

Argos Advanced Solutions

Applied intelligence for missions that matter

Capability overview for government, defense, public safety, healthcare, enterprise, and community partners.

Argos turns complex operational problems into secure, usable systems by combining AI strategy, software, data, automation, biometrics, sensors, immersive training, integration, and workforce development.

Executive overview

Argos Advanced Solutions is a veteran-led applied innovation partner. The company works from the real workflow outward, helping leaders identify where technology can create value, prove the idea through a focused pilot, connect the capability to existing operations, and prepare the people who will use it.

The portfolio spans trusted identity, public-safety training, defense logistics, vehicle intelligence, business operations, program outcomes, digital literacy, family development, ministry, and international community initiatives. The common thread is practical technology designed around mission context, human judgment, security, and accountability.

Why Argos

- One multidisciplinary team across strategy, architecture, development, integration, training, and ongoing support.
- Experience connecting AI with devices, sensors, identity, operational records, policy, and human review.
- A delivery model that can begin with advisory work, a short prototype sprint, a full build, or a long-term partnership.
- A mission orientation shaped by more than 25 years of leadership across small business, CIO roles, cybersecurity, AI, military service, and community work.
- $276,500 in verified non-dilutive funding reported by Argos, including grant and research awards.

The market position

Argos brings technical depth and operational judgment to missions where identity, readiness, accountability, and community trust matter.

The Argos AI Lab

The AI Lab is the clearest expression of Argos capability. It presents a full operating model rather than a narrow model-development offer.

Capability	What it means for a client
AI strategy and readiness	Opportunity mapping, workflow and data readiness, architecture review, build-versus-buy analysis, governance, and a sequenced roadmap.
Custom AI systems	Applications that connect the interface, model layer, data, security controls, and operational guardrails.
Agents and automation	Tool-using agents and workflows with review gates, audit trails, and human checkpoints.
Data and knowledge	Ingestion, databases, vector stores, retrieval design, evaluation, and source-cited answers.
Integration and APIs	AI connected to legacy and line-of-business systems, identity, access, monitoring, and rollback paths.
Private AI infrastructure	Local inference and restricted environments for sensitive data and controlled networks.
Training and support	Executive, technical, operator, and public-sector learning built around the client's systems and policies.

A delivery model built around adoption

Discover. Map the workflow, users, systems, data, decisions, and constraints. Separate the problems AI can move from the problems it cannot.

Design. Define the user experience, architecture, security boundaries, human review, measures, and operating model.

Prototype. Build enough of the system to test the hardest assumptions with users and real evidence.

Validate. Evaluate quality, safety, cost, latency, usability, and whether the intervention changes the target outcome.

Integrate. Connect the capability to existing systems, identity, policies, records, and support processes.

Train. Prepare leaders, technical staff, and operators to use and govern the capability.

Operate and improve. Monitor performance, update models and workflows, strengthen controls, and expand only where evidence supports it.

Portfolio evidence

The following experiences demonstrate the range of problems Argos can structure and build around. Some are public concepts, prototypes, pilots, or draft experiences. They should be presented as evidence of capability unless a separate source confirms deployment status or customer results.

HeartID. Cardiac biometric identity and continuous authentication concepts across wearable and device surfaces.

HeartID Guardian. A Hilliard operational pilot interface that separates authentication from authorization and combines person-specific policy, context, sensor state, short validity windows, and auditable decisions.

Phantom Acquired. Immersive training concepts with scenario practice, performance review, physiological analysis, and adaptive learning for high-consequence environments.

Soldier OCIE. AI-assisted equipment accountability using scanning, photographic condition evidence, catalog validation, signatures, offline workflows, and readiness roll-ups.

KryLocke-vHIP. Vehicle-health intelligence that structures OBD, CAN, diagnostic, and historical evidence before using AI to explain likely causes and next tests.

DriveBridge Dealer OS. A modular dealership operating environment that demonstrates role-based access and integrated financial and operational workflows.

B.E.S.T. Impact Navigator. A structured experience that turns outcome narratives into alignment insights across goals and measures.

Digital Chaplain. Digital literacy, safety, and faith-informed technology education for adults, parents, military personnel, and community organizations.

Building Foundations of Faith. A father-and-son retreat platform that combines program design, registration, logistics, and an AI-guided family interview.

Hope for Angola. A draft project experience connecting clear service goals, milestone tracking, partnership information, and donor communication for sustainable water access.

Trust and security principles

- Separate identity verification from the policy decision to grant access.
- Keep humans accountable for decisions that require judgment.
- Set data boundaries, access controls, audit trails, and rollback paths before deployment.
- Use structured evidence, evaluation, and source traceability to constrain AI outputs.
- Support private or local infrastructure when sensitive data cannot leave the client environment.
- Design for field realities, including offline operation, device variability, and imperfect connectivity.

Ways to engage

Engagement	Best fit	Typical result
Advisory	Leaders deciding where AI belongs	Opportunity map, roadmap, build-versus-buy position
Prototype or pilot sprint	A team that needs something real to test	Working prototype, evaluation findings, pilot plan
Full build and integration	A validated concept moving into operations	Production system, connected workflows, trained users
Ongoing AI partner	An organization building durable capability	Continuous improvement, updates, governance, team development

Leadership and operating perspective

Jim Locke III, Chief Executive Officer. Veteran-led technology executive with more than 25 years across small business, CIO roles, cybersecurity, AI, military service, training, and community leadership.

Ahmad Khan, Chief Operating Officer. Operational leader working across AI, healthcare, government technology, software development, and early-stage execution.

Derick Hodge, Senior Consultant. Serial operator advising on business development, technology creation, and fundraising. The Phantom Acquired experience also presents the team’s depth in VR, blockchain, and technical architecture.

Recommended next step

Start with one workflow that creates delay, risk, rework, uncertainty, or lost trust. In an Argos capability briefing, the team will clarify the user, operating environment, data, decision, constraints, and measurable outcome. The result is a practical recommendation for advisory work, a pilot, a build, or no technology intervention at all.

Argos Advanced Solutions, Inc.
3800 Trueman Blvd, Hilliard, Ohio 43026
614.805.7000
https://argosadvancedsolutions.com
https://argosadvancedsolutions.com/ai-lab

Source and claim notes

Prepared from the Argos corporate site and AI Lab, the supplied public portfolio experiences, and an authorized review of the HeartID Guardian Hilliard pilot console on September 24, 2026. Public pages can change. Verify current deployment status, customer permissions, grant wording, and any performance claim before external publication.