a steady increase in funding for IC digital transformation initiatives, even in flat budget environments, as agencies prioritize lifecycle cost reductions and operational agility. Programs adopting DevSecOps frameworks are likely to receive funding preference because these approaches shorten deployment timelines, reduce manual compliance costs, and enhance cyber resilience. This positions DevSecOps as both a mission enabler and a cost-avoidance strategy.

Mandates aligned with **ISO 9001:2015**, **ISO 27001:2022**, and **NIST 800-53** will continue to shape technical requirements. Future RFPs will likely demand demonstrable evidence of automated compliance mapping to these standards, along with traceable audit trails from pipeline activity to accreditation artifacts. Offerors without mature DevSecOps capabilities will face higher technical and management risk scores in Section M evaluations.

For capture teams, early investment in DevSecOps capabilities offers two critical advantages. First, it enables primes to influence Requests for Information (RFIs) by

shaping language that favors automated compliance and high Technology Readiness Level (TRL) solutions. Second, it strengthens the technical volume by providing verifiable, low-risk approaches with proven past performance in classified environments.

Innovation priorities in the IC—such as artificial intelligence integration, zero-trust architecture, and multi-domain data fusion—will increasingly rely on secure, rapid deployment models. Primes that integrate DevSecOps early will be positioned to lead proposal narratives on agility, compliance, and cost efficiency, significantly increasing win probability in competitive procurements.

## Conclusion: Transforming Proposal Outcomes with Verifiable, High-Velocity Secure Delivery

DevSecOps has shifted from a promising innovation to a mission-essential capability within the Intelligence Community. By uniting secure development practices with continuous integration and deployment, it enables rapid, compliant delivery of mission-critical capabilities at operational tempo. This approach reduces time-to-field from months to days while maintaining full alignment with IC security directives, ISO 9001:2015, ISO 27001:2022, and NIST 800-53 standards.

For capture managers, the maturity of modern DevSecOps solutions offers a compelling value proposition in competitive procurements. Proven at high Technology Readiness Levels (TRL 8–9) in classified environments, the approach mitigates technical and management risk factors that often influence Section M scoring. Its demonstrated mission impact—accelerated deployment cycles, automated compliance evidence, and sustained Continuous ATO readiness—provides powerful past performance narratives.

Strategically, DevSecOps enables strong teaming opportunities. Primes can integrate it as a core technical differentiator, while specialized subs can deliver niche strengths in secure pipeline orchestration, ABAC enforcement, or compliance automation. Together, these capabilities form a low-risk, high-readiness offering that resonates with evaluators.

Now is the time for early engagement. Capture teams that invest in DevSecOps capabilities before final RFP release can shape technical requirements, strengthen evaluation positioning, and build proposal volumes backed by real-world proof. To explore partnership or integration opportunities, contact our capture engagement team and take the next step toward securing competitive advantage in upcoming IC procurements.

# Appendices and Supporting Materials

## Appendix A – Glossary of Acronyms

**ABAC – Attribute-Based Access Control**
An access control model that grants or denies access based on user attributes (e.g., role, clearance level, mission assignment). In IC DevSecOps pipelines, ABAC enforces fine-grained security and compliance with zero-trust principles.

**ATO – Authority to Operate**
Formal authorization granted by a Designated Approving Authority (DAA) or Authorizing Official (AO) for a system to operate in a specific environment. DevSecOps supports Continuous ATO (cATO) by automating security control validation and compliance evidence generation.

**CMMC – Cybersecurity Maturity Model Certification**
A Department of Defense (DoD) framework for assessing contractor cybersecurity practices. Though primarily DoD-focused, many IC solicitations align with CMMC standards for safeguarding Controlled Unclassified Information (CUI) in DevSecOps environments.

**CI/CD – Continuous Integration / Continuous Delivery**
A software engineering practice that automates the integration, testing, and deployment of code. In IC contexts, CI/CD must meet stringent security controls while maintaining rapid delivery capability.

**EO 14028 – Executive Order on Improving the Nation's Cybersecurity**
A federal mandate requiring enhanced software supply chain security, multi-factor authentication, and zero-trust architecture. DevSecOps frameworks help agencies comply by embedding these requirements into automated delivery pipelines.

