Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
NAVWAR PAO approved

Topic # X224-OCSO1
IRONCLAD: Integrated Resilient Operations for Naval Cloud and AI Deployments
Colvin Run Networks, Inc.

WHO

SYSCOM: NAVWAR

Sponsoring Program: Naval Information Warfare Center (NIWC) Atlantic

Transition Target: NAVSEA/ NAVWAR

TPOC: (843) 284-3156

Other Transition Opportunities: PMW 160, Program Executive Office Command, Control, Communications, Computers, and Intelligence (PEO C4I)

Notes: IRONCLAD is built for secure, scalable application hosting and delivery across IL5/6 cloud, legacy shipboard infrastructure, and edge platforms. It includes a live CI/CD pipeline, telemetry, hardened containers, and compliance automation. Its edge-ready architecture makes it ideal for disconnected operations. Built on Google Cloud with consistent codebase between commercial and government regions, it simplifies deployment and accelerates ATO readiness. IRONCLAD is operational today and aligns with the PAS MVP delivery schedule.

IRONCLAD is production-ready for SBIR Phase III pre-competed Colvin Run awards rapidly executable via CDAO Tradewinds, GSA MAS, and Seaport-NxG.

WHAT

Operational Need and Improvement: The Navy requires a flexible and secure platform to rapidly deliver mission-critical software across a range of operational environments, including cloud, edge, and disconnected settings. Existing delivery methods are often fragmented, manual, and slow to adapt to mission needs, limiting the effectiveness of software updates and AI/ML capabilities. IRONCLAD addresses this by providing a unified, automated platform for secure application delivery and management, improving resilience, reducing time to field, and supporting continuous modernization aligned to operational tempo.

Specifications Required: The platform must support containerized applications and enable automated deployment, monitoring, and rollback across secure, bandwidth-constrained environments. It must enforce security policies at every stage of the software lifecycle, including hardened containers, SBOM validation, and role-based access control. The architecture must be modular, scalable, and resource-adaptive to support both cloud-hosted and edge-deployed workloads, with built-in support for observability, asynchronous job handling, and disconnected operations. Compatibility with IL5/IL6 environments and alignment with Continuous ATO requirements is essential to ensure rapid accreditation and operational use.

Technology Developed: IRONCLAD is a modular, operational DevSecOps platform built on Google's secure infrastructure. It includes an end-to-end CI/CD pipeline, ArgoCD-driven deployment logic, hardened container services, and telemetry that operates in DDIL conditions. It has been successfully deployed in a cloud environment and is being adapted for afloat production, with support for multi-tenant workloads and real-time updates.

Warfighter Value: IRONCLAD reduces user time lost by streamlining software updates and enabling sub-minute rollback. It improves operational resilience through asynchronous job handling and local observability, allowing mission systems to remain functional without constant connectivity. Its modular structure makes it easy to field new capabilities while maintaining a stable core, ensuring that ships and operators receive timely, secure, and mission-relevant software.

WHEN

Contract Number: N68335-25-C-0103 **Ending on:** Nov 01, 2026

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Implement DDIL Capabilities (Edge Caching, Async Queueing, Degraded Telemetry)	Low	Successful simulation of edge-mode caching and offline queueing; telemetry functions validate in test environments	5	4th QTR FY25
Build and Demo Kubernetes Abstraction Layer	Low	ArgoCD-based "invisible Kubernetes" demo completed; RBAC and GitOps guardrails documented and functional	5	4th QTR FY25
Complete Keycloak + CAC + Logsink Integration	Medium	Auth flow validation passes with IL5 compliance; logsink capture verified	3	4th QTR FY25
Maintain Live Architecture Documentation	Low	Living document created in Confluence or Gitbook; weekly update cadence established		1st QTR FY26
Story-point and Schedule IL5 Roadmap	Low	Milestone dates formalized in Jira/Gantt view; sprint sizing completed	5	1st QTR FY26
Add Operational Language Sample Testing	Low	Functional ingestion and output comparison for Chinese, Farsi, Spanish datasets (cloud vs. IL5 self-hosted)	5	1st QTR FY26

HOW

Projected Business Model: Colvin Run will deliver IRONCLAD as a modular, extensible platform through multiple federal acquisition pathways, including GSA MAS, Seaport-NxG, and SBIR Phase III. Our delivery model supports both direct deployment to government environments and integration with large prime contractors and system integrators. IRONCLAD can be adopted as a full-stack platform or delivered in modular components, such as observability pipelines, hardened CI/CD environments, or AI model hosting, depending on program office priorities. Colvin Run's approach enables rapid fielding of Minimum Viable Products (MVPs) while also supporting long-term sustainment, customization, and onboarding of third-party mission applications.

Company Objectives: Colvin Run's mission is to accelerate the delivery of secure, operational AI/ML and data capabilities to national security environments. IRONCLAD directly supports this objective by enabling container-native delivery of software to afloat, disconnected, and multi-classification environments. Designed with Navy platform modernization principles in mind, IRONCLAD integrates zero trust, compliance automation, and telemetry-based feedback loops to reduce downtime, increase resilience, and improve developer-operator collaboration. The platform is actively aligned to World-Class Alignment Metrics (WAMs) and built to scale across the PEO C4I ecosystem and beyond.

Potential Commercial Applications: The underlying IRONCLAD architecture, combining hardened DevSecOps, Kubernetes abstraction, policy enforcement, and real-time observability, is relevant across sectors managing distributed or sensitive workloads. Commercial applications include telecommunications edge management, autonomous systems infrastructure, secure software delivery for critical energy and transportation networks, and compliance-driven hybrid cloud platforms for financial or healthcare data. Its ability to operate in constrained, disconnected, or hybrid environments makes it attractive to industries requiring operational resilience and rapid iteration under strict regulatory or environmental conditions.

Contact: Bruce Olson, VP, Growth and Operations
Bruce@colvinrun.com (360) 551-0552