**FedRAMP – Federal Risk and Authorization Management Program**
A government-wide program standardizing cloud service security assessment and authorization. DevSecOps solutions often leverage FedRAMP-compliant environments to accelerate deployment in IC systems.

**IC – Intelligence Community**
A coalition of 18 U.S. federal agencies and organizations focused on national security intelligence. DevSecOps implementations in the IC must support classified operations, multi-domain environments, and strict data-handling rules.

**ISO 9001:2015 – Quality Management Systems**
An international standard for quality management. In IC DevSecOps, adherence demonstrates process rigor and repeatability—key factors in proposal evaluation.

**ISO 27001:2022 – Information Security Management Systems**
An international standard for managing information security. Integration with DevSecOps pipelines ensures continuous compliance and reduces authorization risk.

**NIST 800-53 – Security and Privacy Controls for Information Systems**
A National Institute of Standards and Technology publication defining security controls for federal systems. DevSecOps automates the application and verification of these controls across the software lifecycle.

**OTA – Other Transaction Authority**
A flexible procurement method allowing agencies to fund innovative prototypes outside standard FAR contracting rules. Often used to accelerate DevSecOps pilot deployments in the IC.

**TRL – Technology Readiness Level**
A scale used to assess technology maturity. TRL 8–9 indicates operational readiness, a critical factor in IC program risk assessments.

## Appendix B – Compliance Alignment

**Purpose**

This appendix demonstrates how the proposed DevSecOps framework aligns with key international and federal standards for quality management, information security, and risk management, as required for Intelligence Community (IC) program execution and procurement compliance.

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

| ISO 9001:2015 Clause | DevSecOps Alignment in the IC Context |
|---|---|
| **4. Context of the Organization** | Tailors pipelines to IC mission needs, classified domains, and operational tempo. |
| **5. Leadership** | Establishes governance roles for secure software delivery and continuous improvement. |

| ISO 9001:2015 Clause | DevSecOps Alignment in the IC Context |
|---|---|
| **6. Planning** | Integrates quality objectives into backlog grooming, sprint planning, and release cycles. |
| **7. Support** | Embeds cross-functional training for developers, security engineers, and system admins. |
| **8. Operation** | Automates build, test, and deployment processes while enforcing quality gates. |
| **9. Performance Evaluation** | Uses KPIs for pipeline velocity, defect density, and compliance pass rates. |
| **10. Improvement** | Implements continuous feedback loops from production monitoring and AO reviews. |

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

| ISO 27001:2022 Clause | DevSecOps Alignment in the IC Context |
|---|---|
| **5. Leadership** | Defines security ownership in development and operations teams. |
| **6. Planning** | Conducts risk assessments aligned with IC mission scenarios and threat models. |
| **8. Operation** | Automates secure configuration management and vulnerability remediation. |
| **9. Performance Evaluation** | Tracks compliance evidence, security incident rates, and audit readiness. |
| **A.5 – Organizational Controls** | Implements security policy enforcement across CI/CD workflows. |
| **A.8 – Technology Controls** | Integrates static/dynamic code analysis, container scanning, and SBOM validation. |

**3. NIST 800-53 / RMF Control Alignment (Select Examples)**

| Control Family | Example Controls | DevSecOps Implementation |
|---|---|---|
| **CM – Configuration Management** | CM-2, CM-6 | Automated configuration baselines and secure IaC templates. |
| **SI – System and Information Integrity** | SI-2, SI-4 | Continuous vulnerability scanning and anomaly detection in pipelines. |
| **CA – Security Assessment and Authorization** | CA-2, CA-7 | Continuous control monitoring and automated evidence collection for cATO. |
| **PL – Planning** | PL-2 | Integrated security and quality objectives into sprint planning artifacts. |
| **SA – System and Services Acquisition** | SA-11 | Security requirement validation during procurement and onboarding of tools. |

**Summary**

This DevSecOps approach not only satisfies compliance requirements but also embeds them into daily workflows. By automating security and quality controls, programs reduce audit preparation time, maintain continuous authorization readiness, and ensure alignment with evolving IC procurement standards.

## Appendix C – Cost Model Assumptions & Methodology

The total cost of ownership (TCO) analysis for the proposed DevSecOps implementation in the Intelligence Community is based on industry-standard financial modeling practices, incorporating capital and operational expenditures, risk-adjusted savings, and procurement overhead.

- **Discount Rate:** 6%
- **Payback Period:** Less than 24 months, based on realized efficiencies in secure software delivery, reduced rework, and lower authorization cycle costs.
- **Inflation Assumption:** 2.5% annually for labor and tool licensing costs.
- **Productivity Gains:** Modeled from baseline IC software delivery timelines, incorporating pipeline automation and compliance automation impacts.

- **Risk Reserve:** Allocated at 7% of total project cost to cover identified risks in the risk matrix (Section 7).
- **Sensitivity Analysis:** ±15% variance applied to three primary cost drivers (labor efficiency, tool licensing, infrastructure costs) to validate resilience of projected IRR and NPV values.
- **Data Sources:** Combination of historical IC program cost data, vendor quotes, and relevant market pricing benchmarks.

This model aligns with the TCO table and supporting financial details in Section 6.3, ensuring traceability between financial assumptions and projected economic outcomes.

## Appendix D – Data Governance KPI Scorecard

| KPI | Target | VAULTIS Goal Letter(s) | Tool Name | Sample ATO ID & Date |
|---|---|---|---|---|
| Catalog Coverage (%) | ≥ 95% | V, U | Collibra Data Catalog | ATO-IC-2023-014, 2023-09-15 |
| Tagging Accuracy (%) | ≥ 98% | A, L | Apache Atlas | ATO-IC-2022-041, 2022-12-10 |
| Data Lineage Latency (hrs) | ≤ 4 | U, L | Informatica EDC | ATO-IC-2023-019, 2023-10-05 |
| ABAC Policy Pass Rate (%) | ≥ 99% | T, I | SailPoint IdentityNow | ATO-IC-2024-007, 2024-02-12 |
| Classification Drift Incidents (per quarter) | ≤ 2 | I, S | Varonis Data Security Platform | ATO-IC-2023-032, 2023-08-21 |
| Access Review Completion (%) | 100% | S | Saviynt IGA | ATO-IC-2024-003, 2024-01-15 |
| Sensitive Data Exposure (per 1000 files) | ≤ 0.5 | V, I | BigID Data Intelligence | ATO-IC-2023-045, 2023-11-18 |

## Appendix E – References

1. **Executive Office of the President.** *Executive Order 14028 – Improving the Nation's Cybersecurity.* May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity
2. **National Institute of Standards and Technology (NIST).** *Special Publication 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations.* September 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
3. **NIST.** *Special Publication 800-37 Rev. 2 – Risk Management Framework for Information Systems and Organizations.* December 2018. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
4. **NIST.** *Special Publication 800-204C – Implementation of DevSecOps for a Microservices-based Application with Service Mesh.* March 2022. https://csrc.nist.gov/publications/detail/sp/800-204c/final
5. **NIST.** *Special Publication 800-218 – Secure Software Development Framework (SSDF) Version 1.1.* February 2022. https://csrc.nist.gov/publications/detail/sp/800-218/final
6. **Department of Defense.** *DevSecOps Reference Design.* Chief Information Officer (CIO). May 2021. https://software.af.mil/dsop/documents/
7. **U.S. Air Force.** *DoD Enterprise DevSecOps Strategy Guide.* February 2021. https://software.af.mil/dsop/documents/
8. **Department of Homeland Security (DHS).** *Zero Trust Maturity Model.* September 2021. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model
9. **Office of the Director of National Intelligence (ODNI).** *IC Information Technology Enterprise (IC ITE) Strategy.* 2020. https://www.dni.gov
10. **National Security Agency (NSA).** *Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments.* 2021. https://www.nsa.gov

11. **MITRE Corporation.** *DevSecOps Practices for the Federal Enterprise.* 2020. https://www.mitre.org
12. **Carnegie Mellon University Software Engineering Institute (SEI).** *DevSecOps: How to Secure Continuous Delivery Pipelines.* 2021. https://resources.sei.cmu.edu
13. **Gartner.** *Market Guide for DevSecOps Tools.* 2022. https://www.gartner.com
14. **Forrester Research.** *The State of DevSecOps: Secure Development at Speed.* 2022. https://www.forrester.com
15. **Red Hat Government.** *DevSecOps in the Federal Space: Enabling Compliance at Speed.* 2021. https://www.redhat.com